25th Annual Review of the Field of National Security Law

Conference Manual

Day Two

Sponsored By:

American Bar Association
Standing Committee on Law & National Security

Center for National Security Law
University of Virginia Law School

Center on Law, Ethics, and National Security
Duke University School of Law

Center of National Security and the Law
Georgetown Law

November 5—November 6, 2015

The Capital Hilton
1001 16th Street, NW
Washington, D.C.
## Conference Material: Day Two

### Panel IV

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Bar Association, Model Rules of Professional Conduct</td>
<td>1</td>
</tr>
<tr>
<td>The National Security Lawyer - James Baker</td>
<td>53</td>
</tr>
</tbody>
</table>

### Panel V

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Order: 12333</td>
<td>65</td>
</tr>
<tr>
<td>Information Sharing in the Era of Wikileaks: Balancing Security and Collaboration - Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee – Corin Stone</td>
<td>81</td>
</tr>
<tr>
<td>Notice PCLOB-2015-01, Comments on the Board’s Plan for Examination of EO 12333 Activities</td>
<td>89</td>
</tr>
</tbody>
</table>

### The State of Play: Retooling Uncle Sam Since 9/11

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forty Years After Church-Pike: What’s Different Now? – Joel Brenner</td>
<td>115</td>
</tr>
<tr>
<td>Intelligence Reform and Terrorism Prevention Act of 2004</td>
<td>123</td>
</tr>
<tr>
<td>The Homeland Security Act of 2002</td>
<td>151</td>
</tr>
<tr>
<td>Executive Order 13467</td>
<td>163</td>
</tr>
<tr>
<td>Presidential Policy Directive - 28</td>
<td>169</td>
</tr>
<tr>
<td>USA PATRIOT Improvement and Reauthorization Act of 2005</td>
<td>179</td>
</tr>
<tr>
<td>In re: Sealed Case</td>
<td>189</td>
</tr>
<tr>
<td>Implementing Recommendations of the 9/11 Commission Act of 2007</td>
<td>217</td>
</tr>
<tr>
<td>Intelligence Community Budgets and Appropriations</td>
<td>220</td>
</tr>
</tbody>
</table>
## Conference Material: Day Two (Cont’d)

### Title and Author

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014 Security Clearance Determinations - ODNI</td>
<td>222</td>
</tr>
<tr>
<td>Statistical Transparency Report Regarding Use of National Security Authorities – ODNI</td>
<td>234</td>
</tr>
<tr>
<td>ODNI Organization Chart</td>
<td>239</td>
</tr>
<tr>
<td>IContheRecord.tumblr.com</td>
<td>241</td>
</tr>
<tr>
<td>Intelligence Authorization Act for FY 2010</td>
<td>253</td>
</tr>
<tr>
<td>Weapons of Mass Destruction Commission Report Recommendations - ODNI</td>
<td>257</td>
</tr>
<tr>
<td>Fact Sheet 2011, Office of the Director of National Intelligence</td>
<td>267</td>
</tr>
</tbody>
</table>

### Panel VI

**Domestic Drones**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>North Dakota, House Bill No. 1328</td>
<td>277</td>
</tr>
<tr>
<td>Domestic Drones and Privacy: A Primer – Richard M. Thompson</td>
<td>281</td>
</tr>
</tbody>
</table>

### Panel VII

**The Future of Nuclear Non-Proliferation**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worldwide Threat Assessment of the US Intelligence Community</td>
<td>347</td>
</tr>
<tr>
<td>The Nuclear Nonproliferation Treaty at 45 – Rose Gottemoeller</td>
<td>397</td>
</tr>
<tr>
<td>Achieving a Higher Degree of National Security – Rose Gottemoeller</td>
<td>401</td>
</tr>
<tr>
<td>Towards Zero: Resolving the Contradictions – Rose Gottemoeller</td>
<td>403</td>
</tr>
<tr>
<td>International Law vs the Iran Nuclear Negotiations – David Jonas</td>
<td>405</td>
</tr>
<tr>
<td>Five Reasons Why the Iran Nuclear Deal is Still a Really Bad Idea – David Jonas</td>
<td>407</td>
</tr>
<tr>
<td>Why Iran Doesn’t Trust America – Seyed Hossein Mousavian</td>
<td>411</td>
</tr>
<tr>
<td>Six Achievable Steps for Implementing an Effective Verification Regime</td>
<td>413</td>
</tr>
</tbody>
</table>
Panel IV:

National Security Ethical Challenges and Model Rules

Discussants:
James E. Baker
Lala R. Qadir
Harvey Rishikof
ABA MODEL RULES OF PROFESSIONAL CONDUCT

Client-Lawyer Relationship

Rule 1.1 Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances, for ill-considered action under emergency conditions can jeopardize the client's interest.

[4] A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person. See also Rule 6.2.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may limit the matters for which the lawyer is responsible. See Rule 1.2(c).

Retaining or Contracting With Other Lawyers

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. See also Rules 1.2 (allocation of authority), 1.4 (communication with client), 1.5(c) (fee sharing), 1.6 (confidentiality), and 5.5(a) (unauthorized practice of law). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the education, experience and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[7] When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other and the client about the scope of their respective representations and the
allocation of responsibility among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Rule 1.2 Scope Of Representation And Allocation Of Authority Between Client And Lawyer

(a) Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. A lawyer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.

(b) A lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities.

(c) A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.

(d) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.

Comment

Allocation of Authority between Client and Lawyer

[1] Paragraph (a) confers upon the client the ultimate authority to determine the purposes to be served by legal representation, within the limits imposed by law and the lawyer's professional obligations. The decisions specified in paragraph (a), such as whether to settle a civil matter, must also be made by the client. See Rule 1.4(a)(1) for the lawyer's duty to communicate with the client about such decisions. With respect to the means by which the client's objectives are to be pursued, the lawyer shall consult with the client as required by Rule 1.4(a)(2) and may take such action as is impliedly authorized to carry out the representation.

[2] On occasion, however, a lawyer and a client may disagree about the means to be used to accomplish the client's objectives. Clients normally defer to the special knowledge and skill of their lawyer with respect to the means to be used to accomplish their objectives, particularly with respect to technical, legal and tactical matters. Conversely, lawyers usually defer to the client regarding such questions as the expense to be incurred and concern for third persons who might be adversely affected. Because of the varied nature of the matters about which a lawyer and client might disagree and because the actions in question may implicate the interests of a tribunal or other persons, this Rule does not prescribe how such disagreements are to be resolved. Other law, however, may be applicable and should be consulted by the lawyer. The lawyer should also consult with the client and seek a mutually acceptable resolution of the disagreement. If such efforts are unavailing and the lawyer has a fundamental disagreement with the client, the lawyer may withdraw from the representation. See Rule 1.16(b)(4). Conversely, the client may resolve the disagreement by discharging the lawyer. See Rule 1.16(a)(3).

[3] At the outset of a representation, the client may authorize the lawyer to take specific action on the client's behalf without further consultation. Absent a material change in circumstances and subject to Rule 1.4, a lawyer may rely on such an advance authorization. The client may, however, revoke such authority at any time.

[4] In a case in which the client appears to be suffering diminished capacity, the lawyer's duty to abide by the client's decisions is to be guided by reference to Rule 1.14.
Independence from Client's Views or Activities

[5] Legal representation should not be denied to people who are unable to afford legal services, or whose cause is controversial or the subject of popular disapproval. By the same token, representing a client does not constitute approval of the client's views or activities.

Agreements Limiting Scope of Representation

[6] The scope of services to be provided by a lawyer may be limited by agreement with the client or by the terms under which the lawyer's services are made available to the client. When a lawyer has been retained by an insurer to represent an insured, for example, the representation may be limited to matters related to the insurance coverage. A limited representation may be appropriate because the client has limited objectives for the representation. In addition, the terms upon which representation is undertaken may exclude specific means that might otherwise be used to accomplish the client's objectives. Such limitations may exclude actions that the client thinks are too costly or that the lawyer regards as repugnant or imprudent.

[7] Although this Rule affords the lawyer and client substantial latitude to limit the representation, the limitation must be reasonable under the circumstances. If, for example, a client's objective is limited to securing general information about the law the client needs in order to handle a common and typically uncomplicated legal problem, the lawyer and client may agree that the lawyer's services will be limited to a brief telephone consultation. Such a limitation, however, would not be reasonable if the time allotted was not sufficient to yield advice upon which the client could rely. Although an agreement for a limited representation does not exempt a lawyer from the duty to provide competent representation, the limitation is a factor to be considered when determining the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. See Rule 1.1.


Criminal, Fraudulent and Prohibited Transactions

[9] Paragraph (d) prohibits a lawyer from knowingly counseling or assisting a client to commit a crime or fraud. This prohibition, however, does not preclude the lawyer from giving an honest opinion about the actual consequences that appear likely to result from a client's conduct. Nor does the fact that a client uses advice in a course of action that is criminal or fraudulent of itself make a lawyer a party to the course of action. There is a critical distinction between presenting an analysis of legal aspects of questionable conduct and recommending the means by which a crime or fraud might be committed with impunity.

[10] When the client's course of action has already begun and is continuing, the lawyer's responsibility is especially delicate. The lawyer is required to avoid assisting the client, for example, by drafting or delivering documents that the lawyer knows are fraudulent or by suggesting how the wrongdoing might be concealed. A lawyer may not continue assisting a client in conduct that the lawyer originally supposed was legally proper but then discovers is criminal or fraudulent. The lawyer must, therefore, withdraw from the representation of the client in the matter. See Rule 1.16(a). In some cases, withdrawal alone might be insufficient. It may be necessary for the lawyer to give notice of the fact of withdrawal and to disaffirm any opinion, document, affirmation or the like. See Rule 4.1.

[11] Where the client is a fiduciary, the lawyer may be charged with special obligations in dealings with a beneficiary.

[12] Paragraph (d) applies whether or not the defrauded party is a party to the transaction. Hence, a lawyer must not participate in a transaction to effectuate criminal or fraudulent avoidance of tax liability. Paragraph (d) does not preclude undertaking a criminal defense incident to a general retainer for legal services to a lawful enterprise. The last clause of paragraph (d) recognizes that determining the validity or interpretation of a statute or regulation may require a course of action involving disobedience of the statute or regulation or of the interpretation placed upon it by governmental authorities.

[13] If a lawyer comes to know or reasonably should know that a client expects assistance not permitted by the Rules of Professional Conduct or other law or if the lawyer intends to act contrary to the client's instructions, the lawyer must consult with the client regarding the limitations on the lawyer's conduct. See Rule 1.4(a)(5).

Rule 1.3 Diligence

A lawyer shall act with reasonable diligence and promptness in representing a client.
Comment

[1] A lawyer should pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to
the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor. A lawyer must
also act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf. A lawyer
is not bound, however, to press for every advantage that might be realized for a client. For example, a lawyer may have authority
to exercise professional discretion in determining the means by which a matter should be pursued. See Rule 1.2. The lawyer's
duty to act with reasonable diligence does not require the use of offensive tactics or preclude the treating of all persons involved
in the legal process with courtesy and respect.

[2] A lawyer's work load must be controlled so that each matter can be handled competently.

[3] Perhaps no professional shortcoming is more widely resented than procrastination. A client's interests often can be
adversely affected by the passage of time or the change of conditions; in extreme instances, as when a lawyer overlooks a statute
of limitations, the client's legal position may be destroyed. Even when the client's interests are not affected in substance, however,
unreasonable delay can cause a client needless anxiety and undermine confidence in the lawyer's trustworthiness. A lawyer's duty
to act with reasonable promptness, however, does not preclude the lawyer from agreeing to a reasonable request for a
postponement that will not prejudice the lawyer's client.

[4] Unless the relationship is terminated as provided in Rule 1.16, a lawyer should carry through to conclusion all
matters undertaken for a client. If a lawyer's employment is limited to a specific matter, the relationship terminates when the
matter has been resolved. If a lawyer has served a client over a substantial period in a variety of matters, the client sometimes
may assume that the lawyer will continue to serve on a continuing basis unless the lawyer gives notice of withdrawal. Doubt
about whether a client-lawyer relationship still exists should be clarified by the lawyer, preferably in writing, so that the client
will not mistakenly suppose the lawyer is looking after the client's affairs when the lawyer has ceased to do so. For example, if a
lawyer has handled a judicial or administrative proceeding that produced a result adverse to the client and the lawyer and the
client have not agreed that the lawyer will handle the matter on appeal, the lawyer must consult with the client about the
possibility of appeal before relinquishing responsibility for the matter. See Rule 1.4(a)(2). Whether the lawyer is obligated to
prosecute the appeal for the client depends on the scope of the representation the lawyer has agreed to provide to the client. See
Rule 1.2.

[5] To prevent neglect of client matters in the event of a sole practitioner's death or disability, the duty of diligence may
require that each sole practitioner prepare a plan, in conformity with applicable rules, that designates another competent lawyer to
review client files, notify each client of the lawyer's death or disability, and determine whether there is a need for immediate
protective action. Cf. Rule 28 of the American Bar Association Model Rules for Lawyer Disciplinary Enforcement (providing for
court appointment of a lawyer to inventory files and take other protective action in absence of a plan providing for another lawyer
to protect the interests of the clients of a deceased or disabled lawyer).

Rule 1.4 Communication

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as
defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter; (4) promptly comply with reasonable requests for
information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the
client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed
decisions regarding the representation.

Comment
[1] Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.

**Communicating with Client**

[2] If these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client’s consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously indicated that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. See Rule 1.2(a).

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client’s objectives. In some situations — depending on both the importance of the action under consideration and the feasibility of consulting with the client — this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client’s behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[4] A lawyer’s regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer, or a member of the lawyer’s staff, acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications.

**Explaining Matters**

[5] The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, when there is time to explain a proposal made in a negotiation, the lawyer should review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client’s best interests, and the client’s overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(e).

[6] Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. See Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to the appropriate officials of the organization. See Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

**Withholding Information**

[7] In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer’s own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client. Rule 3.4(c) directs compliance with such rules or orders.

**Rule 1.5 Fees**

(a) A lawyer shall not make an agreement for, charge, or collect an unreasonable fee or an unreasonable amount for expenses. The factors to be considered in determining the reasonableness of a fee include the following:
(1) the time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly;

(2) the likelihood, if apparent to the client, that the acceptance of the particular employment will preclude other employment by the lawyer;

(3) the fee customarily charged in the locality for similar legal services;

(4) the amount involved and the results obtained;

(5) the time limitations imposed by the client or by the circumstances;

(6) the nature and length of the professional relationship with the client;

(7) the experience, reputation, and ability of the lawyer or lawyers performing the services; and

(8) whether the fee is fixed or contingent.

(b) The scope of the representation and the basis or rate of the fee and expenses for which the client will be responsible shall be communicated to the client, preferably in writing, before or within a reasonable time after commencing the representation, except when the lawyer will charge a regularly represented client on the same basis or rate. Any changes in the basis or rate of the fee or expenses shall also be communicated to the client.

(c) A fee may be contingent on the outcome of the matter for which the service is rendered, except in a matter in which a contingent fee is prohibited by paragraph (d) or other law. A contingent fee agreement shall be in a writing signed by the client and shall state the method by which the fee is to be determined, including the percentage or percentages that shall accrue to the lawyer in the event of settlement, trial or appeal; litigation and other expenses to be deducted from the recovery; and whether such expenses are to be deducted before or after the contingent fee is calculated. The agreement must clearly notify the client of any expenses for which the client will be liable whether or not the client is the prevailing party. Upon conclusion of a contingent fee matter, the lawyer shall provide the client with a written statement stating the outcome of the matter and, if there is a recovery, showing the remittance to the client and the method of its determination.

(d) A lawyer shall not enter into an arrangement for, charge, or collect:

(1) any fee in a domestic relations matter, the payment or amount of which is contingent upon the securing of a divorce or upon the amount of alimony or support, or property settlement in lieu thereof; or

(2) a contingent fee for representing a defendant in a criminal case.

(e) A division of a fee between lawyers who are not in the same firm may be made only if:

(1) the division is in proportion to the services performed by each lawyer or each lawyer assumes joint responsibility for the representation;

(2) the client agrees to the arrangement, including the share each lawyer will receive, and the agreement is confirmed in writing; and

(3) the total fee is reasonable.

Comment

Reasonableness of Fee and Expenses

[1] Paragraph (a) requires that lawyers charge fees that are reasonable under the circumstances. The factors specified in (1) through (8) are not exclusive. Nor will each factor be relevant in each instance. Paragraph (a) also requires that expenses for which the client will be charged must be reasonable. A lawyer may seek reimbursement for the cost of services performed in-house, such as copying, or for other expenses incurred in-house, such as telephone charges, either by charging a reasonable
amount to which the client has agreed in advance or by charging an amount that reasonably reflects the cost incurred by the lawyer.

**Basis or Rate of Fee**

[2] When the lawyer has regularly represented a client, they ordinarily will have evolved an understanding concerning the basis or rate of the fee and the expenses for which the client will be responsible. In a new client-lawyer relationship, however, an understanding as to fees and expenses must be promptly established. Generally, it is desirable to furnish the client with at least a simple memorandum or copy of the lawyer's customary fee arrangements that states the general nature of the legal services to be provided, the basis, rate or total amount of the fee and whether and to what extent the client will be responsible for any costs, expenses or disbursements in the course of the representation. A written statement concerning the terms of the engagement reduces the possibility of misunderstanding.

[3] Contingent fees, like any other fees, are subject to the reasonableness standard of paragraph (a) of this Rule. In determining whether a particular contingent fee is reasonable, or whether it is reasonable to charge any form of contingent fee, a lawyer must consider the factors that are relevant under the circumstances. Applicable law may impose limitations on contingent fees, such as a ceiling on the percentage allowable, or may require a lawyer to offer clients an alternative basis for the fee. Applicable law also may apply to situations other than a contingent fee, for example, government regulations regarding fees in certain tax matters.

**Terms of Payment**

[4] A lawyer may require advance payment of a fee, but is obliged to return any unearned portion. See Rule 1.16(d). A lawyer may accept property in payment for services, such as an ownership interest in an enterprise, providing this does not involve acquisition of a proprietary interest in the cause of action or subject matter of the litigation contrary to Rule 1.8 (i). However, a fee paid in property instead of money may be subject to the requirements of Rule 1.8(a) because such fees often have the essential qualities of a business transaction with the client.

[5] An agreement may not be made whose terms might induce the lawyer improperly to curtail services for the client or perform them in a way contrary to the client's interest. For example, a lawyer should not enter into an agreement whereby services are to be provided only up to a stated amount when it is foreseeable that more extensive services probably will be required, unless the situation is adequately explained to the client. Otherwise, the client might have to bargain for further assistance in the midst of a proceeding or transaction. However, it is proper to define the extent of services in light of the client's ability to pay. A lawyer should not exploit a fee arrangement based primarily on hourly charges by using wasteful procedures.

**Prohibited Contingent Fees**

[6] Paragraph (d) prohibits a lawyer from charging a contingent fee in a domestic relations matter when payment is contingent upon the securing of a divorce or upon the amount of alimony or support or property settlement to be obtained. This provision does not preclude a contract for a contingent fee for legal representation in connection with the recovery of post-judgment balances due under support, alimony or other financial orders because such contracts do not implicate the same policy concerns.

**Division of Fee**

[7] A division of fee is a single billing to a client covering the fee of two or more lawyers who are not in the same firm. A division of fee facilitates association of more than one lawyer in a matter in which neither alone could serve the client as well, and most often is used when the fee is contingent and the division is between a referring lawyer and a trial specialist. Paragraph (e) permits the lawyers to divide a fee either on the basis of the proportion of services they render or if each lawyer assumes responsibility for the representation as a whole. In addition, the client must agree to the arrangement, including the share that each lawyer is to receive, and the agreement must be confirmed in writing. Contingent fee agreements must be in a writing signed by the client and must otherwise comply with paragraph (c) of this Rule. Joint responsibility for the representation entails financial and ethical responsibility for the representation as if the lawyers were associated in a partnership. A lawyer should only refer a matter to a lawyer whom the referring lawyer reasonably believes is competent to handle the matter. See Rule 1.1.

[8] Paragraph (e) does not prohibit or regulate division of fees to be received in the future for work done when lawyers were previously associated in a law firm.

**Disputes over Fees**
[9] If a procedure has been established for resolution of fee disputes, such as an arbitration or mediation procedure established by the bar, the lawyer must comply with the procedure when it is mandatory, and, even when it is voluntary, the lawyer should conscientiously consider submitting to it. Law may prescribe a procedure for determining a lawyer's fee, for example, in representation of an executor or administrator, a class or a person entitled to a reasonable fee as part of the measure of damages. The lawyer entitled to such a fee and a lawyer representing another party concerned with the fee should comply with the prescribed procedure.

Rule 1.6 Confidentiality Of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comment

[1] This Rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. See Rule 1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client and Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.
[3] The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope.

[4] Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

**Authorized Disclosure**

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. Lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

**Disclosure Adverse to Client**

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions. Paragraph (b)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial threat that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may disclose this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to eliminate the threat or reduce the number of victims.

[7] Paragraph (b)(2) is a limited exception to the rule of confidentiality that permits the lawyer to reveal information to the extent necessary to make disclosures to affected persons or appropriate authorities to prevent the client from committing a crime or fraud, as defined in Rule 1.0(d), that is reasonably certain to result in substantial injury to the financial or property interests of another and in furtherance of which the client has used or is using the lawyer's services. Such a serious abuse of the client-lawyer relationship by the client forfeits the protection of this Rule. The client can, of course, prevent such disclosure by refraining from the wrongful conduct. Although paragraph (b)(2) does not require the lawyer to reveal the client's misconduct, the lawyer may not counsel or assist the client in conduct the lawyer knows is criminal or fraudulent. See Rule 1.2(d). See also Rule 1.16 with respect to the lawyer's obligation or right to withdraw from the representation of the client in such circumstances, and Rule 1.13(c), which permits the lawyer, where the client is an organization, to reveal information relating to the representation in limited circumstances.

[8] Paragraph (b)(3) addresses the situation in which the lawyer does not learn of the client's crime or fraud until after it has been consummated. Although the client no longer has the option of preventing disclosure by refraining from the wrongful conduct, there will be situations in which the loss suffered by the affected person can be prevented, rectified or mitigated. In such situations, the lawyer may disclose information relating to the representation to the extent necessary to enable the affected persons to prevent or mitigate reasonably certain losses or to attempt to recoup their losses. Paragraph (b)(3) does not apply when a person who has committed a crime or fraud thereafter employs a lawyer for representation concerning that offense.

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer's personal responsibility to comply with these Rules. In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.
[10] Where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true with respect to a claim involving the conduct or representation of a former client. Such a charge can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, for example, a person claiming to have been defrauded by the lawyer and client acting together. The lawyer's right to respond arises when an assertion of such complicity has been made. Paragraph (b)(5) does not require the lawyer to await the commencement of an action or proceeding that charges such complicity, so that the defense may be established by responding directly to a third party who has made such an assertion. The right to defend also applies, of course, where a proceeding has been commenced.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Other law may require that a lawyer disclose information about a client. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of information relating to the representation appears to be required by other law, the lawyer must discuss the matter with the client to the extent required by Rule 1.4. If, however, the other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

Detection of Conflicts of Interest

[13] Paragraph (b)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See Rule 1.17, Comment [7]. Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Any such disclosure should ordinarily include no more than the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information, however, should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. Moreover, the disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (e.g., the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possession of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under these circumstances, paragraph (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these Rules.

[14] Any information disclosed pursuant to paragraph (b)(7) may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. Paragraph (b)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to paragraph (b)(7). Paragraph (b)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, see Comment [5], such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

[15] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4. Unless review is sought, however, paragraph (b)(6) permits the lawyer to comply with the court's order.

[16] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[17] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). In exercising the discretion conferred by this Rule, the
lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may be required, however, by other Rules. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). See Rules 1.2(d), 4.1(b), 8.1 and 8.3. Rule 3.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See Rule 3.3(c).

**Acting Competently to Preserve Confidentiality**

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

**Former Client**

[20] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.

**Rule 1.7 Conflict Of Interest: Current Clients**

(a) Except as provided in paragraph (b), a lawyer shall not represent a client if the representation involves a concurrent conflict of interest. A concurrent conflict of interest exists if:

1. the representation of one client will be directly adverse to another client; or

2. there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer.

(b) Notwithstanding the existence of a concurrent conflict of interest under paragraph (a), a lawyer may represent a client if:

1. the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client;

2. the representation is not prohibited by law;
(3) the representation does not involve the assertion of a claim by one client against another client represented by the lawyer in the same litigation or other proceeding before a tribunal; and

(4) each affected client gives informed consent, confirmed in writing.

Comment

General Principles

[1] Loyalty and independent judgment are essential elements in the lawyer's relationship to a client. Concurrent conflicts of interest can arise from the lawyer's responsibilities to another client, a former client or a third person or from the lawyer's own interests. For specific Rules regarding certain concurrent conflicts of interest, see Rule 1.8. For former client conflicts of interest, see Rule 1.9. For conflicts of interest involving prospective clients, see Rule 1.18. For definitions of "informed consent" and "confirmed in writing," see Rule 1.0(e) and (b).

[2] Resolution of a conflict of interest problem under this Rule requires the lawyer to: 1) clearly identify the client or clients; 2) determine whether a conflict of interest exists; 3) decide whether the representation may be undertaken despite the existence of a conflict, i.e., whether the conflict is consensable; and 4) if so, consult with the clients affected under paragraph (a) and obtain their informed consent, confirmed in writing. The clients affected under paragraph (a) include both of the clients referred to in paragraph (a)(1) and the one or more clients whose representation might be materially limited under paragraph (a)(2).

[3] A conflict of interest may exist before representation is undertaken, in which event the representation must be declined, unless the lawyer obtains the informed consent of each client under the conditions of paragraph (b). To determine whether a conflict of interest exists, a lawyer should adopt reasonable procedures, appropriate for the size and type of firm and practice, to determine in both litigation and non-litigation matters the persons and issues involved. See also Comment to Rule 5.1. Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule. As to whether a client-lawyer relationship exists or, having once been established, is continuing, see Comment to Rule 1.3 and Scope.

[4] If a conflict arises after representation has been undertaken, the lawyer ordinarily must withdraw from the representation, unless the lawyer has obtained the informed consent of the client under the conditions of paragraph (b). See Rule 1.16. Where more than one client is involved, whether the lawyer may continue to represent any of the clients is determined both by the lawyer's ability to comply with duties owed to the former client and by the lawyer's ability to represent adequately the remaining client or clients, given the lawyer's duties to the former client. See Rule 1.9. See also Comments [5] and [29].

[5] Unforeseeable developments, such as changes in corporate and other organizational affiliations or the addition or realignment of parties in litigation, might create conflicts in the midst of a representation, as when a company sued by the lawyer on behalf of one client is bought by another client represented by the lawyer in an unrelated matter. Depending on the circumstances, the lawyer may have the option to withdraw from one of the representations in order to avoid the conflict. The lawyer must seek court approval where necessary and take steps to minimize harm to the clients. See Rule 1.16. The lawyer must continue to protect the confidences of the client from whose representation the lawyer has withdrawn. See Rule 1.9(c).

Identifying Conflicts of Interest: Directly Adverse

[6] Loyalty to a current client prohibits undertaking representation directly adverse to that client without that client's informed consent. Thus, absent consent, a lawyer may not act as an advocate in one matter against a person the lawyer represents in some other matter, even when the matters are wholly unrelated. The client as to whom the representation is directly adverse is likely to feel betrayed, and the resulting damage to the client-lawyer relationship is likely to impair the lawyer's ability to represent the client effectively. In addition, the client on whose behalf the adverse representation is undertaken reasonably may fear that the lawyer will pursue that client's case less effectively out of deference to the other client, i.e., that the representation may be materially limited by the lawyer's interest in retaining the current client. Similarly, a directly adverse conflict may arise when a lawyer is required to cross-examine a client who appears as a witness in a lawsuit involving another client, as when the testimony will be damaging to the client who is represented in the lawsuit. On the other hand, simultaneous representation in unrelated matters of clients whose interests are only economically adverse, such as representation of competing economic enterprises in unrelated litigation, does not ordinarily constitute a conflict of interest and thus may not require consent of the respective clients.

[7] Directly adverse conflicts can also arise in transactional matters. For example, if a lawyer is asked to represent the seller of a business in negotiations with a buyer represented by the lawyer, not in the same transaction but in another, unrelated matter, the lawyer could not undertake the representation without the informed consent of each client.
Identifying Conflicts of Interest: Material Limitation

[8] Even where there is no direct adverseness, a conflict of interest exists if there is a significant risk that a lawyer’s ability to consider, recommend or carry out an appropriate course of action for the client will be materially limited as a result of the lawyer’s other responsibilities or interests. For example, a lawyer asked to represent several individuals seeking to form a joint venture is likely to be materially limited in the lawyer’s ability to recommend or advocate possible positions that each might take because of the lawyer’s duty of loyalty to the others. The conflict in effect forecloses alternatives that would otherwise be available to the client. The mere possibility of subsequent harm does not itself require disclosure and consent. The critical questions are the likelihood that a difference in interests will eventuate and, if it does, whether it will materially interfere with the lawyer’s independent professional judgment in considering alternatives or foreclose courses of action that reasonably should be pursued on behalf of the client.

Lawyer’s Responsibilities to Former Clients and Other Third Persons

[9] In addition to conflicts with other current clients, a lawyer’s duties of loyalty and independence may be materially limited by responsibilities to former clients under Rule 1.9 or by the lawyer’s responsibilities to other persons, such as fiduciary duties arising from a lawyer’s service as a trustee, executor or corporate director.

Personal Interest Conflicts

[10] The lawyer’s own interests should not be permitted to have an adverse effect on representation of a client. For example, if the probity of a lawyer’s own conduct in a transaction is in serious question, it may be difficult or impossible for the lawyer to give a client detached advice. Similarly, when a lawyer has discussions concerning possible employment with an opponent of the lawyer’s client, or with a law firm representing the opponent, such discussions could materially limit the lawyer’s representation of the client. In addition, a lawyer may not allow related business interests to affect representation, for example, by referring clients to an enterprise in which the lawyer has an undisclosed financial interest. See Rule 1.8 for specific Rules pertaining to a number of personal interest conflicts, including business transactions with clients. See also Rule 1.10 (personal interest conflicts under Rule 1.7 ordinarily are not imputed to other lawyers in a law firm).

[11] When lawyers representing different clients in the same matter or in substantially related matters are closely related by blood or marriage, there may be a significant risk that client confidences will be revealed and that the lawyer’s family relationship will interfere with both loyalty and independent professional judgment. As a result, each client is entitled to know of the existence and implications of the relationship between the lawyers before the lawyer agrees to undertake the representation. Thus, a lawyer related to another lawyer, e.g., as parent, child, sibling or spouse, ordinarily may not represent a client in a matter where that lawyer is representing another party, unless each client gives informed consent. The disqualification arising from a close family relationship is personal and ordinarily is not imputed to members of firms with whom the lawyers are associated. See Rule 1.10.

[12] A lawyer is prohibited from engaging in sexual relationships with a client unless the sexual relationship predates the formation of the client-lawyer relationship. See Rule 1.8(j).

Interest of Person Paying for a Lawyer’s Service

[13] A lawyer may be paid from a source other than the client, including a co-client, if the client is informed of that fact and consents and the arrangement does not compromise the lawyer’s duty of loyalty or independent judgment to the client. See Rule 1.8(f). If acceptance of the payment from any other source presents a significant risk that the lawyer’s representation of the client will be materially limited by the lawyer’s own interest in accommodating the person paying the lawyer’s fee or by the lawyer’s responsibilities to a payer who is also a co-client, then the lawyer must comply with the requirements of paragraph (b) before accepting the representation, including determining whether the conflict is consentable and, if so, that the client has adequate information about the material risks of the representation.

Prohibited Representations

[14] Ordinarily, clients may consent to representation notwithstanding a conflict. However, as indicated in paragraph (b), some conflicts are nonconsentable, meaning that the lawyer involved cannot properly ask for such agreement or provide representation on the basis of the client’s consent. When the lawyer is representing more than one client, the question of consentability must be resolved as to each client.

[15] Consentability is typically determined by considering whether the interests of the clients will be adequately protected if the clients are permitted to give their informed consent to representation burdened by a conflict of interest. Thus,
under paragraph (b)(1), representation is prohibited if in the circumstances the lawyer cannot reasonably conclude that the lawyer will be able to provide competent and diligent representation. See Rule 1.1 (competence) and Rule 1.3 (diligence).

[16] Paragraph (b)(2) describes conflicts that are nonconsentable because the representation is prohibited by applicable law. For example, in some states substantive law provides that the same lawyer may not represent more than one defendant in a capital case, even with the consent of the clients, and under federal criminal statutes certain representations by a former government lawyer are prohibited, despite the informed consent of the former client. In addition, decisional law in some states limits the ability of a governmental client, such as a municipality, to consent to a conflict of interest.

[17] Paragraph (b)(3) describes conflicts that are nonconsentable because of the institutional interest in vigorous development of each client's position when the clients are aligned directly against each other in the same litigation or other proceeding before a tribunal. Whether clients are aligned directly against each other within the meaning of this paragraph requires examination of the context of the proceeding. Although this paragraph does not preclude a lawyer's multiple representation of adverse parties to a mediation (because mediation is not a proceeding before a "tribunal" under Rule 1.0(m)), such representation may be precluded by paragraph (b)(1).

Informed Consent

[18] Informed consent requires that each affected client be aware of the relevant circumstances and of the material and reasonably foreseeable ways that the conflict could have adverse effects on the interests of that client. See Rule 1.0(e) (informed consent). The information required depends on the nature of the conflict and the nature of the risks involved. When representation of multiple clients in a single matter is undertaken, the information must include the implications of the common representation, including possible effects on loyalty, confidentiality and the attorney-client privilege and the advantages and risks involved. See Comments [30] and [31] (effect of common representation on confidentiality).

[19] Under some circumstances it may be impossible to make the disclosure necessary to obtain consent. For example, when the lawyer represents different clients in related matters and one of the clients refuses to consent to the disclosure necessary to permit the other client to make an informed decision, the lawyer cannot properly ask the latter to consent. In some cases the alternative to common representation can be that each party may have to obtain separate representation with the possibility of incurring additional costs. These costs, along with the benefits of securing separate representation, are factors that may be considered by the affected client in determining whether common representation is in the client's interests.

Consent Confirmed in Writing

[20] Paragraph (b) requires the lawyer to obtain the informed consent of the client, confirmed in writing. Such a writing may consist of a document executed by the client or one that the lawyer promptly records and transmits to the client following an oral consent. See Rule 1.0(b). See also Rule 1.0(n) (writing includes electronic transmission). If it is not feasible to obtain or transmit the writing at the time the client gives informed consent, then the lawyer must obtain or transmit it within a reasonable time thereafter. See Rule 1.0(b). The requirement of a writing does not supplant the need in most cases for the lawyer to talk with the client, to explain the risks and advantages, if any, of representation burdened with a conflict of interest, as well as reasonably available alternatives, and to afford the client a reasonable opportunity to consider the risks and alternatives and to raise questions and concerns. Rather, the writing is required in order to impress upon clients the seriousness of the decision the client is being asked to make and to avoid disputes or ambiguities that might later occur in the absence of a writing.

Revoking Consent

[21] A client who has given consent to a conflict may revoke the consent and, like any other client, may terminate the lawyer's representation at any time. Whether revoking consent to the client's own representation precludes the lawyer from continuing to represent other clients depends on the circumstances, including the nature of the conflict, whether the client revoked consent because of a material change in circumstances, the reasonable expectations of the other client and whether material detriment to the other clients or the lawyer would result.

Consent to Future Conflict

[22] Whether a lawyer may properly request a client to waive conflicts that might arise in the future is subject to the test of paragraph (b). The effectiveness of such waivers is generally determined by the extent to which the client reasonably understands the material risks that the waiver entails. The more comprehensive the explanation of the types of future representations that might arise and the actual and reasonably foreseeable adverse consequences of those representations, the greater the likelihood that the client will have the requisite understanding. Thus, if the client agrees to consent to a particular type of conflict with which the client is already familiar, then the consent ordinarily will be effective with regard to that type of
conflict. If the consent is general and open-ended, then the consent ordinarily will be ineffective, because it is not reasonably likely that the client will have understood the material risks involved. On the other hand, if the client is an experienced user of the legal services involved and is reasonably informed regarding the risk that a conflict may arise, such consent is more likely to be effective, particularly if, e.g., the client is independently represented by other counsel in giving consent and the consent is limited to future conflicts unrelated to the subject of the representation. In any case, advance consent cannot be effective if the circumstances that materialize in the future are such as would make the conflict nonconsentable under paragraph (b).

**Conflicts in Litigation**

[23] Paragraph (b)(3) prohibits representation of opposing parties in the same litigation, regardless of the clients' consent. On the other hand, simultaneous representation of parties whose interests in litigation may conflict, such as coplaintiffs or codefendants, is governed by paragraph (a)(2). A conflict may exist by reason of substantial discrepancy in the parties' testimony, incompatibility in positions in relation to an opposing party or the fact that there are substantially different possibilities of settlement of the claims or liabilities in question. Such conflicts can arise in criminal cases as well as civil. The potential for conflict of interest in representing multiple defendants in a criminal case is so grave that ordinarily a lawyer should decline to represent more than one codefendant. On the other hand, common representation of persons having similar interests in civil litigation is proper if the requirements of paragraph (b) are met.

[24] Ordinarily a lawyer may take inconsistent legal positions in different tribunals at different times on behalf of different clients. The mere fact that advocating a legal position on behalf of one client might create precedent adverse to the interests of a client represented by the lawyer in an unrelated matter does not create a conflict of interest. A conflict of interest exists, however, if there is a significant risk that a lawyer's action on behalf of one client will materially limit the lawyer's effectiveness in representing another client in a different case; for example, when a decision favoring one client will create a precedent likely to seriously weaken a position taken on behalf of the other client. Factors relevant in determining whether the clients need to be advised of the risk include: where the cases are pending, whether the issue is substantive or procedural, the temporal relationship between the matters, the significance of the issue to the immediate and long-term interests of the clients involved and the clients' reasonable expectations in retaining the lawyer. If there is significant risk of material limitation, then absent informed consent of the affected clients, the lawyer must refuse one of the representations or withdraw from one or both matters.

[25] When a lawyer represents or seeks to represent a class of plaintiffs or defendants in a class-action lawsuit, unnamed members of the class are ordinarily not considered to be clients of the lawyer for purposes of applying paragraph (a)(1) of this Rule. Thus, the lawyer does not typically need to get the consent of such a person before representing a client suing the person in an unrelated matter. Similarly, a lawyer seeking to represent an opponent in a class action does not typically need the consent of an unnamed member of the class whom the lawyer represents in an unrelated matter.

**Nonlitigation Conflicts**

[26] Conflicts of interest under paragraphs (a)(1) and (a)(2) arise in contexts other than litigation. For a discussion of directly adverse conflicts in transactional matters, see Comment [7]. Relevant factors in determining whether there is significant potential for material limitation include the duration and intimacy of the lawyer's relationship with the client or clients involved, the functions being performed by the lawyer, the likelihood that disagreements will arise and the likely prejudice to the client from the conflict. The question is often one of proximity and degree. See Comment [8].

[27] For example, conflict questions may arise in estate planning and estate administration. A lawyer may be called upon to prepare wills for several family members, such as husband and wife, and, depending upon the circumstances, a conflict of interest may be present. In estate administration the identity of the client may be unclear under the law of a particular jurisdiction. Under one view, the client is the fiduciary; under another view the client is the estate or trust, including its beneficiaries. In order to comply with conflict of interest rules, the lawyer should make clear the lawyer's relationship to the parties involved.

[28] Whether a conflict is consentable depends on the circumstances. For example, a lawyer may not represent multiple parties to a negotiation whose interests are fundamentally antagonistic to each other, but common representation is permissible where the clients are generally aligned in interest even though there is some difference in interest among them. Thus, a lawyer may seek to establish or adjust a relationship between clients on an amicable and mutually advantageous basis; for example, in helping to organize a business in which two or more clients are entrepreneurs, working out the financial reorganization of an enterprise in which two or more clients have an interest or arranging a property distribution in settlement of an estate. The lawyer seeks to resolve potentially adverse interests by developing the parties' mutual interests. Otherwise, each party might have to obtain separate representation, with the possibility of incurring additional cost, complication or even litigation. Given these and other relevant factors, the clients may prefer that the lawyer act for all of them.
Special Considerations in Common Representation

[29] In considering whether to represent multiple clients in the same matter, a lawyer should be mindful that if the common representation fails because the potentially adverse interests cannot be reconciled, the result can be additional cost, embarrassment and recrimination. Ordinarily, the lawyer will be forced to withdraw from representing all of the clients if the common representation fails. In some situations, the risk of failure is so great that multiple representation is plainly impossible. For example, a lawyer cannot undertake common representation of clients where contentious litigation or negotiations between them are imminent or contemplated. Moreover, because the lawyer is required to be impartial between commonly represented clients, representation of multiple clients is improper when it is unlikely that impartiality can be maintained. Generally, if the relationship between the parties has already assumed antagonism, the possibility that the clients' interests can be adequately served by common representation is not very good. Other relevant factors are whether the lawyer subsequently will represent both parties on a continuing basis and whether the situation involves creating or terminating a relationship between the parties.

[30] A particularly important factor in determining the appropriateness of common representation is the effect on client-lawyer confidentiality and the attorney-client privilege. With regard to the attorney-client privilege, the prevailing rule is that, as between commonly represented clients, the privilege does not attach. Hence, it must be assumed that if litigation eventuates between the clients, the privilege will not protect any such communications, and the clients should be so advised.

[31] As to the duty of confidentiality, continued common representation will almost certainly be inadequate if one client asks the lawyer not to disclose to the other client information relevant to the common representation. This is so because the lawyer has an equal duty of loyalty to each client, and each client has the right to be informed of anything bearing on the representation that might affect that client's interests and the right to expect that the lawyer will use that information to that client's benefit. See Rule 1.4. The lawyer should, at the outset of the common representation and as part of the process of obtaining each client's informed consent, advise each client that information will be shared and that the lawyer will have to withdraw if one client decides that some matter material to the representation should be kept from the other. In limited circumstances, it may be appropriate for the lawyer to proceed with the representation when the clients have agreed, after being properly informed, that the lawyer will keep certain information confidential. For example, the lawyer may reasonably conclude that failure to disclose one client's trade secrets to another client will not adversely affect representation involving a joint venture between the clients and agree to keep that information confidential with the informed consent of both clients.

[32] When seeking to establish or adjust a relationship between clients, the lawyer should make clear that the lawyer's role is not that of partisanship normally expected in other circumstances and, thus, that the clients may be required to assume greater responsibility for decisions than when each client is separately represented. Any limitations on the scope of the representation made necessary as a result of the common representation should be fully explained to the clients at the outset of the representation. See Rule 1.2(c).

[33] Subject to the above limitations, each client in the common representation has the right to loyal and diligent representation and the protection of Rule 1.9 concerning the obligations to a former client. The client also has the right to discharge the lawyer as stated in Rule 1.16.

Organizational Clients

[34] A lawyer who represents a corporation or other organization does not, by virtue of that representation, necessarily represent any constituent or affiliated organization, such as a parent or subsidiary. See Rule 1.13(a). Thus, the lawyer for an organization is not barred from accepting representation adverse to an affiliate in an unrelated matter, unless the circumstances are such that the affiliate should also be considered a client of the lawyer, there is an understanding between the lawyer and the organizational client that the lawyer will avoid representation adverse to the client's affiliates, or the lawyer's obligations to either the organizational client or the new client are likely to limit materially the lawyer's representation of the other client.

[35] A lawyer for a corporation or other organization who is also a member of its board of directors should determine whether the responsibilities of the two roles may conflict. The lawyer may be called on to advise the corporation in matters involving actions of the directors. Consideration should be given to the frequency with which such situations may arise, the potential intensity of the conflict, the effect of the lawyer's resignation from the board and the possibility of the corporation's obtaining legal advice from another lawyer in such situations. If there is material risk that the dual role will compromise the lawyer's independence of professional judgment, the lawyer should not serve as a director or should cease to act as the corporation's lawyer when conflicts of interest arise. The lawyer should advise the other members of the board that in some circumstances matters discussed at board meetings while the lawyer is present in the capacity of director might not be protected by the attorney-client privilege and that conflict of interest considerations might require the lawyer's recusal as a director or might require the lawyer and the lawyer's firm to decline representation of the corporation in a matter.
Rule 1.8 Conflict Of Interest: Current Clients: Specific Rules

(a) A lawyer shall not enter into a business transaction with a client or knowingly acquire an ownership, possessory, security or other pecuniary interest adverse to a client unless:

(1) the transaction and terms on which the lawyer acquires the interest are fair and reasonable to the client and are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;

(2) the client is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel on the transaction; and

(3) the client gives informed consent, in a writing signed by the client, to the essential terms of the transaction and the lawyer's role in the transaction, including whether the lawyer is representing the client in the transaction.

(b) A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these Rules.

(c) A lawyer shall not solicit any substantial gift from a client, including a testamentary gift, or prepare on behalf of a client an instrument giving the lawyer or a person related to the lawyer any substantial gift unless the lawyer or other recipient of the gift is related to the client. For purposes of this paragraph, related persons include a spouse, child, grandchild, parent, grandparent or other relative or individual with whom the lawyer or the client maintains a close, familial relationship.

(d) Prior to the conclusion of representation of a client, a lawyer shall not make or negotiate an agreement giving the lawyer literary or media rights to a portrayal or account based in substantial part on information relating to the representation.

(e) A lawyer shall not provide financial assistance to a client in connection with pending or contemplated litigation, except that:

(1) a lawyer may advance court costs and expenses of litigation, the repayment of which may be contingent on the outcome of the matter; and

(2) a lawyer representing an indigent client may pay court costs and expenses of litigation on behalf of the client.

(f) A lawyer shall not accept compensation for representing a client from one other than the client unless:

(1) the client gives informed consent;

(2) there is no interference with the lawyer's independence of professional judgment or with the client-lawyer relationship; and

(3) information relating to representation of a client is protected as required by Rule 1.6.

(g) A lawyer who represents two or more clients shall not participate in making an aggregate settlement of the claims of or against the clients, or in a criminal case an aggregated agreement as to guilty or nolo contendere pleas, unless each client gives informed consent, in a writing signed by the client. The lawyer's disclosure shall include the existence and nature of all the claims or pleas involved and of the participation of each person in the settlement.

(h) A lawyer shall not:

(1) make an agreement prospectively limiting the lawyer's liability to a client for malpractice unless the client is independently represented in making the agreement; or

(2) settle a claim or potential claim for such liability with an unrepresented client or former client unless that person is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel in connection therewith.
(i) A lawyer shall not acquire a proprietary interest in the cause of action or subject matter of litigation the lawyer is conducting for a client, except that the lawyer may:

(1) acquire a lien authorized by law to secure the lawyer's fee or expenses; and

(2) contract with a client for a reasonable contingent fee in a civil case.

(j) A lawyer shall not have sexual relations with a client unless a consensual sexual relationship existed between them when the client-lawyer relationship commenced.

(k) While lawyers are associated in a firm, a prohibition in the foregoing paragraphs (a) through (i) that applies to any one of them shall apply to all of them.

Comment

Business Transactions Between Client and Lawyer

[1] A lawyer's legal skill and training, together with the relationship of trust and confidence between lawyer and client, create the possibility of overreaching when the lawyer participates in a business, property or financial transaction with a client, for example, a loan or sales transaction or a lawyer investment on behalf of a client. The requirements of paragraph (a) must be met even when the transaction is not closely related to the subject matter of the representation, as when a lawyer drafting a will for a client learns that the client needs money for unrelated expenses and offers to make a loan to the client. The Rule applies to lawyers engaged in the sale of goods or services related to the practice of law, for example, the sale of title insurance or investment services to existing clients of the lawyer's legal practice. See Rule 5.7. It also applies to lawyers purchasing property from estates they represent. It does not apply to ordinary fee arrangements between client and lawyer, which are governed by Rule 1.5, although its requirements must be met when the lawyer accepts an interest in the client's business or other nonmonetary property as payment of all or part of a fee. In addition, the Rule does not apply to standard commercial transactions between the lawyer and the client for products or services that the client generally markets to others, for example, banking or brokerage services, medical services, products manufactured or distributed by the client, and utilities' services. In such transactions, the lawyer has no advantage in dealing with the client, and the restrictions in paragraph (a) are unnecessary and impracticable.

[2] Paragraph (a)(1) requires that the transaction itself be fair to the client and that its essential terms be communicated to the client, in writing, in a manner that can be reasonably understood. Paragraph (a)(2) requires that the client also be advised, in writing, of the desirability of seeking the advice of independent legal counsel. It also requires that the client be given a reasonable opportunity to obtain such advice. Paragraph (a)(3) requires that the lawyer obtain the client's informed consent, in a writing signed by the client, both to the essential terms of the transaction and to the lawyer's role. When necessary, the lawyer should discuss both the material risks of the proposed transaction, including any risk presented by the lawyer's involvement, and the existence of reasonably available alternatives and should explain why the advice of independent legal counsel is desirable. See Rule 1.0(e) (definition of informed consent).

[3] The risk to a client is greatest when the client expects the lawyer to represent the client in the transaction itself or when the lawyer's financial interest otherwise poses a significant risk that the lawyer's representation of the client will be materially limited by the lawyer's financial interest in the transaction. Here the lawyer's role requires that the lawyer must comply, not only with the requirements of paragraph (a), but also with the requirements of Rule 1.7. Under that Rule, the lawyer must disclose the risks associated with the lawyer's dual role as both legal adviser and participant in the transaction, such as the risk that the lawyer will structure the transaction or give legal advice in a way that favors the lawyer's interests at the expense of the client. Moreover, the lawyer must obtain the client's informed consent. In some cases, the lawyer's interest may be such that Rule 1.7 will preclude the lawyer from seeking the client's consent to the transaction.

[4] If the client is independently represented in the transaction, paragraph (a)(2) of this Rule is inapplicable, and the paragraph (a)(1) requirement for full disclosure is satisfied either by a written disclosure by the lawyer involved in the transaction or by the client's independent counsel. The fact that the client was independently represented in the transaction is relevant in determining whether the agreement was fair and reasonable to the client as paragraph (a)(1) further requires.

Use of Information Related to Representation

[5] Use of information relating to the representation to the disadvantage of the client violates the lawyer's duty of loyalty. Paragraph (b) applies when the information is used to benefit either the lawyer or a third person, such as another client or business associate of the lawyer. For example, if a lawyer learns that a client intends to purchase and develop several parcels of
land, the lawyer may not use that information to purchase one of the parcels in competition with the client or to recommend that another client make such a purchase. The Rule does not prohibit uses that do not disadvantage the client. For example, a lawyer who learns a government agency's interpretation of trade legislation during the representation of one client may properly use that information to benefit other clients. Paragraph (b) prohibits disadvantageous use of client information unless the client gives informed consent, except as permitted or required by these Rules. See Rules 1.2(d), 1.6, 1.9(c), 3.3, 4.1(b), 8.1 and 8.3.

Gifts to Lawyers

[6] A lawyer may accept a gift from a client, if the transaction meets general standards of fairness. For example, a simple gift such as a present given at a holiday or as a token of appreciation is permitted. If a client offers the lawyer a more substantial gift, paragraph (c) does not prohibit the lawyer from accepting it, although such a gift may be voidable by the client under the doctrine of undue influence, which treats client gifts as presumptively fraudulent. In any event, due to concerns about overreaching and imposition on clients, a lawyer may not suggest that a substantial gift be made to the lawyer or for the lawyer's benefit, except where the lawyer is related to the client as set forth in paragraph (c).

[7] If effectuation of a substantial gift requires preparing a legal instrument such as a will or conveyance the client should have the detached advice that another lawyer can provide. The sole exception to this Rule is where the client is a relative of the donee.

[8] This Rule does not prohibit a lawyer from seeking to have the lawyer or a partner or associate of the lawyer named as executor of the client's estate or to another potentially lucrative fiduciary position. Nevertheless, such appointments will be subject to the general conflict of interest provision in Rule 1.7 when there is a significant risk that the lawyer's interest in obtaining the appointment will materially limit the lawyer's independent professional judgment in advising the client concerning the choice of an executor or other fiduciary. In obtaining the client's informed consent to the conflict, the lawyer should advise the client concerning the nature and extent of the lawyer's financial interest in the appointment, as well as the availability of alternative candidates for the position.

Literary Rights

[9] An agreement by which a lawyer acquires literary or media rights concerning the conduct of the representation creates a conflict between the interests of the client and the personal interests of the lawyer. Measures suitable in the representation of the client may detract from the publication value of an account of the representation. Paragraph (d) does not prohibit a lawyer representing a client in a transaction concerning literary property from agreeing that the lawyer's fee shall consist of a share in ownership in the property, if the arrangement conforms to Rule 1.5 and paragraphs (a) and (i).

Financial Assistance

[10] Lawyers may not subsidize lawsuits or administrative proceedings brought on behalf of their clients, including making or guaranteeing loans to their clients for living expenses, because to do so would encourage clients to pursue lawsuits that might not otherwise be brought and because such assistance gives lawyers too great a financial stake in the litigation. These dangers do not warrant a prohibition on a lawyer lending a client court costs and litigation expenses, including the expenses of medical examination and the costs of obtaining and presenting evidence, because these advances are virtually indistinguishable from contingent fees and help ensure access to the courts. Similarly, an exception allowing lawyers representing indigent clients to pay court costs and litigation expenses regardless of whether these funds will be repaid is warranted.

Person Paying for a Lawyer's Services

[11] Lawyers are frequently asked to represent a client under circumstances in which a third person will compensate the lawyer, in whole or in part. The third person might be a relative or friend, an indemnitor (such as a liability insurance company) or a co-client (such as a corporation sued along with one or more of its employees). Because third-party payers frequently have interests that differ from those of the client, including interests in minimizing the amount spent on the representation and in learning how the representation is progressing, lawyers are prohibited from accepting or continuing such representations unless the lawyer determines that there will be no interference with the lawyer's independent professional judgment and there is informed consent from the client. See also Rule 5.4(c) (prohibiting interference with a lawyer's professional judgment by one who recommends, employs or pays the lawyer to render legal services for another).

[12] Sometimes, it will be sufficient for the lawyer to obtain the client's informed consent regarding the fact of the payment and the identity of the third-party payer. If, however, the fee arrangement creates a conflict of interest for the lawyer, then the lawyer must comply with Rule 1.7. The lawyer must also conform to the requirements of Rule 1.6 concerning confidentiality. Under Rule 1.7(a), a conflict of interest exists if there is significant risk that the lawyer's representation of the
client will be materially limited by the lawyer's own interest in the fee arrangement or by the lawyer's responsibilities to the third-party payer (for example, when the third-party payer is a co-client). Under Rule 1.7(b), the lawyer may accept or continue the representation with the informed consent of each affected client, unless the conflict is nonconsentable under that paragraph. Under Rule 1.7(b), the informed consent must be confirmed in writing.

**Aggregate Settlements**

[13] Differences in willingness to make or accept an offer of settlement are among the risks of common representation of multiple clients by a single lawyer. Under Rule 1.7, this is one of the risks that should be discussed before undertaking the representation, as part of the process of obtaining the clients' informed consent. In addition, Rule 1.2(a) protects each client's right to have the final say in deciding whether to accept or reject an offer of settlement and in deciding whether to enter a guilty or nolo contendere plea in a criminal case. The rule stated in this paragraph is a corollary of both these Rules and provides that, before any settlement offer or plea bargain is made or accepted on behalf of multiple clients, the lawyer must inform each of them about all the material terms of the settlement, including what the other clients will receive or pay if the settlement or plea offer is accepted. See also Rule 1.0(c) (definition of informed consent). Lawyers representing a class of plaintiffs or defendants, or those proceeding derivatively, may not have a full client-lawyer relationship with each member of the class; nevertheless, such lawyers must comply with applicable rules regulating notification of class members and other procedural requirements designed to ensure adequate protection of the entire class.

**Limiting Liability and Settling Malpractice Claims**

[14] Agreements prospectively limiting a lawyer's liability for malpractice are prohibited unless the client is independently represented in making the agreement because they are likely to undermine competent and diligent representation. Also, many clients are unable to evaluate the desirability of making such an agreement before a dispute has arisen, particularly if they are then represented by the lawyer seeking the agreement. This paragraph does not, however, prohibit a lawyer from entering into an agreement with the client to arbitrate legal malpractice claims, provided such agreements are enforceable and the client is fully informed of the scope and effect of the agreement. Nor does this paragraph limit the ability of lawyers to practice in the form of a limited-liability entity, where permitted by law, provided that each lawyer remains personally liable to the client for his or her own conduct and the firm complies with any conditions required by law, such as provisions requiring client notification or maintenance of adequate liability insurance. Nor does it prohibit an agreement in accordance with Rule 1.2 that defines the scope of the representation, although a definition of scope that makes the obligations of representation illusory will amount to an attempt to limit liability.

[15] Agreements settling a claim or a potential claim for malpractice are not prohibited by this Rule. Nevertheless, in view of the danger that a lawyer will take unfair advantage of an unrepresented client or former client, the lawyer must first advise such a person in writing of the appropriateness of independent representation in connection with such a settlement. In addition, the lawyer must give the client or former client a reasonable opportunity to find and consult independent counsel.

**Acquiring Proprietary Interest in Litigation**

[16] Paragraph (i) states the traditional general rule that lawyers are prohibited from acquiring a proprietary interest in litigation. Like paragraph (e), the general rule has its basis in common law chomperty and maintenance and is designed to avoid giving the lawyer too great an interest in the representation. In addition, when the lawyer acquires an ownership interest in the subject of the representation, it will be more difficult for a client to discharge the lawyer if the client so desires. The Rule is subject to specific exceptions developed in decisional law and continued in these Rules. The exception for certain advances of the costs of litigation is set forth in paragraph (e). In addition, paragraph (i) sets forth exceptions for liens authorized by law to secure the lawyer's fees or expenses and contracts for reasonable contingent fees. The law of each jurisdiction determines which liens are authorized by law. These may include liens granted by statute, liens originating in common law and liens acquired by contract with the client. When a lawyer acquires by contract a security interest in property other than that recovered through the lawyer's efforts in the litigation, such an acquisition is a business or financial transaction with a client and is governed by the requirements of paragraph (a). Contracts for contingent fees in civil cases are governed by Rule 1.5.

**Client-Lawyer Sexual Relationships**

[17] The relationship between lawyer and client is a fiduciary one in which the lawyer occupies the highest position of trust and confidence. The relationship is almost always unequal; thus, a sexual relationship between lawyer and client can involve unfair exploitation of the lawyer's fiduciary role, in violation of the lawyer's basic ethical obligation not to use the trust of the client to the client's disadvantage. In addition, such a relationship presents a significant danger that, because of the lawyer's emotional involvement, the lawyer will be unable to represent the client without impairment of the exercise of independent professional judgment. Moreover, a blurred line between the professional and personal relationships may make it difficult to predict to what extent client confidences will be protected by the attorney-client evidentiary privilege, since client confidences
are protected by privilege only when they are imparted in the context of the client-lawyer relationship. Because of the significant danger of harm to client interests and because the client's own emotional involvement renders it unlikely that the client could give adequate informed consent, this Rule prohibits the lawyer from having sexual relations with a client regardless of whether the relationship is consensual and regardless of the absence of prejudice to the client.

[18] Sexual relationships that predate the client-lawyer relationship are not prohibited. Issues relating to the exploitation of the fiduciary relationship and client dependency are diminished when the sexual relationship existed prior to the commencement of the client-lawyer relationship. However, before proceeding with the representation in these circumstances, the lawyer should consider whether the lawyer's ability to represent the client will be materially limited by the relationship. See Rule 1.7(a)(2).

[19] When the client is an organization, paragraph (j) of this Rule prohibits a lawyer for the organization (whether inside counsel or outside counsel) from having a sexual relationship with a constituent of the organization who supervises, directs or regularly consults with that lawyer concerning the organization's legal matters.

Imputation of Prohibitions

[20] Under paragraph (k), a prohibition on conduct by an individual lawyer in paragraphs (a) through (i) also applies to all lawyers associated in a firm with the personally prohibited lawyer. For example, one lawyer in a firm may not enter into a business transaction with a client of another member of the firm without complying with paragraph (a), even if the first lawyer is not personally involved in the representation of the client. The prohibition set forth in paragraph (j) is personal and is not applied to associated lawyers.

Rule 1.9 Duties To Former Clients

(a) A lawyer who has formerly represented a client in a matter shall not thereafter represent another person in the same or a substantially related matter in which that person's interests are materially adverse to the interests of the former client unless the former client gives informed consent, confirmed in writing.

(b) A lawyer shall not knowingly represent a person in the same or a substantially related matter in which a firm with which the lawyer formerly was associated had previously represented a client

(1) whose interests are materially adverse to that person; and

(2) about whom the lawyer had acquired information protected by Rules 1.6 and 1.9(c) that is material to the matter; unless the former client gives informed consent, confirmed in writing.

(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter:

(1) use information relating to the representation to the disadvantage of the former client except as these Rules would permit or require with respect to a client, or when the information has become generally known; or

(2) reveal information relating to the representation except as these Rules would permit or require with respect to a client.

Comment

[1] After termination of a client-lawyer relationship, a lawyer has certain continuing duties with respect to confidentiality and conflicts of interest and thus may not represent another client except in conformity with this Rule. Under this Rule, for example, a lawyer could not properly seek to rescind on behalf of a new client a contract drafted on behalf of the former client. So also a lawyer who has prosecuted an accused person could not properly represent the accused in a subsequent civil action against the government concerning the same transaction. Nor could a lawyer who has represented multiple clients in a matter represent one of the clients against the others in the same or a substantially related matter after a dispute arose among the clients in that matter, unless all affected clients give informed consent. See Comment [9]. Current and former government lawyers must comply with this Rule to the extent required by Rule 1.11.

[2] The scope of a "matter" for purposes of this Rule depends on the facts of a particular situation or transaction. The lawyer's involvement in a matter can also be a question of degree. When a lawyer has been directly involved in a specific
transaction, subsequent representation of other clients with materially adverse interests in that transaction clearly is prohibited. On the other hand, a lawyer who recurrently handled a type of problem for a former client is not precluded from later representing another client in a factually distinct problem of that type even though the subsequent representation involves a position adverse to the prior client. Similar considerations can apply to the reassignment of military lawyers between defense and prosecution functions within the same military jurisdictions. The underlying question is whether the lawyer was so involved in the matter that the subsequent representation can be justly regarded as a changing of sides in the matter in question.

[3] Matters are "substantially related" for purposes of this Rule if they involve the same transaction or legal dispute or if there otherwise is a substantial risk that confidential factual information as would normally have been obtained in the prior representation would materially advance the client's position in the subsequent matter. For example, a lawyer who has represented a businessperson and learned extensive private financial information about that person may not then represent that person's spouse in seeking a divorce. Similarly, a lawyer who has previously represented a client in securing environmental permits to build a shopping center would be precluded from representing neighbors seeking to oppose rezoning of the property on the basis of environmental considerations; however, the lawyer would not be precluded, on the grounds of substantial relationship, from defending a tenant of the completed shopping center in resisting eviction for nonpayment of rent. Information that has been disclosed to the public or to other parties adverse to the former client ordinarily will not be disqualifying. Information acquired in a prior representation may have been rendered obsolete by the passage of time, a circumstance that may be relevant in determining whether two representations are substantially related. In the case of an organizational client, general knowledge of the client's policies and practices ordinarily will not preclude a subsequent representation; on the other hand, knowledge of specific facts gained in a prior representation that are relevant to the matter in question ordinarily will preclude such a representation. A former client is not required to reveal the confidential information learned by the lawyer in order to establish a substantial risk that the lawyer has confidential information to use in the subsequent matter. A conclusion about the possession of such information may be based on the nature of the services the lawyer provided the former client and information that would in ordinary practice be learned by a lawyer providing such services.

Lawyers Moving Between Firms

[4] When lawyers have been associated within a firm but then end their association, the question of whether a lawyer should undertake representation is more complicated. There are several competing considerations. First, the client previously represented by the former firm must be reasonably assured that the principle of loyalty to the client is not compromised. Second, the rule should not be so broadly cast as to preclude other persons from having reasonable choice of legal counsel. Third, the rule should not unreasonably hamper lawyers from forming new associations and taking on new clients after having left a previous association. In this connection, it should be recognized that today many lawyers practice in firms; that many lawyers to some degree limit their practice to one field or another, and that many move from one association to another several times in their careers. If the concept of imputation were applied with unqualified rigor, the result would be radical curtailment of the opportunity of lawyers to move from one practice setting to another and of the opportunity of clients to change counsel.

[5] Paragraph (b) operates to disqualify the lawyer only when the lawyer involved has actual knowledge of information protected by Rules 1.6 and 1.9(c). Thus, if a lawyer while with one firm acquired no knowledge or information relating to a particular client of the firm, and that lawyer later joined another firm, neither the lawyer individually nor the second firm is disqualified from representing another client in the same or a related matter even though the interests of the two clients conflict. See Rule 1.10(b) for the restrictions on a firm once a lawyer has terminated association with the firm.

[6] Application of paragraph (b) depends on a situation's particular facts, aided by inferences, deductions or working presumptions that reasonably may be made about the way in which lawyers work together. A lawyer may have general access to files of all clients of a law firm and may regularly participate in discussions of their affairs; it should be inferred that such a lawyer in fact is privy to all information about all the firm's clients. In contrast, another lawyer may have access to the files of only a limited number of clients and participate in discussions of the affairs of no other clients; in the absence of information to the contrary, it should be inferred that such a lawyer in fact is privy to information about the clients actually served but not those of other clients. In such an inquiry, the burden of proof should rest upon the firm whose disqualification is sought.

[7] Independent of the question of disqualification of a firm, a lawyer changing professional association has a continuing duty to preserve confidentiality of information about a client formerly represented. See Rules 1.6 and 1.9(c).

[8] Paragraph (c) provides that information acquired by the lawyer in the course of representing a client may not subsequently be used or revealed by the lawyer to the disadvantage of the client. However, the fact that a lawyer has once served a client does not preclude the lawyer from using generally known information about that client when later representing another client.

[9] The provisions of this Rule are for the protection of former clients and can be waived if the client gives informed consent, which consent must be confirmed in writing under paragraphs (a) and (b). See Rule 1.0(c). With regard to the
effectiveness of an advance waiver, see Comment [22] to Rule 1.7. With regard to disqualification of a firm with which a lawyer is or was formerly associated, see Rule 1.10.

Rule 1.10 Imputation Of Conflicts Of Interest:

General Rule

(a) While lawyers are associated in a firm, none of them shall knowingly represent a client when any one of them practicing alone would be prohibited from doing so by Rules 1.7 or 1.9, unless

(1) the prohibition is based on a personal interest of the disqualified lawyer and does not present a significant risk of materially limiting the representation of the client by the remaining lawyers in the firm; or

(2) the prohibition is based upon Rule 1.9(a) or (b) and arises out of the disqualified lawyer’s association with a prior firm, and

(i) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom;

(ii) written notice is promptly given to any affected former client to enable the former client to ascertain compliance with the provisions of this Rule, which shall include a description of the screening procedures employed; a statement of the firm’s and of the screened lawyer’s compliance with these Rules; a statement that review may be available before a tribunal; and an agreement by the firm to respond promptly to any written inquiries or objections by the former client about the screening procedures; and

(iii) certifications of compliance with these Rules and with the screening procedures are provided to the former client by the screened lawyer and by a partner of the firm, at reasonable intervals upon the former client's written request and upon termination of the screening procedures.

(b) When a lawyer has terminated an association with a firm, the firm is not prohibited from thereafter representing a person with interests materially adverse to those of a client represented by the formerly associated lawyer and not currently represented by the firm, unless:

(1) the matter is the same or substantially related to that in which the formerly associated lawyer represented the client; and

(2) any lawyer remaining in the firm has information protected by Rules 1.6 and 1.9(c) that is material to the matter.

(c) A disqualification prescribed by this rule may be waived by the affected client under the conditions stated in Rule 1.7.

(d) The disqualification of lawyers associated in a firm with former or current government lawyers is governed by Rule 1.11.

Comment

Definition of “Firm”

[1] For purposes of the Rules of Professional Conduct, the term “firm” denotes lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization. See Rule 1.0(c). Whether two or more lawyers constitute a firm within this definition can depend upon the specific facts. See Rule 1.10, Comments [2] - [4].

Principles of Imputed Disqualification

[2] The rule of imputed disqualification stated in paragraph (a) gives effect to the principle of loyalty to the client as it applies to lawyers who practice in a law firm. Such situations can be considered from the premise that a firm of lawyers is
essentially one lawyer for purposes of the rules governing loyalty to the client, or from the premise that each lawyer is vicariously bound by the obligation of loyalty owed by each lawyer with whom the lawyer is associated. Paragraph (a)(1) operates only among the lawyers currently associated in a firm. When a lawyer moves from one firm to another, the situation is governed by Rules 1.9(b) and 1.10(a)(2) and 1.10 (b).

[3] The rule in paragraph (a) does not prohibit representation whether neither questions of client loyalty nor protection of confidential information are presented. Where one lawyer in a firm could not effectively represent a given client because of strong political beliefs, for example, but that lawyer will do no work on the case and the personal beliefs of the lawyer will not materially limit the representation by others in the firm, the firm should not be disqualified. On the other hand, if an opposing party in a case were owned by a lawyer in the law firm, and others in the firm would be materially limited in pursuing the matter because of loyalty to that lawyer, the personal disqualification of the lawyer would be imputed to all others in the firm.

[4] The rule in paragraph (a) also does not prohibit representation by others in the law firm where the person prohibited from involvement in a matter is a nonlawyer, such as a paralegal or legal secretary. Nor does paragraph (a) prohibit representation if the lawyer is prohibited from acting because of events before the person became a lawyer, for example, work that the person did as a law student. Such persons, however, ordinarily must be screened from any personal participation in the matter to avoid communication to others in the firm of confidential information that both the nonlawyers and the firm have a legal duty to protect. See Rules 1.0(k) and 5.3.

[5] Rule 1.10(b) operates to permit a law firm, under certain circumstances, to represent a person with interests directly adverse to those of a client represented by a lawyer who formerly was associated with the firm. The Rule applies regardless of when the formerly associated lawyer represented the client. However, the law firm may not represent a person with interests adverse to those of a present client of the firm, which would violate Rule 1.7. Moreover, the firm may not represent the person where the matter is the same or substantially related to that in which the formerly associated lawyer represented the client and any other lawyer currently in the firm has material information protected by Rules 1.6 and 1.9(c).

[6] Rule 1.10(c) removes imputation with the informed consent of the affected client or former client under the conditions stated in Rule 1.7. The conditions stated in Rule 1.7 require the lawyer to determine that the representation is not prohibited by Rule 1.7(b) and that each affected client or former client has given informed consent to the representation, confirmed in writing. In some cases, the risk may be so severe that the conflict may not be cured by client consent. For a discussion of the effectiveness of client waivers of conflicts that might arise in the future, see Rule 1.7, Comment [22]. For a definition of informed consent, see Rule 1.0(e).

[7] Rule 1.10(a)(2) similarly removes the imputation otherwise required by Rule 1.10(a), but unlike section (c), it does so without requiring that there be informed consent by the former client. Instead, it requires that the procedures laid out in sections (a)(2)(i)-(iii) be followed. A description of effective screening mechanisms appears in Rule 1.0(k). Lawyers should be aware, however, that, even where screening mechanisms have been adopted, tribunals may consider additional factors in ruling upon motions to disqualify a lawyer from pending litigation.

[8] Paragraph (a)(2)(i) does not prohibit the screened lawyer from receiving a salary or partnership share established by prior independent agreement, but that lawyer may not receive compensation directly related to the matter in which the lawyer is disqualified.

[9] The notice required by paragraph (a)(2)(ii) generally should include a description of the screened lawyer’s prior representation and be given as soon as practicable after the need for screening becomes apparent. It also should include a statement by the screened lawyer and the firm that the client’s material confidential information has not been disclosed or used in violation of the Rules. The notice is intended to enable the former client to evaluate and comment upon the effectiveness of the screening procedures.

[10] The certifications required by paragraph (a)(2)(iii) give the former client assurance that the client’s material confidential information has not been disclosed or used inappropriately, either prior to timely implementation of a screen or thereafter. If compliance cannot be certified, the certificate must describe the failure to comply.

[11] Where a lawyer has joined a private firm after having represented the government, imputation is governed under Rule 1.11(b) and (c), not this Rule. Under Rule 1.11(d), where a lawyer represents the government after having served clients in private practice, nongovernmental employment or in another government agency, former client conflicts are not imputed to government lawyers associated with the individually disqualified lawyer.

[12] Where a lawyer is prohibited from engaging in certain transactions under Rule 1.8, paragraph (k) of that Rule, and not this Rule, determines whether that prohibition also applies to other lawyers associated in a firm with the personally prohibited lawyer.
Rule 1.11 Special Conflicts Of Interest For Former And Current Government Officers And Employees

(a) Except as law may otherwise expressly permit, a lawyer who has formerly served as a public officer or employee of the government:

(1) is subject to Rule 1.9(c); and

(2) shall not otherwise represent a client in connection with a matter in which the lawyer participated personally and substantially as a public officer or employee, unless the appropriate government agency gives its informed consent, confirmed in writing, to the representation.

(b) When a lawyer is disqualified from representation under paragraph (a), no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter unless:

(1) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and

(2) written notice is promptly given to the appropriate government agency to enable it to ascertain compliance with the provisions of this rule.

(c) Except as law may otherwise expressly permit, a lawyer having information that the lawyer knows is confidential government information about a person acquired when the lawyer was a public officer or employee, may not represent a private client whose interests are adverse to that person in a matter in which the information could be used to the material disadvantage of that person. As used in this Rule, the term "confidential government information" means information that has been obtained under governmental authority and which, at the time this Rule is applied, the government is prohibited by law from disclosing to the public or has a legal privilege not to disclose and which is not otherwise available to the public. A firm with which that lawyer is associated may undertake or continue representation in the matter only if the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom.

(d) Except as law may otherwise expressly permit, a lawyer currently serving as a public officer or employee:

(1) is subject to Rules 1.7 and 1.9; and

(2) shall not:

(i) participate in a matter in which the lawyer participated personally and substantially while in private practice or nongovernmental employment, unless the appropriate government agency gives its informed consent, confirmed in writing; or

(ii) negotiate for private employment with any person who is involved as a party or as lawyer for a party in a matter in which the lawyer is participating personally and substantially, except that a lawyer serving as a law clerk to a judge, other adjudicative officer or arbitrator may negotiate for private employment as permitted by Rule 1.12(b) and subject to the conditions stated in Rule 1.12(b).

(e) As used in this Rule, the term "matter" includes:

(1) any judicial or other proceeding, application, request for a ruling or other determination, contract, claim, controversy, investigation, charge, accusation, arrest or other particular matter involving a specific party or parties, and

(2) any other matter covered by the conflict of interest rules of the appropriate government agency.

Comment

[1] A lawyer who has served or is currently serving as a public officer or employee is personally subject to the Rules of Professional Conduct, including the prohibition against concurrent conflicts of interest stated in Rule 1.7. In addition, such a
lawyer may be subject to statutes and government regulations regarding conflict of interest. Such statutes and regulations may circumscribe the extent to which the government agency may give consent under this Rule. See Rule 1.0(e) for the definition of informed consent.

[2] Paragraphs (a)(1), (a)(2) and (d)(1) restate the obligations of an individual lawyer who has served or is currently serving as an officer or employee of the government toward a former government or private client. Rule 1.10 is not applicable to the conflicts of interest addressed by this Rule. Rather, paragraph (b) sets forth a special imputation rule for former government lawyers that provides for screening and notice. Because of the special problems raised by imputation within a government agency, paragraph (d) does not impute the conflicts of a lawyer currently serving as an officer or employee of the government to other associated government officers or employees, although ordinarily it will be prudent to screen such lawyers.

[3] Paragraphs (a)(2) and (d)(2) apply regardless of whether a lawyer is adverse to a former client and are thus designed not only to protect the former client, but also to prevent a lawyer from exploiting public office for the advantage of another client. For example, a lawyer who has pursued a claim on behalf of the government may not pursue the same claim on behalf of a later private client after the lawyer has left government service, except when authorized to do so by the government agency under paragraph (a). Similarly, a lawyer who has pursued a claim on behalf of a private client may not pursue the claim on behalf of the government, except when authorized to do so by paragraph (d). As with paragraphs (a)(1) and (d)(1), Rule 1.10 is not applicable to the conflicts of interest addressed by these paragraphs.

[4] This Rule represents a balancing of interests. On the one hand, where the successive clients are a government agency and another client, public or private, the risk exists that power or discretion vested in that agency might be used for the special benefit of the other client. A lawyer should not be in a position where benefit to the other client might affect performance of the lawyer's professional functions on behalf of the government. Also, unfair advantage could accrue to the other client by reason of access to confidential government information about the client's adversary obtainable only through the lawyer's government service. On the other hand, the rules governing lawyers presently or formerly employed by a government agency should not be so restrictive as to inhibit transfer of employment to and from the government. The government has a legitimate need to attract qualified lawyers as well as to maintain high ethical standards. Thus a former government lawyer is disqualified only from particular matters in which the lawyer participated personally and substantially. The provisions for screening and waiver in paragraph (b) are necessary to prevent the disqualification rule from imposing too severe a deterrent against entering public service. The limitation of disqualification in paragraphs (a)(2) and (d)(2) to matters involving a specific party or parties, rather than extending disqualification to all substantive issues on which the lawyer worked, serves a similar function.

[5] When a lawyer has been employed by one government agency and then moves to a second government agency, it may be appropriate to treat that second agency as another client for purposes of this Rule, as when a lawyer is employed by a city and subsequently is employed by a federal agency. However, because the conflict of interest is governed by paragraph (d), the latter agency is not required to screen the lawyer as paragraph (b) requires a law firm to do. The question of whether two government agencies should be regarded as the same or different clients for conflict of interest purposes is beyond the scope of these Rules. See Rule 1.13 Commentary [9].

[6] Paragraphs (b) and (c) contemplate a screening arrangement. See Rule 1.0(k) (requirements for screening procedures). These paragraphs do not prohibit a lawyer from receiving a salary or partnership share established by prior independent agreement, but that lawyer may not receive compensation directly relating the lawyer's compensation to the fee in the matter in which the lawyer is disqualified.

[7] Notice, including a description of the screened lawyer's prior representation and of the screening procedures employed, generally should be given as soon as practicable after the need for screening becomes apparent.

[8] Paragraph (c) operates only when the lawyer in question has knowledge of the information, which means actual knowledge; it does not operate with respect to information that merely could be imputed to the lawyer.

[9] Paragraphs (a) and (d) do not prohibit a lawyer from jointly representing a private party and a government agency when doing so is permitted by Rule 1.7 and is not otherwise prohibited by law.

[10] For purposes of paragraph (e) of this Rule, a "matter" may continue in another form. In determining whether two particular matters are the same, the lawyer should consider the extent to which the matters involve the same basic facts, the same or related parties, and the time elapsed.

**Rule 1.12 Former Judge, Arbitrator, Mediator Or Other Third-Party Neutral**
(a) Except as stated in paragraph (d), a lawyer shall not represent anyone in connection with a matter in which the lawyer participated personally and substantially as a judge or other adjudicative officer or law clerk to such a person or as an arbitrator, mediator or other third-party neutral, unless all parties to the proceeding give informed consent, confirmed in writing.

(b) A lawyer shall not negotiate for employment with any person who is involved as a party or as lawyer for a party in a matter in which the lawyer is participating personally and substantially as a judge or other adjudicative officer or as an arbitrator, mediator or other third-party neutral. A lawyer serving as a law clerk to a judge or other adjudicative officer may negotiate for employment with a party or lawyer involved in a matter in which the clerk is participating personally and substantially, but only after the lawyer has notified the judge or other adjudicative officer.

(c) If a lawyer is disqualified by paragraph (a), no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in the matter unless:

(1) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and

(2) written notice is promptly given to the parties and any appropriate tribunal to enable them to ascertain compliance with the provisions of this rule.

(d) An arbitrator selected as a partisan of a party in a multimember arbitration panel is not prohibited from subsequently representing that party.

Comment

[1] This Rule generally parallels Rule 1.11. The term "personally and substantially" signifies that a judge who was a member of a multimember court, and thereafter left judicial office to practice law, is not prohibited from representing a client in a matter pending in the court, but in which the former judge did not participate. So also the fact that a former judge exercised administrative responsibility in a court does not prevent the former judge from acting as a lawyer in a matter where the judge had previously exercised remote or incidental administrative responsibility that did not affect the merits. Compare the Comment to Rule 1.11. The term "adjudicative officer" includes such officials as judges pro tempore, referees, special masters, hearing officers and other parajudicial officers, and also lawyers who serve as part-time judges. Compliance Canons A(2), B(2) and C of the Model Code of Judicial Conduct provide that a part-time judge, judge pro tempore or retired judge recalled to active service, may not "act as a lawyer in any proceeding in which he served as a judge or in any other proceeding related thereto." Although phrased differently from this Rule, those Rules correspond in meaning.

[2] Like former judges, lawyers who have served as arbitrators, mediators or other third-party neutrals may be asked to represent a client in a matter in which the lawyer participated personally and substantially. This Rule forbids such representation unless all of the parties to the proceedings give their informed consent, confirmed in writing. See Rule 1.0(e) and (b). Other law or codes of ethics governing third-party neutrals may impose more stringent standards of personal or imputed disqualification. See Rule 2.4.

[3] Although lawyers who serve as third-party neutrals do not have information concerning the parties that is protected under Rule 1.6, they typically owe the parties an obligation of confidentiality under law or codes of ethics governing third-party neutrals. Thus, paragraph (c) provides that conflicts of the personally disqualified lawyer will be imputed to other lawyers in a law firm unless the conditions of this paragraph are met.

[4] Requirements for screening procedures are stated in Rule 1.0(k). Paragraph (c)(1) does not prohibit the screened lawyer from receiving a salary or partnership share established by prior independent agreement, but that lawyer may not receive compensation directly related to the matter in which the lawyer is disqualified.

[5] Notice, including a description of the screened lawyer's prior representation and of the screening procedures employed, generally should be given as soon as practicable after the need for screening becomes apparent.

Rule 1.13 Organization As Client

(a) A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.
(b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances to the highest authority that can act on behalf of the organization as determined by applicable law.

(c) Except as provided in paragraph (d), if

(1) despite the lawyer's efforts in accordance with paragraph (b) the highest authority that can act on behalf of the organization insists upon or fails to address in a timely and appropriate manner an action, or a refusal to act, that is clearly a violation of law, and

(2) the lawyer reasonably believes that the violation is reasonably certain to result in substantial injury to the organization,

then the lawyer may reveal information relating to the representation whether or not Rule 1.6 permits such disclosure, but only if and to the extent the lawyer reasonably believes necessary to prevent substantial injury to the organization.

(d) Paragraph (c) shall not apply with respect to information relating to a lawyer's representation of an organization to investigate an alleged violation of law, or to defend the organization or an officer, employee or other constituent associated with the organization against a claim arising out of an alleged violation of law.

(e) A lawyer who reasonably believes that he or she has been discharged because of the lawyer's actions taken pursuant to paragraphs (b) or (c), or who withdraws under circumstances that require or permit the lawyer to take action under either of those paragraphs, shall proceed as the lawyer reasonably believes necessary to assure that the organization's highest authority is informed of the lawyer's discharge or withdrawal.

(f) In dealing with an organization's directors, officers, employees, members, shareholders or other constituents, a lawyer shall explain the identity of the client when the lawyer knows or reasonably should know that the organization's interests are adverse to those of the constituents with whom the lawyer is dealing.

(g) A lawyer representing an organization may also represent any of its directors, officers, employees, members, shareholders or other constituents, subject to the provisions of Rule 1.7. If the organization's consent to the dual representation is required by Rule 1.7, the consent shall be given by an appropriate official of the organization other than the individual who is to be represented, or by the shareholders.

Comment

The Entity as the Client

[1] An organizational client is a legal entity, but it cannot act except through its officers, directors, employees, shareholders and other constituents. Officers, directors, employees and shareholders are the constituents of the corporate organizational client. The duties defined in this Comment apply equally to unincorporated associations. "Other constituents" as used in this Comment means the positions equivalent to officers, directors, employees and shareholders held by persons acting for organizational clients that are not corporations.

[2] When one of the constituents of an organizational client communicates with the organization's lawyer in that person's organizational capacity, the communication is protected by Rule 1.6. Thus, by way of example, if an organizational client requests its lawyer to investigate allegations of wrongdoing, interviews made in the course of that investigation between the lawyer and the client's employees or other constituents are covered by Rule 1.6. This does not mean, however, that constituents of an organizational client are the clients of the lawyer. The lawyer may not disclose to such constituents information relating to the representation except for disclosures explicitly or impliedly authorized by the organizational client in order to carry out the representation or as otherwise permitted by Rule 1.6.

[3] When constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province. Paragraph (b) makes clear, however, that when the lawyer knows that the organization is
likely to be substantially injured by action of an officer or other constituent that violates a legal obligation to the organization or is in violation of law that might be imputed to the organization, the lawyer must proceed as is reasonably necessary in the best interest of the organization. As defined in Rule 1.0(f), knowledge can be inferred from circumstances, and a lawyer cannot ignore the obvious.

[4] In determining how to proceed under paragraph (b), the lawyer should give due consideration to the seriousness of the violation and its consequences, the responsibility in the organization and the apparent motivation of the person involved, the policies of the organization concerning such matters, and any other relevant considerations. Ordinarily, referral to a higher authority would be necessary. In some circumstances, however, it may be appropriate for the lawyer to ask the constituent to reconsider the matter; for example, if the circumstances involve a constituent's innocent misunderstanding of law and subsequent acceptance of the lawyer's advice, the lawyer may reasonably conclude that the best interest of the organization does not require that the matter be referred to higher authority. If a constituent persists in conduct contrary to the lawyer's advice, it will be necessary for the lawyer to take steps to have the matter reviewed by a higher authority in the organization. If the matter is of sufficient seriousness and importance or urgency to the organization, referral to higher authority in the organization may be necessary even if the lawyer has not communicated with the constituent. Any measures taken should, to the extent practicable, minimize the risk of revealing information relating to the representation to persons outside the organization. Even in circumstances where a lawyer is not obligated by Rule 1.13 to proceed, a lawyer may bring to the attention of an organizational client, including its highest authority, matters that the lawyer reasonably believes to be of sufficient importance to warrant doing so in the best interest of the organization.

[5] Paragraph (b) also makes clear that when it is reasonably necessary to enable the organization to address the matter in a timely and appropriate manner, the lawyer must refer the matter to higher authority, including, if warranted by the circumstances, the highest authority that can act on behalf of the organization under applicable law. The organization's highest authority to whom a matter may be referred ordinarily will be the board of directors or similar governing body. However, applicable law may prescribe that under certain conditions the highest authority reposes elsewhere, for example, in the independent directors of a corporation.

Relation to Other Rules

[6] The authority and responsibility provided in this Rule are concurrent with the authority and responsibility provided in other Rules. In particular, this Rule does not limit or expand the lawyer's responsibility under Rules 1.8, 1.16, 3.3 or 4.1. Paragraph (c) of this Rule supplements Rule 1.6(b) by providing an additional basis upon which the lawyer may reveal information relating to the representation, but does not modify, restrict, or limit the provisions of Rule 1.6(b)(1) - (6). Under paragraph (c) the lawyer may reveal such information only when the organization's highest authority insists upon or fails to address threatened or ongoing action that is clearly a violation of law, and then only to the extent the lawyer reasonably believes necessary to prevent reasonably certain substantial injury to the organization. It is not necessary that the lawyer's services be used in furtherance of the violation, but it is required that the matter be related to the lawyer's representation of the organization. If the lawyer's services are being used by an organization to further a crime or fraud by the organization, Rules 1.6(b)(2) and 1.6(b)(3) may permit the lawyer to disclose confidential information. In such circumstances Rule 1.2(d) may also be applicable, in which event, withdrawal from the representation under Rule 1.6(a)(1) may be required.

[7] Paragraph (d) makes clear that the authority of a lawyer to disclose information relating to a representation in circumstances described in paragraph (c) does not apply with respect to information relating to a lawyer's engagement by an organization to investigate an alleged violation of law or to defend the organization or an officer, employee or other person associated with the organization against a claim arising out of an alleged violation of law. This is necessary in order to enable organizational clients to enjoy the full benefits of legal counsel in conducting an investigation or defending against a claim.

[8] A lawyer who reasonably believes that he or she has been discharged because of the lawyer's actions taken pursuant to paragraph (b) or (c), or who withdraws in circumstances that require or permit the lawyer to take action under either of these paragraphs, must proceed as the lawyer reasonably believes necessary to assure that the organization's highest authority is informed of the lawyer's discharge or withdrawal.

Government Agency

[9] The duty defined in this Rule applies to governmental organizations. Defining precisely the identity of the client and prescribing the resulting obligations of such lawyers may be more difficult in the government context and is a matter beyond the scope of these Rules. See Scope [18]. Although in some circumstances the client may be a specific agency, it may also be a branch of government, such as the executive branch, or the government as a whole. For example, if the action or failure to act involves the head of a bureau, either the department of which the bureau is a part or the relevant branch of government may be the client for purposes of this Rule. Moreover, in a matter involving the conduct of government officials, a government lawyer may have authority under applicable law to question such conduct more extensively than that of a lawyer for a private
organization in similar circumstances. Thus, when the client is a governmental organization, a different balance may be 
appropriate between maintaining confidentiality and assuring that the wrongful act is prevented or rectified, for public business is 
involved. In addition, duties of lawyers employed by the government or lawyers in military service may be defined by statutes 
and regulation. This Rule does not limit that authority. See Scope.

**Clarifying the Lawyer's Role**

[10] There are times when the organization's interest may be or become adverse to those of one or more of its 
constituents. In such circumstances the lawyer should advise any constituent, whose interest the lawyer finds adverse to that of 
the organization of the conflict or potential conflict of interest, that the lawyer cannot represent such constituent, and that such 
person may wish to obtain independent representation. Care must be taken to assure that the individual understands that, when 
there is such adversity of interest, the lawyer for the organization cannot provide legal representation for that constituent 
individual, and that discussions between the lawyer for the organization and the individual may not be privileged.

[11] Whether such a warning should be given by the lawyer for the organization to any constituent individual may turn 
on the facts of each case.

**Dual Representation**

[12] Paragraph (g) recognizes that a lawyer for an organization may also represent a principal officer or major 
shareholder.

**Derivative Actions**

[13] Under generally prevailing law, the shareholders or members of a corporation may bring suit to compel the 
directors to perform their legal obligations in the supervision of the organization. Members of unincorporated associations have 
essentially the same right. Such an action may be brought nominally by the organization, but usually is, in fact, a legal 
controversy over management of the organization.

[14] The question can arise whether counsel for the organization may defend such an action. The proposition that the 
organization is the lawyer's client does not alone resolve the issue. Most derivative actions are a normal incident of an 
organization's affairs, to be defended by the organization's lawyer like any other suit. However, if the claim involves serious 
charges of wrongdoing by those in control of the organization, a conflict may arise between the lawyer's duty to the organization 
and the lawyer's relationship with the board. In those circumstances, Rule 1.7 governs who should represent the directors and the 
organization.

**Rule 1.14 Client With Diminished Capacity**

(a) When a client's capacity to make adequately considered decisions in connection with a representation is 
diminished, whether because of minority, mental impairment or for some other reason, the lawyer shall, as far as 
reasonably possible, maintain a normal client-lawyer relationship with the client.

(b) When the lawyer reasonably believes that the client has diminished capacity, is at risk of substantial physical, 
financial or other harm unless action is taken and cannot adequately act in the client's own interest, the lawyer may take 
reasonably necessary protective action, including consulting with individuals or entities that have the ability to take action 
to protect the client and, in appropriate cases, seeking the appointment of a guardian ad litem, conservator or guardian.

(c) Information relating to the representation of a client with diminished capacity is protected by Rule 1.6. When taking 
protective action pursuant to paragraph (b), the lawyer is impliedly authorized under Rule 1.6(a) to reveal information 
about the client, but only to the extent reasonably necessary to protect the client's interests.

**Comment**

[1] The normal client-lawyer relationship is based on the assumption that the client, when properly advised and 
assisted, is capable of making decisions about important matters. When the client is a minor or suffers from a diminished mental 
capacity, however, maintaining the ordinary client-lawyer relationship may not be possible in all respects. In particular, a 
severely incapacitated person may have no power to make legally binding decisions. Nevertheless, a client with diminished 
capacity often has the ability to understand, deliberate upon, and reach conclusions about matters affecting the client's own well-
being. For example, children as young as five or six years of age, and certainly those of ten or twelve, are regarded as having opinions that are entitled to weight in legal proceedings concerning their custody. So also, it is recognized that some persons of advanced age can be quite capable of handling routine financial matters while needing special legal protection concerning major transactions.

[2] The fact that a client suffers a disability does not diminish the lawyer's obligation to treat the client with attention and respect. Even if the person has a legal representative, the lawyer should as far as possible accord the represented person the status of client, particularly in maintaining communication.

[3] The client may wish to have family members or other persons participate in discussions with the lawyer. When necessary to assist in the representation, the presence of such persons generally does not affect the applicability of the attorney-client evidentiary privilege. Nevertheless, the lawyer must keep the client's interests foremost and, except for protective action authorized under paragraph (b), must look to the client, and not family members, to make decisions on the client's behalf.

[4] If a legal representative has already been appointed for the client, the lawyer should ordinarily look to the representative for decisions on behalf of the client. In matters involving a minor, whether the lawyer should look to the parents as natural guardians may depend on the type of proceeding or matter in which the lawyer is representing the minor. If the lawyer represents the guardian as distinct from the ward, and is aware that the guardian is acting adversely to the ward's interest, the lawyer may have an obligation to prevent or rectify the guardian's misconduct. See Rule 1.2(d).

Taking Protective Action

[5] If a lawyer reasonably believes that a client is at risk of substantial physical, financial or other harm unless action is taken, and that a normal client-lawyer relationship cannot be maintained as provided in paragraph (a) because the client lacks sufficient capacity to communicate or to make adequately considered decisions in connection with the representation, then paragraph (b) permits the lawyer to take protective measures deemed necessary. Such measures could include: consulting with family members, using a reconsideration period to permit clarification or improvement of circumstances, using voluntary surrogate decisionmaking tools such as durable powers of attorney or consulting with support groups, professional services, adult-protective agencies or other individuals or entities that have the ability to protect the client. In taking any protective action, the lawyer should be guided by such factors as the wishes and values of the client to the extent known, the client's best interests and the goals of intruding into the client's decisionmaking autonomy to the least extent feasible, maximizing client capacities and respecting the client's family and social connections.

[6] In determining the extent of the client's diminished capacity, the lawyer should consider and balance such factors as: the client's ability to articulate reasoning leading to a decision; variability of state of mind and ability to appreciate consequences of a decision; the substantive fairness of a decision; and the consistency of a decision with the known long-term commitments and values of the client. In appropriate circumstances, the lawyer may seek guidance from an appropriate diagnostician.

[7] If a legal representative has not been appointed, the lawyer should consider whether appointment of a guardian ad litem, conservator or guardian is necessary to protect the client's interests. Thus, if a client with diminished capacity has substantial property that should be sold for the client's benefit, effective completion of the transaction may require appointment of a legal representative. In addition, rules of procedure in litigation sometimes provide that minors or persons with diminished capacity must be represented by a guardian or next friend if they do not have a general guardian. In many circumstances, however, appointment of a legal representative may be more expensive or traumatic for the client than circumstances in fact require. Evaluation of such circumstances is a matter entrusted to the professional judgment of the lawyer. In considering alternatives, however, the lawyer should be aware of any law that requires the lawyer to advocate the least restrictive action on behalf of the client.

Disclosure of the Client's Condition

[8] Disclosure of the client's diminished capacity could adversely affect the client's interests. For example, raising the question of diminished capacity could, in some circumstances, lead to proceedings for involuntary commitment. Information relating to the representation is protected by Rule 1.6. Therefore, unless authorized to do so, the lawyer may not disclose such information. When taking protective action pursuant to paragraph (b), the lawyer is impliedly authorized to make the necessary disclosures, even when the client directs the lawyer to the contrary. Nevertheless, given the risks of disclosure, paragraph (c) limits what the lawyer may disclose in consulting with other individuals or entities or seeking the appointment of a legal representative. At the very least, the lawyer should determine whether it is likely that the person or entity consulted with will act adversely to the client's interests before discussing matters related to the client. The lawyer's position in such cases is an unavoidably difficult one.
Emergency Legal Assistance

[9] In an emergency where the health, safety or a financial interest of a person with seriously diminished capacity is threatened with imminent and irreparable harm, a lawyer may take legal action on behalf of such a person even though the person is unable to establish a client-lawyer relationship or to make or express considered judgments about the matter, when the person or another acting in good faith on that person's behalf has consulted with the lawyer. Even in such an emergency, however, the lawyer should not act unless the lawyer reasonably believes that the person has no other lawyer, agent or other representative available. The lawyer should take legal action on behalf of the person only to the extent reasonably necessary to maintain the status quo or otherwise avoid imminent and irreparable harm. A lawyer who undertakes to represent a person in such an exigent situation has the same duties under these Rules as the lawyer would with respect to a client.

[10] A lawyer who acts on behalf of a person with seriously diminished capacity in an emergency should keep the confidences of the person as if dealing with a client, disclosing them only to the extent necessary to accomplish the intended protective action. The lawyer should disclose to any tribunal involved and to any other counsel involved the nature of his or her relationship with the person. The lawyer should take steps to regularize the relationship or implement other protective solutions as soon as possible. Normally, a lawyer would not seek compensation for such emergency actions taken.

Rule 1.15 Safekeeping Property

(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.

(b) A lawyer may deposit the lawyer's own funds in a client trust account for the sole purpose of paying bank service charges on that account, but only in an amount necessary for that purpose.

(c) A lawyer shall deposit into a client trust account legal fees and expenses that have been paid in advance, to be withdrawn by the lawyer only as fees are earned or expenses incurred.

(d) Upon receiving funds or other property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person. Except as stated in this rule or otherwise permitted by law or by agreement with the client, a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive and, upon request by the client or third person, shall promptly render a full accounting regarding such property.

(e) When in the course of representation a lawyer is in possession of property in which two or more persons (one of whom may be the lawyer) claim interests, the property shall be kept separate by the lawyer until the dispute is resolved. The lawyer shall promptly distribute all portions of the property to which the interests are not in dispute.

Comment

[1] A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property and, if monies, in one or more trust accounts. Separate trust accounts may be warranted when administering estate monies or acting in similar fiduciary capacities. A lawyer should maintain on a current basis books and records in accordance with generally accepted accounting practice and comply with any recordkeeping rules established by law or court order. See, e.g., Model Rules for Client Trust Account Records.

[2] While normally it is impermissible to commingle the lawyer's own funds with client funds, paragraph (b) provides that it is permissible when necessary to pay bank service charges on that account. Accurate records must be kept regarding which part of the funds are the lawyer's.

[3] Lawyers often receive funds from which the lawyer's fee will be paid. The lawyer is not required to remit to the client funds that the lawyer reasonably believes represent fees owed. However, a lawyer may not hold funds to coerce a client into accepting the lawyer's contention. The disputed portion of the funds must be kept in a trust account and the lawyer should
suggestion means for prompt resolution of the dispute, such as arbitration. The undisputed portion of the funds shall be promptly distributed.

[4] Paragraph (e) also recognizes that third parties may have lawful claims against specific funds or other property in a lawyer's custody, such as a client's creditor who has a lien on funds recovered in a personal injury action. A lawyer may have a duty under applicable law to protect such third-party claims against wrongful interference by the client. In such cases, when the third-party claim is not frivolous under applicable law, the lawyer must refuse to surrender the property to the client until the claims are resolved. A lawyer should not unilaterally assume to arbitrate a dispute between the client and the third party, but, when there are substantial grounds for dispute as to the person entitled to the funds, the lawyer may file an action to have a court resolve the dispute.

[5] The obligations of a lawyer under this Rule are independent of those arising from activity other than rendering legal services. For example, a lawyer who serves only as an escrow agent is governed by the applicable law relating to fiduciaries even though the lawyer does not render legal services in the transaction and is not governed by this Rule.

[6] A lawyers' fund for client protection provides a means through the collective efforts of the bar to reimburse persons who have lost money or property as a result of dishonest conduct of a lawyer. Where such a fund has been established, a lawyer must participate where it is mandatory, and, even when it is voluntary, the lawyer should participate.

**Rule 1.16 Declining Or Terminating Representation**

(a) Except as stated in paragraph (c), a lawyer shall not represent a client or, where representation has commenced, shall withdraw from the representation of a client if:

(1) the representation will result in violation of the rules of professional conduct or other law;

(2) the lawyer's physical or mental condition materially impairs the lawyer's ability to represent the client; or

(3) the lawyer is discharged.

(b) Except as stated in paragraph (c), a lawyer may withdraw from representing a client if:

(1) withdrawal can be accomplished without material adverse effect on the interests of the client;

(2) the client persists in a course of action involving the lawyer's services that the lawyer reasonably believes is criminal or fraudulent;

(3) the client has used the lawyer's services to perpetrate a crime or fraud;

(4) the client insists upon taking action that the lawyer considers repugnant or with which the lawyer has a fundamental disagreement;

(5) the client fails substantially to fulfill an obligation to the lawyer regarding the lawyer's services and has been given reasonable warning that the lawyer will withdraw unless the obligation is fulfilled;

(6) the representation will result in an unreasonable financial burden on the lawyer or has been rendered unreasonably difficult by the client; or

(7) other good cause for withdrawal exists.

(c) A lawyer must comply with applicable law requiring notice to or permission of a tribunal when terminating a representation. When ordered to do so by a tribunal, a lawyer shall continue representation notwithstanding good cause for terminating the representation.

(d) Upon termination of representation, a lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering
papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred. The lawyer may retain papers relating to the client to the extent permitted by other law.

Comment

[1] A lawyer should not accept representation in a matter unless it can be performed competently, promptly, without improper conflict of interest and to completion. Ordinarily, a representation in a matter is completed when the agreed-upon assistance has been concluded. See Rules 1.2(c) and 6.5. See also Rule 1.3, Comment [4].

Mandatory Withdrawal

[2] A lawyer ordinarily must decline or withdraw from representation if the client demands that the lawyer engage in conduct that is illegal or violates the Rules of Professional Conduct or other law. The lawyer is not obliged to decline or withdraw simply because the client suggests such a course of conduct; a client may make such a suggestion in the hope that a lawyer will not be constrained by a professional obligation.

[3] When a lawyer has been appointed to represent a client, withdrawal ordinarily requires approval of the appointing authority. See also Rule 6.2. Similarly, court approval or notice to the court is often required by applicable law before a lawyer withdraws from pending litigation. Difficulty may be encountered if withdrawal is based on the client's demand that the lawyer engage in unprofessional conduct. The court may request an explanation for the withdrawal, while the lawyer may be bound to keep confidential the facts that would constitute such an explanation. The lawyer's statement that professional considerations require termination of the representation ordinarily should be accepted as sufficient. Lawyers should be mindful of their obligations to both clients and the court under Rules 1.6 and 3.3.

Discharge

[4] A client has a right to discharge a lawyer at any time, with or without cause, subject to liability for payment for the lawyer's services. Where future dispute about the withdrawal may be anticipated, it may be advisable to prepare a written statement reciting the circumstances.

[5] Whether a client can discharge appointed counsel may depend on applicable law. A client seeking to do so should be given a full explanation of the consequences. These consequences may include a decision by the appointing authority that appointment of successor counsel is unjustified, thus requiring self-representation by the client.

[6] If the client has severely diminished capacity, the client may lack the legal capacity to discharge the lawyer, and in any event the discharge may be seriously adverse to the client's interests. The lawyer should make special effort to help the client consider the consequences and may take reasonably necessary protective action as provided in Rule 1.14.

Optional Withdrawal

[7] A lawyer may withdraw from representation in some circumstances. The lawyer has the option to withdraw if it can be accomplished without material adverse effect on the client's interests. Withdrawal is also justified if the client persists in a course of action that the lawyer reasonably believes is criminal or fraudulent, for a lawyer is not required to be associated with such conduct even if the lawyer does not further it. Withdrawal is also permitted if the lawyer's services were misused in the past even if that would materially prejudice the client. The lawyer may also withdraw where the client insists on taking action that the lawyer considers repugnant or with which the lawyer has a fundamental disagreement.

[8] A lawyer may withdraw if the client refuses to abide by the terms of an agreement relating to the representation, such as an agreement concerning fees or court costs or an agreement limiting the objectives of the representation.

Assisting the Client upon Withdrawal

[9] Even if the lawyer has been unfairly discharged by the client, a lawyer must take all reasonable steps to mitigate the consequences to the client. The lawyer may retain papers as security for a fee only to the extent permitted by law. See Rule 1.15.

Rule 1.17 Sale Of Law Practice
A lawyer or a law firm may sell or purchase a law practice, or an area of law practice, including good will, if the following conditions are satisfied:

(a) The seller ceases to engage in the private practice of law, or in the area of practice that has been sold, [in the geographic area] [in the jurisdiction] (a jurisdiction may elect either version) in which the practice has been conducted;

(b) The entire practice, or the entire area of practice, is sold to one or more lawyers or law firms;

(c) The seller gives written notice to each of the seller's clients regarding:

(1) the proposed sale;

(2) the client's right to retain other counsel or to take possession of the file; and

(3) the fact that the client's consent to the transfer of the client's files will be presumed if the client does not take any action or does not otherwise object within ninety (90) days of receipt of the notice.

If a client cannot be given notice, the representation of that client may be transferred to the purchaser only upon entry of an order so authorizing by a court having jurisdiction. The seller may disclose to the court in camera information relating to the representation only to the extent necessary to obtain an order authorizing the transfer of a file.

(d) The fees charged clients shall not be increased by reason of the sale.

Comment

[1] The practice of law is a profession, not merely a business. Clients are not commodities that can be purchased and sold at will. Pursuant to this Rule, when a lawyer or an entire firm ceases to practice, or ceases to practice in an area of law, and other lawyers or firms take over the representation, the selling lawyer or firm may obtain compensation for the reasonable value of the practice as may withdrawing partners of law firms. See Rules 5.4 and 5.6.

Termination of Practice by the Seller

[2] The requirement that all of the private practice, or all of an area of practice, be sold is satisfied if the seller in good faith makes the entire practice, or the area of practice, available for sale to the purchasers. The fact that a number of the seller's clients decide not to be represented by the purchasers but take their matters elsewhere, therefore, does not result in a violation. Return to private practice as a result of an unanticipated change in circumstances does not necessarily result in a violation. For example, a lawyer who has sold the practice to accept an appointment to judicial office does not violate the requirement that the sale be attendant to cessation of practice if the lawyer later resumes private practice upon being defeated in a contested or a retention election for the office or resigns from a judiciary position.

[3] The requirement that the seller cease to engage in the private practice of law does not prohibit employment as a lawyer on the staff of a public agency or a legal services entity that provides legal services to the poor, or as in-house counsel to a business.

[4] The Rule permits a sale of an entire practice attendant upon retirement from the private practice of law within the jurisdiction. Its provisions, therefore, accommodate the lawyer who sells the practice on the occasion of moving to another state. Some states are so large that a move from one locale therein to another is tantamount to leaving the jurisdiction in which the lawyer has engaged in the practice of law. To also accommodate lawyers so situated, states may permit the sale of the practice when the lawyer leaves the geographical area rather than the jurisdiction. The alternative desired should be indicated by selecting one of the two provided for in Rule 1.17(a).

[5] This Rule also permits a lawyer or law firm to sell an area of practice. If an area of practice is sold and the lawyer remains in the active practice of law, the lawyer must cease accepting any matters in the area of practice that has been sold, either as counsel or co-counsel or by assuming joint responsibility for a matter in connection with the division of a fee with another lawyer as would otherwise be permitted by Rule 1.5(e). For example, a lawyer with a substantial number of estate planning matters and a substantial number of probate administration cases may sell the estate planning portion of the practice but remain in the practice of law by concentrating on probate administration; however, that practitioner may not thereafter accept any estate planning matters. Although a lawyer who leaves a jurisdiction or geographical area typically would sell the entire practice, this
Rule permits the lawyer to limit the sale to one or more areas of the practice, thereby preserving the lawyer's right to continue practice in the areas of the practice that were not sold.

Sale of Entire Practice or Entire Area of Practice

[6] The Rule requires that the seller's entire practice, or an entire area of practice, be sold. The prohibition against sale of less than an entire practice area protects those clients whose matters are less lucrative and who might find it difficult to secure other counsel if a sale could be limited to substantial fee-generating matters. The purchasers are required to undertake all client matters in the practice or practice area, subject to client consent. This requirement is satisfied, however, even if a purchaser is unable to undertake a particular client matter because of a conflict of interest.

Client Confidences, Consent and Notice

[7] Negotiations between seller and prospective purchaser prior to disclosure of information relating to a specific representation of an identifiable client no more violate the confidentiality provisions of Model Rule 1.6 than do preliminary discussions concerning the possible association of another lawyer or mergers between firms, with respect to which client consent is not required. See Rule 1.6(b)(7). Providing the purchaser access to detailed information relating to the representation, such as the client's file, however, requires client consent. The Rule provides that before such information can be disclosed by the seller to the purchaser the client must be given actual written notice of the contemplated sale, including the identity of the purchaser, and must be told that the decision to consent or make other arrangements must be made within 90 days. If nothing is heard from the client within that time, consent to the sale is presumed.

[8] A lawyer or law firm ceasing to practice cannot be required to remain in practice because some clients cannot be given actual notice of the proposed purchase. Since these clients cannot themselves consent to the purchase or direct any other disposition of their files, the Rule requires an order from a court having jurisdiction authorizing their transfer or other disposition. The court can be expected to determine whether reasonable efforts to locate the client have been exhausted, and whether the absent client's legitimate interests will be served by authorizing the transfer of the file so that the purchaser may continue the representation. Preservation of client confidences requires that the petition for a court order be considered in camera. (A procedure by which such an order can be obtained needs to be established in jurisdictions in which it presently does not exist).

[9] All elements of client autonomy, including the client's absolute right to discharge a lawyer and transfer the representation to another, survive the sale of the practice or area of practice.

Fee Arrangements Between Client and Purchaser

[10] The sale may not be financed by increases in fees charged the clients of the practice. Existing arrangements between the seller and the client as to fees and the scope of the work must be honored by the purchaser.

Other Applicable Ethical Standards

[11] Lawyers participating in the sale of a law practice or a practice area are subject to the ethical standards applicable to involving another lawyer in the representation of a client. These include, for example, the seller's obligation to exercise competence in identifying a purchaser qualified to assume the practice and the purchaser's obligation to undertake the representation competently (see Rule 1.1); the obligation to avoid disqualifying conflicts, and to secure the client's informed consent for those conflicts that can be agreed to (see Rule 1.7 regarding conflicts and Rule 1.0(e) for the definition of informed consent); and the obligation to protect information relating to the representation (see Rules 1.6 and 1.9).

[12] If approval of the substitution of the purchasing lawyer for the selling lawyer is required by the rules of any tribunal in which a matter is pending, such approval must be obtained before the matter can be included in the sale (see Rule 1.16).

Applicability of the Rule

[13] This Rule applies to the sale of a law practice of a deceased, disabled or disappeared lawyer. Thus, the seller may be represented by a non-lawyer representative not subject to these Rules. Since, however, no lawyer may participate in a sale of a law practice which does not conform to the requirements of this Rule, the representatives of the seller as well as the purchasing lawyer can be expected to see to it that they are met.
[14] Admission to or retirement from a law partnership or professional association, retirement plans and similar arrangements, and a sale of tangible assets of a law practice, do not constitute a sale or purchase governed by this Rule.

[15] This Rule does not apply to the transfers of legal representation between lawyers when such transfers are unrelated to the sale of a practice or an area of practice.

**Rule 1.18 Duties To Prospective Client**

(a) A person who consults with a lawyer about the possibility of forming a client-lawyer relationship with respect to a matter is a prospective client.

(b) Even when no client-lawyer relationship ensues, a lawyer who has learned information from a prospective client shall not use or reveal that information, except as Rule 1.9 would permit with respect to information of a former client.

(c) A lawyer subject to paragraph (b) shall not represent a client with interests materially adverse to those of a prospective client in the same or a substantially related matter if the lawyer received information from the prospective client that could be significantly harmful to that person in the matter, except as provided in paragraph (d). If a lawyer is disqualified from representation under this paragraph, no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter, except as provided in paragraph (d).

(d) When the lawyer has received disqualifying information as defined in paragraph (c), representation is permissible if:

(1) both the affected client and the prospective client have given informed consent, confirmed in writing, or:

(2) the lawyer who received the information took reasonable measures to avoid exposure to more disqualifying information than was reasonably necessary to determine whether to represent the prospective client; and

(i) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and

(ii) written notice is promptly given to the prospective client.

**Comment**

[1] Prospective clients, like clients, may disclose information to a lawyer, place documents or other property in the lawyer's custody, or rely on the lawyer's advice. A lawyer's consultations with a prospective client usually are limited in time and depth and leave both the prospective client and the lawyer free (and sometimes required) to proceed no further. Hence, prospective clients should receive some but not all of the protection afforded clients.

[2] A person becomes a prospective client by consulting with a lawyer about the possibility of forming a client-lawyer relationship with respect to a matter. Whether communications, including written, oral, or electronic communications, constitute a consultation depends on the circumstances. For example, a consultation is likely to have occurred if a lawyer, either in person or through the lawyer's advertising in any medium, specifically requests or invites the submission of information about a potential representation without clear and reasonably understandable warnings and cautionary statements that limit the lawyer's obligations, and a person provides information in response. See also Comment [4]. In contrast, a consultation does not occur if a person provides information to a lawyer in response to advertising that merely describes the lawyer's education, experience, areas of practice, and contact information, or provides legal information of general interest. Such a person communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship, and is thus not a "prospective client." Moreover, a person who communicates with a lawyer for the purpose of disqualifying the lawyer is not a "prospective client."

[3] It is often necessary for a prospective client to reveal information to the lawyer during an initial consultation prior to the decision about formation of a client-lawyer relationship. The lawyer often must learn such information to determine whether there is a conflict of interest with an existing client and whether the matter is one that the lawyer is willing to undertake. Paragraph (b) prohibits the lawyer from using or revealing that information, except as permitted by Rule 1.9, even if the client or lawyer decides not to proceed with the representation. The duty exists regardless of how brief the initial conference may be.
[4] In order to avoid acquiring disqualifying information from a prospective client, a lawyer considering whether or not to undertake a new matter should limit the initial consultation to only such information as reasonably appears necessary for that purpose. Where the information indicates that a conflict of interest or other reason for non-representation exists, the lawyer should so inform the prospective client or decline the representation. If the prospective client wishes to retain the lawyer, and if consent is possible under Rule 1.7, then consent from all affected present or former clients must be obtained before accepting the representation.

[5] A lawyer may condition a consultation with a prospective client on the person's informed consent that no information disclosed during the consultation will prohibit the lawyer from representing a different client in the matter. See Rule 1.0(c) for the definition of informed consent. If the agreement expressly so provides, the prospective client may also consent to the lawyer's subsequent use of information received from the prospective client.

[6] Even in the absence of an agreement, under paragraph (c), the lawyer is not prohibited from representing a client with interests adverse to those of the prospective client in the same or a substantially related matter unless the lawyer has received from the prospective client information that could be significantly harmful if used in the matter.

[7] Under paragraph (c), the prohibition in this Rule is imputed to other lawyers as provided in Rule 1.10, but, under paragraph (d)(1), imputation may be avoided if the lawyer obtains the informed consent, confirmed in writing, of both the prospective and affected clients. In the alternative, imputation may be avoided if the conditions of paragraph (d)(2) are met and all disqualified lawyers are timely screened and written notice is promptly given to the prospective client. See Rule 1.0(k) (requirements for screening procedures). Paragraph (d)(2)(i) does not prohibit the screened lawyer from receiving a salary or partnership share established by prior independent agreement, but that lawyer may not receive compensation directly related to the matter in which the lawyer is disqualified.

[8] Notice, including a general description of the subject matter about which the lawyer was consulted, and of the screening procedures employed, generally should be given as soon as practicable after the need for screening becomes apparent.

[9] For the duty of competence of a lawyer who gives assistance on the merits of a matter to a prospective client, see Rule 1.1. For a lawyer's duties when a prospective client entrusts valuables or papers to the lawyer's care, see Rule 1.15.

**Counselor**  
**Rule 2.1 Advisor**

In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.

**Comment**

**Scope of Advice**

[1] A client is entitled to straightforward advice expressing the lawyer's honest assessment. Legal advice often involves unpleasant facts and alternatives that a client may be disinclined to confront. In presenting advice, a lawyer endeavors to sustain the client's morale and may put advice in as acceptable a form as honesty permits. However, a lawyer should not be deterred from giving candid advice by the prospect that the advice will be unpalatable to the client.

[2] Advice couched in narrow legal terms may be of little value to a client, especially where practical considerations, such as cost or effects on other people, are predominant. Purely technical legal advice, therefore, can sometimes be inadequate. It is proper for a lawyer to refer to relevant moral and ethical considerations in giving advice. Although a lawyer is not a moral advisor as such, moral and ethical considerations impinge upon most legal questions and may decisively influence how the law will be applied.

[3] A client may expressly or impliedly ask the lawyer for purely technical advice. When such a request is made by a client experienced in legal matters, the lawyer may accept it at face value. When such a request is made by a client inexperienced in legal matters, however, the lawyer's responsibility as advisor may include indicating that more may be involved than strictly legal considerations.
[4] Matters that go beyond strictly legal questions may also be in the domain of another profession. Family matters can involve problems within the professional competence of psychiatry, clinical psychology or social work; business matters can involve problems within the competence of the accounting profession or of financial specialists. Where consultation with a professional in another field is itself something a competent lawyer would recommend, the lawyer should make such a recommendation. At the same time, a lawyer's advice at its best often consists of recommending a course of action in the face of conflicting recommendations of experts.

Offering Advice

[5] In general, a lawyer is not expected to give advice until asked by the client. However, when a lawyer knows that a client proposes a course of action that is likely to result in substantial adverse legal consequences to the client, the lawyer's duty to the client under Rule 1.4 may require that the lawyer offer advice if the client's course of action is related to the representation. Similarly, when a matter is likely to involve litigation, it may be necessary under Rule 1.4 to inform the client of forms of dispute resolution that might constitute reasonable alternatives to litigation. A lawyer ordinarily has no duty to initiate investigation of a client's affairs or to give advice that the client has indicated is unwanted, but a lawyer may initiate advice to a client when doing so appears to be in the client's interest.

Rule 2.3 Evaluation For Use By Third Persons

(a) A lawyer may provide an evaluation of a matter affecting a client for the use of someone other than the client if the lawyer reasonably believes that making the evaluation is compatible with other aspects of the lawyer's relationship with the client.

(b) When the lawyer knows or reasonably should know that the evaluation is likely to affect the client's interests materially and adversely, the lawyer shall not provide the evaluation unless the client gives informed consent.

(c) Except as disclosure is authorized in connection with a report of an evaluation, information relating to the evaluation is otherwise protected by Rule 1.6.

Comment

Definition

[1] An evaluation may be performed at the client's direction or when impliedly authorized in order to carry out the representation. See Rule 1.2. Such an evaluation may be for the primary purpose of establishing information for the benefit of third parties; for example, an opinion concerning the title of property rendered at the behest of a vendor for the information of a prospective purchaser, or at the behest of a borrower for the information of a prospective lender. In some situations, the evaluation may be required by a government agency; for example, an opinion concerning the legality of the securities registered for sale under the securities laws. In other instances, the evaluation may be required by a third person, such as a purchaser of a business.

[2] A legal evaluation should be distinguished from an investigation of a person with whom the lawyer does not have a client-lawyer relationship. For example, a lawyer retained by a purchaser to analyze a vendor's title to property does not have a client-lawyer relationship with the vendor. So also, an investigation into a person's affairs by a government lawyer, or by special counsel employed by the government, is not an evaluation as that term is used in this Rule. The question is whether the lawyer is retained by the person whose affairs are being examined. When the lawyer is retained by that person, the general rules concerning loyalty to client and preservation of confidences apply, which is not the case if the lawyer is retained by someone else. For this reason, it is essential to identify the person by whom the lawyer is retained. This should be made clear not only to the person under examination, but also to others to whom the results are to be made available.

Duties Owed to Third Person and Client

[3] When the evaluation is intended for the information or use of a third person, a legal duty to that person may or may not arise. That legal question is beyond the scope of this Rule. However, since such an evaluation involves a departure from the normal client-lawyer relationship, careful analysis of the situation is required. The lawyer must be satisfied as a matter of professional judgment that making the evaluation is compatible with other functions undertaken in behalf of the client. For example, if the lawyer is acting as advocate in defending the client against charges of fraud, it would normally be incompatible with that responsibility for the lawyer to perform an evaluation for others concerning the same or a related transaction. Assuming
no such impediment is apparent, however, the lawyer should advise the client of the implications of the evaluation, particularly the lawyer's responsibilities to third persons and the duty to disseminate the findings.

Access to and Disclosure of Information

[4] The quality of an evaluation depends on the freedom and extent of the investigation upon which it is based. Ordinarily a lawyer should have whatever latitude of investigation seems necessary as a matter of professional judgment. Under some circumstances, however, the terms of the evaluation may be limited. For example, certain issues or sources may be categorically excluded, or the scope of search may be limited by time constraints or the noncooperation of persons having relevant information. Any such limitations that are material to the evaluation should be described in the report. If after a lawyer has commenced an evaluation, the client refuses to comply with the terms upon which it was understood the evaluation was to have been made, the lawyer's obligations are determined by law, having reference to the terms of the client's agreement and the surrounding circumstances. In no circumstances is the lawyer permitted to knowingly make a false statement of material fact or law in providing an evaluation under this Rule. See Rule 4.1.

Obtaining Client's Informed Consent

[5] Information relating to an evaluation is protected by Rule 1.6. In many situations, providing an evaluation to a third party poses no significant risk to the client; thus, the lawyer may be impliedly authorized to disclose information to carry out the representation. See Rule 1.6(a). Where, however, it is reasonably likely that providing the evaluation will affect the client's interests materially and adversely, the lawyer must first obtain the client's consent after the client has been adequately informed concerning the important possible effects on the client's interests. See Rules 1.6(a) and 1.0(c).

Financial Auditors' Requests for Information

[6] When a question concerning the legal situation of a client arises at the instance of the client's financial auditor and the question is referred to the lawyer, the lawyer's response may be made in accordance with procedures recognized in the legal profession. Such a procedure is set forth in the American Bar Association Statement of Policy Regarding Lawyers' Responses to Auditors' Requests for Information, adopted in 1975.

Rule 2.4 Lawyer Serving As Third-Party Neutral

(a) A lawyer serves as a third-party neutral when the lawyer assists two or more persons who are not clients of the lawyer to reach a resolution of a dispute or other matter that has arisen between them. Service as a third-party neutral may include service as an arbitrator, a mediator or in such other capacity as will enable the lawyer to assist the parties to resolve the matter.

(b) A lawyer serving as a third-party neutral shall inform unrepresented parties that the lawyer is not representing them. When the lawyer knows or reasonably should know that a party does not understand the lawyer's role in the matter, the lawyer shall explain the difference between the lawyer's role as a third-party neutral and a lawyer's role as one who represents a client.

Comment

[1] Alternative dispute resolution has become a substantial part of the civil justice system. Aside from representing clients in dispute-resolution processes, lawyers often serve as third-party neutrals. A third-party neutral is a person, such as a mediator, arbitrator, conciliator or evaluator, who assists the parties, represented or unrepresented, in the resolution of a dispute or in the arrangement of a transaction. Whether a third-party neutral serves primarily as a facilitator, evaluator or decisionmaker depends on the particular process that is either selected by the parties or mandated by a court.

[2] The role of a third-party neutral is not unique to lawyers, although, in some court-connected contexts, only lawyers are allowed to serve in this role or to handle certain types of cases. In performing this role, the lawyer may be subject to court rules or other law that apply either to third-party neutrals generally or to lawyers serving as third-party neutrals. Lawyer-neutrals may also be subject to various codes of ethics, such as the Code of Ethics for Arbitrators in Commercial Disputes prepared by a joint committee of the American Bar Association and the American Arbitration Association or the Model Standards of Conduct for Mediators jointly prepared by the American Bar Association, the American Arbitration Association and the Society of Professionals in Dispute Resolution.
[3] Unlike nonlawyers who serve as third-party neutrals, lawyers serving in this role may experience unique problems as a result of differences between the role of a third-party neutral and a lawyer's service as a client representative. The potential for confusion is significant when the parties are unrepresented in the process. Thus, paragraph (b) requires a lawyer-neutral to inform unrepresented parties that the lawyer is not representing them. For some parties, particularly parties who frequently use dispute-resolution processes, this information will be sufficient. For others, particularly those who are using the process for the first time, more information will be required. Where appropriate, the lawyer should inform unrepresented parties of the important differences between the lawyer's role as third-party neutral and a lawyer's role as a client representative, including the inapplicability of the attorney-client evidentiary privilege. The extent of disclosure required under this paragraph will depend on the particular parties involved and the subject matter of the proceeding, as well as the particular features of the dispute-resolution process selected.

[4] A lawyer who serves as a third-party neutral subsequently may be asked to serve as a lawyer representing a client in the same matter. The conflicts of interest that arise for both the individual lawyer and the lawyer's law firm are addressed in Rule 1.12.

[5] Lawyers who represent clients in alternative dispute-resolution processes are governed by the Rules of Professional Conduct. When the dispute-resolution process takes place before a tribunal, as in binding arbitration (see Rule 1.0(m)), the lawyer's duty of candor is governed by Rule 3.3. Otherwise, the lawyer's duty of candor toward both the third-party neutral and other parties is governed by Rule 4.1.

**Advocate**

**Rule 3.1 Meritorious Claims And Contentions**

A lawyer shall not bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous, which includes a good faith argument for an extension, modification or reversal of existing law. A lawyer for the defendant in a criminal proceeding, or the respondent in a proceeding that could result in incarceration, may nevertheless so defend the proceeding as to require that every element of the case be established.

**Comment**

[1] The advocate has a duty to use legal procedure for the fullest benefit of the client's cause, but also a duty not to abuse legal procedure. The law, both procedural and substantive, establishes the limits within which an advocate may proceed. However, the law is not always clear and never is static. Accordingly, in determining the proper scope of advocacy, account must be taken of the law's ambiguities and potential for change.

[2] The filing of an action or defense or similar action taken for a client is not frivolous merely because the facts have not first been fully substantiated or because the lawyer expects to develop vital evidence only by discovery. What is required of lawyers, however, is that they inform themselves about the facts of their clients' cases and the applicable law and determine that they can make good faith arguments in support of their clients' positions. Such action is not frivolous even though the lawyer believes that the client's position ultimately will not prevail. The action is frivolous, however, if the lawyer is unable either to make a good faith argument on the merits of the action taken or to support the action taken by a good faith argument for an extension, modification or reversal of existing law.

[3] The lawyer's obligations under this Rule are subordinate to federal or state constituitional law that entitles a defendant in a criminal matter to the assistance of counsel in presenting a claim or contention that otherwise would be prohibited by this Rule.

**Rule 3.2 Expediting Litigation**

A lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client.

**Comment**

[1] Dilatory practices bring the administration of justice into disrepute. Although there will be occasions when a lawyer may properly seek a postponement for personal reasons, it is not proper for a lawyer to routinely fail to expedite litigation solely for the convenience of the advocates. Nor will a failure to expedite be reasonable if done for the purpose of frustrating an opposing party's attempt to obtain rightful redress or repose. It is not a justification that similar conduct is often tolerated by the
bench and bar. The question is whether a competent lawyer acting in good faith would regard the course of action as having some substantial purpose other than delay. Realizing financial or other benefit from otherwise improper delay in litigation is not a legitimate interest of the client.

Rule 3.3 Candor Toward The Tribunal

(a) A lawyer shall not knowingly:

(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;

(2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or

(3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.

(d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

Comment

[1] This Rule governs the conduct of a lawyer who is representing a client in the proceedings of a tribunal. See Rule 1.0(m) for the definition of "tribunal." It also applies when the lawyer is representing a client in an ancillary proceeding conducted pursuant to the tribunal's adjudicative authority, such as a deposition. Thus, for example, paragraph (a)(3) requires a lawyer to take reasonable remedial measures if the lawyer comes to know that a client who is testifying in a deposition has offered evidence that is false.

[2] This Rule sets forth the special duties of lawyers as officers of the court to avoid conduct that undermines the integrity of the adjudicative process. A lawyer acting as an advocate in an adjudicative proceeding has an obligation to present the client's case with persuasive force. Performance of that duty while maintaining confidences of the client, however, is qualified by the advocate's duty of candor to the tribunal. Consequently, although a lawyer in an adversary proceeding is not required to present an impartial exposition of the law or to vouch for the evidence submitted in a cause, the lawyer must not allow the tribunal to be misled by false statements of law or fact or evidence that the lawyer knows to be false.

Representations by a Lawyer

[3] An advocate is responsible for pleadings and other documents prepared for litigation, but is usually not required to have personal knowledge of matters asserted therein, for litigation documents ordinarily present assertions by the client, or by someone on the client's behalf, and not assertions by the lawyer. Compare Rule 3.1. However, an assertion purporting to be on the lawyer's own knowledge, as in an affidavit by the lawyer or in a statement in open court, may properly be made only when the lawyer knows the assertion is true or believes it to be true on the basis of a reasonably diligent inquiry. There are circumstances where failure to make a disclosure is the equivalent of an affirmative misrepresentation. The obligation prescribed in Rule 1.2(d) not to counsel a client to commit or assist the client in committing a fraud applies in litigation. Regarding compliance with Rule 1.2(d), see the Comment to that Rule. See also the Comment to Rule 8.4(b).

Legal Argument
Legal argument based on a knowingly false representation of law constitutes dishonesty toward the tribunal. A lawyer is not required to make a disinterested exposition of the law, but must recognize the existence of pertinent legal authorities. Furthermore, as stated in paragraph (a)(2), an advocate has a duty to disclose directly adverse authority in the controlling jurisdiction that has not been disclosed by the opposing party. The underlying concept is that legal argument is a discussion seeking to determine the legal premises properly applicable to the case.

Offering Evidence

Paragraph (a)(3) requires that the lawyer refuse to offer evidence that the lawyer knows to be false, regardless of the client's wishes. This duty is premised on the lawyer's obligation as an officer of the court to prevent the trier of fact from being misled by false evidence. A lawyer does not violate this Rule if the lawyer offers the evidence for the purpose of establishing its falsity.

If a lawyer knows that the client intends to testify falsely or wants the lawyer to introduce false evidence, the lawyer should seek to persuade the client that the evidence should not be offered. If the persuasion is ineffective and the lawyer continues to represent the client, the lawyer must refuse to offer the false evidence. If only a portion of a witness's testimony will be false, the lawyer may call the witness to testify but may not elicit or otherwise permit the witness to present the testimony that the lawyer knows is false.

The duties stated in paragraphs (a) and (b) apply to all lawyers, including defense counsel in criminal cases. In some jurisdictions, however, courts have required counsel to present the accused as a witness or to give a narrative statement if the accused so desires, even if counsel knows that the testimony or statement will be false. The obligation of the advocate under the Rules of Professional Conduct is subordinate to such requirements. See also Comment [9].

The prohibition against offering false evidence only applies if the lawyer knows that the evidence is false. A lawyer's reasonable belief that evidence is false does not preclude its presentation to the trier of fact. A lawyer's knowledge that evidence is false, however, can be inferred from the circumstances. See Rule 1.0(f). Thus, although a lawyer should resolve doubts about the veracity of testimony or other evidence in favor of the client, the lawyer cannot ignore an obvious falsehood.

Although paragraph (a)(3) only prohibits a lawyer from offering evidence the lawyer knows to be false, it permits the lawyer to refuse to offer testimony or other proof that the lawyer reasonably believes is false. Offering such proof may reflect adversely on the lawyer's ability to discriminate in the quality of evidence and thus impair the lawyer's effectiveness as an advocate. Because of the special protections historically provided criminal defendants, however, this Rule does not permit a lawyer to refuse to offer the testimony of such a client where the lawyer reasonably believes but does not know that the testimony will be false. Unless the lawyer knows the testimony will be false, the lawyer must honor the client's decision to testify. See also Comment [7].

Remedial Measures

Having offered material evidence in the belief that it was true, a lawyer may subsequently come to know that the evidence is false. Or, a lawyer may be surprised when the lawyer's client, or another witness called by the lawyer, offers testimony the lawyer knows to be false, either during the lawyer's direct examination or in response to cross-examination by the opposing lawyer. In such situations or if the lawyer knows of the falsity of testimony elicited from the client during a deposition, the lawyer must take reasonable remedial measures. In such situations, the advocate's proper course is to remonstrate with the client confidentially, advise the client of the lawyer's duty of candor to the tribunal and seek the client's cooperation with respect to the withdrawal or correction of the false statements or evidence. If that fails, the advocate must take further remedial action. If withdrawal from the representation is not permitted or will not undo the effect of the false evidence, the advocate must make such disclosure to the tribunal as is reasonably necessary to remedy the situation, even if doing so requires the lawyer to reveal information that otherwise would be protected by Rule 1.6. It is for the tribunal then to determine what should be done — making a statement about the matter to the trier of fact, ordering a mistrial or perhaps nothing.

The disclosure of a client's false testimony can result in grave consequences to the client, including not only a sense of betrayal but also loss of the case and perhaps a prosecution for perjury. But the alternative is that the lawyer cooperate in deceiving the court, thereby subverting the truth-finding process which the adversary system is designed to implement. See Rule 1.2(d). Furthermore, unless it is clearly understood that the lawyer will act upon the duty to disclose the existence of false evidence, the client can simply reject the lawyer's advice to reveal the false evidence and insist that the lawyer keep silent. Thus the client could in effect coerce the lawyer into being a party to fraud on the court.

Preserving Integrity of Adjudicative Process
[12] Lawyers have a special obligation to protect a tribunal against criminal or fraudulent conduct that undermines the integrity of the adjudicative process, such as bribing, intimidating or otherwise unlawfully communicating with a witness, juror, court official or other participant in the proceeding, unlawfully destroying or concealing documents or other evidence or failing to disclose information to the tribunal when required by law to do so. Thus, paragraph (b) requires a lawyer to take reasonable remedial measures, including disclosure if necessary, whenever the lawyer knows that a person, including the lawyer’s client, intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding.

**Duration of Obligation**

[13] A practical time limit on the obligation to rectify false evidence or false statements of law and fact has to be established. The conclusion of the proceeding is a reasonably definite point for the termination of the obligation. A proceeding has concluded within the meaning of this Rule when a final judgment in the proceeding has been affirmed on appeal or the time for review has passed.

**Ex Parte Proceedings**

[14] Ordinarily, an advocate has the limited responsibility of presenting one side of the matters that a tribunal should consider in reaching a decision; the conflicting position is expected to be presented by the opposing party. However, in any ex parte proceeding, such as an application for a temporary restraining order, there is no balance of presentation by opposing advocates. The object of an ex parte proceeding is nevertheless to yield a substantially just result. The judge has an affirmative responsibility to accord the absent party just consideration. The lawyer for the represented party has the correlative duty to make disclosures of material facts known to the lawyer and that the lawyer reasonably believes are necessary to an informed decision.

**Withdrawal**

[15] Normally, a lawyer’s compliance with the duty of candor imposed by this Rule does not require that the lawyer withdraw from the representation of a client whose interests will be or have been adversely affected by the lawyer’s disclosure. The lawyer may, however, be required by Rule 1.16(a) to seek permission of the tribunal to withdraw if the lawyer’s compliance with this Rule’s duty of candor results in such an extreme deterioration of the client-lawyer relationship that the lawyer can no longer competently represent the client. Also see Rule 1.16(b) for the circumstances in which a lawyer will be permitted to seek a tribunal’s permission to withdraw. In connection with a request for permission to withdraw that is premised on a client’s misconduct, a lawyer may reveal information relating to the representation only to the extent reasonably necessary to comply with this Rule or as otherwise permitted by Rule 1.6.

**Rule 3.4 Fairness To Opposing Party And Counsel**

A lawyer shall not:

(a) unlawfully obstruct another party’s access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act;

(b) falsify evidence, counsel or assist a witness to testify falsely, or offer an inducement to a witness that is prohibited by law;

(c) knowingly disobey an obligation under the rules of a tribunal except for an open refusal based on an assertion that no valid obligation exists;

(d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party;

(e) in trial, allude to any matter that the lawyer does not reasonably believe is relevant or that will not be supported by admissible evidence, assert personal knowledge of facts in issue except when testifying as a witness, or state a personal opinion as to the justness of a cause, the credibility of a witness, the culpability of a civil litigant or the guilt or innocence of an accused; or

(f) request a person other than a client to refrain from voluntarily giving relevant information to another party unless:

(1) the person is a relative or an employee or other agent of a client; and

...
(2) the lawyer reasonably believes that the person's interests will not be adversely affected by refraining from giving such information.

Comment

[1] The procedure of the adversary system contemplates that the evidence in a case is to be marshalled competitively by the contending parties. Fair competition in the adversary system is secured by prohibitions against destruction or concealment of evidence, improperly influencing witnesses, obstructive tactics in discovery procedure, and the like.

[2] Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying evidence is also generally a criminal offense. Paragraph (a) applies to evidentiary material generally, including computerized information. Applicable law may permit a lawyer to take temporary possession of physical evidence of client crimes for the purpose of conducting a limited examination that will not alter or destroy material characteristics of the evidence. In such a case, applicable law may require the lawyer to turn the evidence over to the police or other prosecuting authority, depending on the circumstances.

[3] With regard to paragraph (b), it is not improper to pay a witness's expenses or to compensate an expert witness on terms permitted by law. The common law rule in most jurisdictions is that it is improper to pay an occurrence witness any fee for testifying and that it is improper to pay an expert witness a contingent fee.

[4] Paragraph (f) permits a lawyer to advise employees of a client to refrain from giving information to another party, for the employees may identify their interests with those of the client. See also Rule 4.2.

Rule 3.5 Impartiality And Decorum Of The Tribunal

A lawyer shall not:

(a) seek to influence a judge, juror, prospective juror or other official by means prohibited by law;

(b) communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order;

(c) communicate with a juror or prospective juror after discharge of the jury if:

   (1) the communication is prohibited by law or court order;

   (2) the juror has made known to the lawyer a desire not to communicate; or

   (3) the communication involves misrepresentation, coercion, duress or harassment; or

   (d) engage in conduct intended to disrupt a tribunal.

Comment

[1] Many forms of improper influence upon a tribunal are proscribed by criminal law. Others are specified in the ABA Model Code of Judicial Conduct, with which an advocate should be familiar. A lawyer is required to avoid contributing to a violation of such provisions.

[2] During a proceeding a lawyer may not communicate ex parte with persons serving in an official capacity in the proceeding, such as judges, masters or jurors, unless authorized to do so by law or court order.

[3] A lawyer may on occasion want to communicate with a juror or prospective juror after the jury has been discharged. The lawyer may do so unless the communication is prohibited by law or a court order but must respect the desire of the juror not to talk with the lawyer. The lawyer may not engage in improper conduct during the communication.
[4] The advocate's function is to present evidence and argument so that the cause may be decided according to law. Refraining from abusive or obstreperous conduct is a corollary of the advocate's right to speak on behalf of litigants. A lawyer may stand firm against abuse by a judge but should avoid reciprocation; the judge's default is no justification for similar dereliction by an advocate. An advocate can present the cause, protect the record for subsequent review and preserve professional integrity by patient firmness no less effectively than by belligerence or theatrics.

[5] The duty to refrain from disruptive conduct applies to any proceeding of a tribunal, including a deposition. See Rule 1.0(m).

Rule 3.6 Trial Publicity

(a) A lawyer who is participating or has participated in the investigation or litigation of a matter shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

(b) Notwithstanding paragraph (a), a lawyer may state:

(i) the claim, offense or defense involved and, except when prohibited by law, the identity of the persons involved;

(ii) information contained in a public record;

(iii) that an investigation of a matter is in progress;

(iv) the scheduling or result of any step in litigation;

(v) a request for assistance in obtaining evidence and information necessary thereto;

(vi) a warning of danger concerning the behavior of a person involved, when there is reason to believe that there exists the likelihood of substantial harm to an individual or to the public interest; and

(vii) in a criminal case, in addition to subparagraphs (i) through (vi):

(i) the identity, residence, occupation and family status of the accused;

(ii) if the accused has not been apprehended, information necessary to aid in apprehension of that person;

(iii) the fact, time and place of arrest; and

(iv) the identity of investigating and arresting officers or agencies and the length of the investigation.

(c) Notwithstanding paragraph (a), a lawyer may make a statement that a reasonable lawyer would believe is required to protect a client from the substantial undue prejudicial effect of recent publicity not initiated by the lawyer or the lawyer's client. A statement made pursuant to this paragraph shall be limited to such information as is necessary to mitigate the recent adverse publicity.

(d) No lawyer associated in a firm or government agency with a lawyer subject to paragraph (a) shall make a statement prohibited by paragraph (a).

Comment

Comment

[1] It is difficult to strike a balance between protecting the right to a fair trial and safeguarding the right of free expression. Preserving the right to a fair trial necessarily entails some curtailment of the information that may be disseminated about a party prior to trial, particularly where trial by jury is involved. If there were no such limits, the result would be the practical nullification of the protective effect of the rules of forensic decorum and the exclusionary rules of evidence. On the
other hand, there are vital social interests served by the free dissemination of information about events having legal consequences and about legal proceedings themselves. The public has a right to know about threats to its safety and measures aimed at assuring its security. It also has a legitimate interest in the conduct of judicial proceedings, particularly in matters of general public concern. Furthermore, the subject matter of legal proceedings is often of direct significance in debate and deliberation over questions of public policy.

[2] Special rules of confidentiality may validly govern proceedings in juvenile, domestic relations and mental disability proceedings, and perhaps other types of litigation. Rule 3.4(c) requires compliance with such rules.

[3] The Rule sets forth a basic general prohibition against a lawyer's making statements that the lawyer knows or should know will have a substantial likelihood of materially prejudicing an adjudicative proceeding. Recognizing that the public value of informed commentary is great and the likelihood of prejudice to a proceeding by the commentary of a lawyer who is not involved in the proceeding is small, the rule applies only to lawyers who are, or who have been involved in the investigation or litigation of a case, and their associates.

[4] Paragraph (b) identifies specific matters about which a lawyer's statements would not ordinarily be considered to present a substantial likelihood of material prejudice, and should not in any event be considered prohibited by the general prohibition of paragraph (a). Paragraph (b) is not intended to be an exhaustive listing of the subjects upon which a lawyer may make a statement, but statements on other matters may be subject to paragraph (a).

[5] There are, on the other hand, certain subjects that are more likely than not to have a material prejudicial effect on a proceeding, particularly when they refer to a civil matter triable to a jury, a criminal matter, or any other proceeding that could result in incarceration. These subjects relate to:

(1) the character, credibility, reputation or criminal record of a party, suspect in a criminal investigation or witness, or the identity of a witness, or the expected testimony of a party or witness;

(2) in a criminal case or proceeding that could result in incarceration, the possibility of a plea of guilty to the offense or the existence or contents of any confession, admission, or statement given by a defendant or suspect or that person's refusal or failure to make a statement;

(3) the performance or results of any examination or test or the refusal or failure of a person to submit to an examination or test, or the identity or nature of physical evidence expected to be presented;

(4) any opinion as to the guilt or innocence of a defendant or suspect in a criminal case or proceeding that could result in incarceration;

(5) information that the lawyer knows or reasonably should know is likely to be inadmissible as evidence in a trial and that would, if disclosed, create a substantial risk of prejudicing an impartial trial; or

(6) the fact that a defendant has been charged with a crime, unless there is included therein a statement explaining that the charge is merely an accusation and that the defendant is presumed innocent until and unless proven guilty.

[6] Another relevant factor in determining prejudice is the nature of the proceeding involved. Criminal jury trials will be most sensitive to extrajudicial speech. Civil trials may be less sensitive. Non-jury hearings and arbitration proceedings may be even less affected. The Rule will still place limitations on prejudicial comments in these cases, but the likelihood of prejudice may be different depending on the type of proceeding.

[7] Finally, extrajudicial statements that might otherwise raise a question under this Rule may be permissible when they are made in response to statements made publicly by another party, another party's lawyer, or third persons, where a reasonable lawyer would believe a public response is required in order to avoid prejudice to the lawyer's client. When prejudicial statements have been publicly made by others, responsive statements may have the salutary effect of lessening any resulting adverse impact on the adjudicative proceeding. Such responsive statements should be limited to contain only such information as is necessary to mitigate undue prejudice created by the statements made by others.

[8] See Rule 3.8(f) for additional duties of prosecutors in connection with extrajudicial statements about criminal proceedings.
Rule 3.7 Lawyer As Witness

(a) A lawyer shall not act as advocate at a trial in which the lawyer is likely to be a necessary witness unless:

(1) the testimony relates to an uncontested issue;

(2) the testimony relates to the nature and value of legal services rendered in the case; or

(3) disqualification of the lawyer would work substantial hardship on the client.

(b) A lawyer may act as advocate in a trial in which another lawyer in the lawyer’s firm is likely to be called as a witness unless precluded from doing so by Rule 1.7 or Rule 1.9.

Comment

[1] Combining the roles of advocate and witness can prejudice the tribunal and the opposing party and can also involve a conflict of interest between the lawyer and client.

Advocate-Witness Rule

[2] The tribunal has proper objection when the trier of fact may be confused or misled by a lawyer serving as both advocate and witness. The opposing party has proper objection where the combination of roles may prejudice that party’s rights in the litigation. A witness is required to testify on the basis of personal knowledge, while an advocate is expected to explain and comment on evidence given by others. It may not be clear whether a statement by an advocate-witness should be taken as proof or as an analysis of the proof.

[3] To protect the tribunal, paragraph (a) prohibits a lawyer from simultaneously serving as advocate and necessary witness except in those circumstances specified in paragraphs (a)(1) through (a)(3). Paragraph (a)(1) recognizes that if the testimony will be uncontested, the ambiguities in the dual role are purely theoretical. Paragraph (a)(2) recognizes that where the testimony concerns the extent and value of legal services rendered in the action in which the testimony is offered, permitting the lawyers to testify avoids the need for a second trial with new counsel to resolve that issue. Moreover, in such a situation the judge has firsthand knowledge of the matter in issue; hence, there is less dependence on the adversary process to test the credibility of the testimony.

[4] Apart from these two exceptions, paragraph (a)(3) recognizes that a balancing is required between the interests of the client and those of the tribunal and the opposing party. Whether the tribunal is likely to be misled or the opposing party is likely to suffer prejudice depends on the nature of the case, the importance and probable tenor of the lawyer’s testimony, and the probability that the lawyer’s testimony will conflict with that of other witnesses. Even if there is risk of such prejudice, in determining whether the lawyer should be disqualified, due regard must be given to the effect of disqualification on the lawyer’s client. It is relevant that one or both parties could reasonably foresee that the lawyer would probably be a witness. The conflict of interest principles stated in Rules 1.7, 1.9 and 1.10 have no application to this aspect of the problem.

[5] Because the tribunal is not likely to be misled when a lawyer acts as advocate in a trial in which another lawyer in the lawyer’s firm will testify as a necessary witness, paragraph (b) permits the lawyer to do so except in situations involving a conflict of interest.

Conflict of Interest

[6] In determining if it is permissible to act as advocate in a trial in which the lawyer will be a necessary witness, the lawyer must also consider that the dual role may give rise to a conflict of interest that will require compliance with Rules 1.7 or 1.9. For example, if there is likely to be substantial conflict between the testimony of the client and that of the lawyer the representation involves a conflict of interest that requires compliance with Rule 1.7. This would be true even though the lawyer might not be prohibited by paragraph (a) from simultaneously serving as advocate and witness because the lawyer’s disqualification would work a substantial hardship on the client. Similarly, a lawyer who might be permitted to simultaneously serve as an advocate and a witness by paragraph (a)(3) might be precluded from doing so by Rule 1.9. The problem can arise whether the lawyer is called as a witness on behalf of the client or is called by the opposing party. Determining whether or not such a conflict exists is primarily the responsibility of the lawyer involved. If there is a conflict of interest, the lawyer must secure the client’s informed consent, confirmed in writing. In some cases, the lawyer will be precluded from seeking the client’s consent.
See Rule 1.7. See Rule 1.0(b) for the definition of "confirmed in writing" and Rule 1.0(e) for the definition of "informed consent."

[7] Paragraph (b) provides that a lawyer is not disqualified from serving as an advocate because a lawyer with whom the lawyer is associated in a firm is precluded from doing so by paragraph (a). If, however, the testifying lawyer would also be disqualified by Rule 1.7 or Rule 1.9 from representing the client in the matter, other lawyers in the firm will be precluded from representing the client by Rule 1.10 unless the client gives informed consent under the conditions stated in Rule 1.7.

Rule 3.8 Special Responsibilities Of A Prosecutor

The prosecutor in a criminal case shall:

(a) refrain from prosecuting a charge that the prosecutor knows is not supported by probable cause;

(b) make reasonable efforts to assure that the accused has been advised of the right to, and the procedure for obtaining, counsel and has been given reasonable opportunity to obtain counsel;

(c) not seek to obtain from an unrepresented accused a waiver of important pretrial rights, such as the right to a preliminary hearing;

(d) make timely disclosure to the defense of all evidence or information known to the prosecutor that tends to negate the guilt of the accused or mitigates the offense, and, in connection with sentencing, disclose to the defense and to the tribunal all unprivileged mitigating information known to the prosecutor, except when the prosecutor is relieved of this responsibility by a protective order of the tribunal;

(e) not subpoena a lawyer in a grand jury or other criminal proceeding to present evidence about a past or present client unless the prosecutor reasonably believes:

(1) the information sought is not protected from disclosure by any applicable privilege;

(2) the evidence sought is essential to the successful completion of an ongoing investigation or prosecution; and

(3) there is no other feasible alternative to obtain the information;

(f) except for statements that are necessary to inform the public of the nature and extent of the prosecutor's action and that serve a legitimate law enforcement purpose, refrain from making extrajudicial comments that have a substantial likelihood of heightening public condemnation of the accused and exercise reasonable care to prevent investigators, law enforcement personnel, employees or other persons assisting or associated with the prosecutor in a criminal case from making an extrajudicial statement that the prosecutor would be prohibited from making under Rule 3.6 or this Rule.

(g) When a prosecutor knows of new, credible and material evidence creating a reasonable likelihood that a convicted defendant did not commit an offense of which the defendant was convicted, the prosecutor shall:

(1) promptly disclose that evidence to an appropriate court or authority, and

(2) if the conviction was obtained in the prosecutor's jurisdiction,

(i) promptly disclose that evidence to the defendant unless a court authorizes delay, and

(ii) undertake further investigation, or make reasonable efforts to cause an investigation, to determine whether the defendant was convicted of an offense that the defendant did not commit.

(h) When a prosecutor knows of clear and convincing evidence establishing that a defendant in the prosecutor's jurisdiction was convicted of an offense that the defendant did not commit, the prosecutor shall seek to remedy the conviction.
Comment

[1] A prosecutor has the responsibility of a minister of justice and not simply that of an advocate. This responsibility carries with it specific obligations to see that the defendant is accorded procedural justice, that guilt is decided upon the basis of sufficient evidence, and that special precautions are taken to prevent and to rectify the conviction of innocent persons. The extent of mandated remedial action is a matter of debate and varies in different jurisdictions. Many jurisdictions have adopted the ABA Standards of Criminal Justice Relating to the Prosecution Function, which are the product of prolonged and careful deliberation by lawyers experienced in both criminal prosecution and defense. Competent representation of the sovereignty may require a prosecutor to undertake some procedural and remedial measures as a matter of obligation. Applicable law may require other measures by the prosecutor and knowing disregard of those obligations or a systematic abuse of prosecutorial discretion could constitute a violation of Rule 8.4.

[2] In some jurisdictions, a defendant may waive a preliminary hearing and thereby lose a valuable opportunity to challenge probable cause. Accordingly, prosecutors should not seek to obtain waivers of preliminary hearings or other important pretrial rights from unrepresented accused persons. Paragraph (c) does not apply, however, to an accused appearing pro se with the approval of the tribunal. Nor does it forbid the lawful questioning of an uncharged suspect who has knowingly waived the rights to counsel and silence.

[3] The exception in paragraph (d) recognizes that a prosecutor may seek an appropriate protective order from the tribunal if disclosure of information to the defense could result in substantial harm to an individual or to the public interest.

[4] Paragraph (e) is intended to limit the issuance of lawyer subpoenas in grand jury and other criminal proceedings to those situations in which there is a genuine need to intrude into the client-lawyer relationship.

[5] Paragraph (f) supplements Rule 3.6, which prohibits extrajudicial statements that have a substantial likelihood of prejudicing an adjudicatory proceeding. In the context of a criminal prosecution, a prosecutor's extrajudicial statement can create the additional problem of increasing public condemnation of the accused. Although the announcement of an indictment, for example, will necessarily have severe consequences for the accused, a prosecutor can, and should, avoid comments which have no legitimate law enforcement purpose and have a substantial likelihood of increasing public opprobrium of the accused. Nothing in this Comment is intended to restrict the statements which a prosecutor may make which comply with Rule 3.6(b) or 3.6(c).

[6] Like other lawyers, prosecutors are subject to Rules 5.1 and 5.3, which relate to responsibilities regarding lawyers and nonlawyers who work for or are associated with the lawyer's office. Paragraph (f) reminds the prosecutor of the importance of these obligations in connection with the unique dangers of improper extrajudicial statements in a criminal case. In addition, paragraph (f) requires a prosecutor to exercise reasonable care to prevent persons assisting or associated with the prosecutor from making improper extrajudicial statements, even when such persons are not under the direct supervision of the prosecutor. Ordinarily, the reasonable care standard will be satisfied if the prosecutor issues the appropriate cautions to law-enforcement personnel and other relevant individuals.

[7] When a prosecutor knows of new, credible and material evidence creating a reasonable likelihood that a person outside the prosecutor's jurisdiction was convicted of a crime that the person did not commit, paragraph (g) requires prompt disclosure to the court or other appropriate authority, such as the chief prosecutor of the jurisdiction where the conviction occurred. If the conviction was obtained in the prosecutor's jurisdiction, paragraph (g) requires the prosecutor to examine the evidence and undertake further investigation to determine whether the defendant is in fact innocent or make reasonable efforts to cause another appropriate authority to undertake the necessary investigation, and to promptly disclose the evidence to the court and, absent court-authorized delay, to the defendant. Consistent with the objectives of Rules 4.2 and 4.3, disclosure to a represented defendant must be made through the defendant's counsel, and, in the case of an unrepresented defendant, would ordinarily be accompanied by a request to a court for the appointment of counsel to assist the defendant in taking such legal measures as may be appropriate.

[8] Under paragraph (h), once the prosecutor knows of clear and convincing evidence that the defendant was convicted of an offense that the defendant did not commit, the prosecutor must seek to remedy the conviction. Necessary steps may include disclosure of the evidence to the defendant, requesting that the court appoint counsel for an unrepresented indigent defendant and, where appropriate, notifying the court that the prosecutor has knowledge that the defendant did not commit the offense of which the defendant was convicted.

[9] A prosecutor's independent judgment, made in good faith, that the new evidence is not of such nature as to trigger the obligations of sections (g) and (h), though subsequently determined to have been erroneous, does not constitute a violation of this Rule.
Rule 3.9 Advocate In Nonadjudicative Proceedings

A lawyer representing a client before a legislative body or administrative agency in a nonadjudicative proceeding shall disclose that the appearance is in a representative capacity and shall conform to the provisions of Rules 3.3(a) through (c), 3.4(a) through (c), and 3.5.

Comment

[1] In representation before bodies such as legislatures, municipal councils, and executive and administrative agencies acting in a rule-making or policy-making capacity, lawyers present facts, formulate issues and advance argument in the matters under consideration. The decision-making body, like a court, should be able to rely on the integrity of the submissions made to it. A lawyer appearing before such a body must deal with it honestly and in conformity with applicable rules of procedure. See Rules 3.3(a) through (c), 3.4(a) through (c) and 3.5.

[2] Lawyers have no exclusive right to appear before nonadjudicative bodies, as they do before a court. The requirements of this Rule therefore may subject lawyers to regulations inapplicable to advocates who are not lawyers. However, legislatures and administrative agencies have a right to expect lawyers to deal with them as they deal with courts.

[3] This Rule only applies when a lawyer represents a client in connection with an official hearing or meeting of a governmental agency or a legislative body to which the lawyer or the lawyer’s client is presenting evidence or argument. It does not apply to representation of a client in a negotiation or other bilateral transaction with a governmental agency or in connection with an application for a license or other privilege or the client’s compliance with generally applicable reporting requirements, such as the filing of income-tax returns. Nor does it apply to the representation of a client in connection with an investigation or examination of the client’s affairs conducted by government investigators or examiners. Representation in such matters is governed by Rules 4.1 through 4.4.
learned from the long and somewhat eventful history of intelligence oversight may be fruitful. What has worked well? What has proved redundant or unduly subject to politicization?

The intelligence experience offers a fourth additional lesson. Homeland security is arguably the most legally intensive of the national security law fields. There are complex questions of constitutional law involving federalism, the military, privacy, and federal regulation of the private sector. It is no surprise that Northern Command has the largest staff judge advocate's office. What's more, many of these issues are new issues, for which there is no practice or precedent on which to call. That means that lawyers should not just advise on the substance and process of law. They should actively and aggressively appraise the implementation of law for unintended consequences and efficacy. As the DNI is required to report to the president and the Congress each year on the state of intelligence law, homeland security lawyers should identify any statute, regulation, or practice that impedes the ability of their agency to fully and effectively secure the nation. Likewise, policymakers and lawyers should take note from the intelligence experience – law can facilitate response, but legislation marks a beginning of the process, not its conclusion. Homeland security like intelligence ultimately depends on the human factor – leadership and the moral courage to face hard risks and make hard choices.


10 The National Security Lawyer

This book has considered national security law and processes, in the context of four security threats. First is the threat of attack by nonstate and state-sponsored or supported actors using terrorist means. Overseas, this threat is realized on a daily basis. Within the United States the threat is continuous, but intermittent. The threat of high-explosive attack, like car and truck bombs, targeted suicide bombings, or the sabotage of aircraft, is most likely to materialize. The threat of catastrophic attack with nuclear weapons has the greatest potential impact on our way of life and in terms of human cost. It is in relation to this threat in particular that we need to evaluate and test national security law and process, both because of the potential consequence and because of the focus the enemy has placed on this means of attack.

Second, U.S. constitutional values may ebb and wane in an endless conflict against state and nonstate actors engaged in acts of terrorism or posing the threat of terrorism. In light of the interminable nature of this threat, assertions of presidential authority made in extremis may become embedded in U.S. practice and law without a corresponding application of checks and balances. Left outside the reach of effective and independent mechanisms of appraisal, broad assertions of executive authority may in time diminish both the principles of law that define American life as well as the physical security at which they are directed.

Third, since policy differences, as well as those that are politically inspired, regarding the nature of the terrorist threat and the corresponding measure of response may result in a zero-sum compromise; that is, a diminution of security or a diminution of law, rather than contextual formulas that advance both at once. If the executive needs broad and rapid authority to engage in intelligence collection – as it does – the better course is not to limit the authority, for fear of misuse, but to increase the opportunities for meaningful internal and external appraisal. Such appraisal will deter misuse, but as importantly, encourage effective use. In this enduring conflict we may exhaust our resources or our principles in a manner that leaves us unwilling
or unable to effectively address this century's other crises, including the proliferation of weapons of mass destruction to unreliable state actors, the advent of pandemic disease, and environmental degradation and change.

This book has focused on the threat of terrorist attack because this threat today drives the legal debate about the president's constitutional authority. More generally, it drives the purpose and meaning of national security law. It will continue to do so. It is also the threat with the greatest potential to transform U.S. national security, in both a physical and a values sense. The importance of addressing other issues, such as conflict in the Middle East, totalitarian regimes, or pandemic disease, must not be overlooked. Each bears the potential to spiral beyond control resulting in catastrophe at home and overseas. Each of these issues warrants full consideration of the national security instruments and processes described in this book.

In each context, law and national security lawyers may contribute to national security in multiple ways. First, the law provides an array of positive or substantive instruments the president may wield to provide for security. Second, the law provides procedural mechanisms offering opportunities to consider, validate, appraise, and improve policy, as well as to ensure its lawful execution. These mechanisms include the horizontal separation of constitutional powers at the federal level, and the vertical separation of powers between the federal government and state government. They are found as well in statute and in internal executive directive.

The most effective means of appraisal are often found through informal practice. Informal contact allows participants to speak with a freedom not permitted or not often found when bearing the institutional mantle of an office or branch of government. Consider the difference in reaction between the counsel that sits down with the policymaker for a discussion and the counsel who requests the policymaker to put down in a memorandum everything that occurred. With informal practice the role of personality and friendship can serve to facilitate information exchange and the frank exchange of views.

Third, in the international context, law provides mechanisms to achieve U.S. national security objectives. This is evident in the context of maritime security, where U.S. law is pegged to an international framework, and effective security requires international as well as domestic participation. In the area of intelligence integration, bilateral and multilateral agreements, like the PSI and bilateral aviation agreements, provide essential mechanisms for identifying, sharing, intelligence, and acting on intelligence.

Fourth, the law reflects and projects American values of democracy and liberty. Values are silent force multipliers as well as positive national security tools. As Lawrence Wright, the author of The Looming Tower, and others argue, jihadists like Osama Bin Laden offer no programs or policies for governance, no alternative to Western democracy. They offer only the opportunity for revenge. Rule of law is the West's alternative to jihadist terrorism. Law, and respect for law, offers the structure of democracy, the opportunity for individual fulfillment regardless of sex, race, or creed, and a process for the impartial administration of justice. Sustained commitment to the rule of law in practice and perception will serve as a positive national security tool in curtailing recruitment of the next wave and generation of jihadists.

But law, like homeland security, is an incremental endeavor. It is dependent on sustained action, not rhetoric, and perceptions can be swept aside in a few ill-chosen moments. Law, like this conflict, requires sustained sacrifice and sustained support. Thus, divisive legal arguments should be eschewed, unless they are essential to security and there are no alternative means to accomplish the same necessary security end.

The law may contribute to national security in other ways as well. The law is a source of predictability. Through prediction, it becomes a source of deterrence. If the law is understood to permit the use of force, or the collection of intelligence, then allies and opponents alike may modulate their behavior accordingly.

Law can also be a source of calm and stability at times of crisis, guiding but not compelling decisionmakers to processes of decision that rapidly identify risks and benefits and fix accountability. Rapid decision can be obtained through secrecy and by truncating process; it can also be found through the expectation and practice that process provides. This is evident in the case of the military chain of command. This can be true with the president's national security processes as well.

The law is also a source of continuity. An enduring conflict requires enduring commitment, in values, funding, and sacrifice, and thus unity across party or factional transitions. Where essential policy is embedded in framework statutes, it is less subject to, but not immune from the vicissitudes of momentary political advantage or the policy pressures of immediacy. In a conflict marked by intermittent attacks over years, at least in the United States, law can insulate policy from the loss of public or even official attention. For example, where a tool is dependent on sustained funding and policy commitment, legal mandates can hold bureaucratic focus. And, where policy is embedded in law, intelligence and law enforcement operatives may take greater risks knowing the authority for their actions is documented in law and not dependent on classified authorities or recollections of approval.

At the same time, there is much the law cannot do. Law and process provide an opportunity for success, but do not guarantee result. Leadership, culture, personality, and sometimes good luck are as important as law. A well-crafted emergency response directive does not compel first responders to climb the stairs of a burning building—courage, leadership, and commitment do.

Law is a human endeavor that is dependent on the human factor. We are a nation of laws, but we are also a nation of men and women, or if you like a
nati

The National Security Lawyer

including lawyers, to certify requests for electronic surveillance or physical search before they are submitted to the FISA court. In other cases, the presi-
dent has directed a specific process of legal review, for example, in areas
historically prone to peril, such as covert action. However, the majority
of legal advice within the national security process is not required by law
or directive, but is the product of practice, custom, and the rapport, if any,
between officials and their lawyers.

At the national level the daily participants are generally the same from
administration to administration: the attorney general and deputy attorney
general; the Office of Legal Counsel within the Department of Justice; and
other agencies’ general counsels, especially those at Defense, State, CIA, and
DEA, as well as the chairman’s legal advisor. Of course, in context, senior
depu
deputy and alter egos play an equivalent role.

Traditionally, lawyers for the president engaged in national security law
have included the counsel to the president and the National Security Coun-
cil’s legal advisor. Practice varies as to the relative role and weight of each
and the extent to which other White House lawyers, such as the deputy White
House counsel, are involved in national security decision-making, if at all.2
Depending on administrations, and personalities, the role of the counsel to
the vice president has ranged from a defining one to no role at all with respect
to national security law.3

Other lawyers play central roles as well. The judge advocates general
of the military services, for example, are central players in the development of
military law and legal policy as well as the application of the law of armed
conflict within the Department of Justice, the assistant attorney general for
national security, the head of the Office of Intelligence Policy and Review,
the Office of Legal Counsel, and the assistant attorney general for the crim-
nal division are all central players on issues of intelligence and counter-
terrorism. Counsel at each of the intelligence community components and
those engaged in issues of terrorism asset control and money laundering at
Treasury also engage in daily national security practice. Each of these official
is supported by line attorneys who in many cases are the experts in
their discipline and serve as the initial (and often) final point of contact for
legal advice.

Each president, agency head, and commander will adopt his or her own
approach to legal advice, ranging from active engagement with their lawyers
and an understanding of the law to avoidance. Some officials do not seek
legal advice unless the word “law” is mentioned and then only if it is men-
tioned four times in the subject line of a memo. Other officials view their
lawyers as wide-ranging advisors, officials outside the policy process—non-
stakeholders, and thus troubleshooters who may serve in capacity of coun-
selor and not just legal advisors.

Officials and lawyers sometimes refer to lawyers “staying in their lane.”
But with national security there is rarely a street map. It is not always clear

A. NATIONAL SECURITY LEGAL PRACTICE

In a constitutional democracy decisions are intended to be made accord-
ing to law. That means that sound national security process must incor-
porate timely and competent legal advice. What form should that advice
take?

In some cases, legal review is dictated by statute, as in the case of the
Foreign Intelligence Surveillance Act, which requires designated officials,
where the lane begins or ends, and whether the intended road is a goat path or an informational superhighway. Some lawyers will operate on a defined track—litigators litigate, Office of Intelligence Policy and Review (OIPR) attorneys process FISA requests (among other things), the ABCA lawyer-reviews munitions list licenses. However, for more senior lawyers there are rarely set templates outside those dictated by law or directive for how to practice national security law. That means the individual lawyer will define the role as much as he or she will assume it. Moreover, policy officials will ultimately find those lawyers whose style and advice they trust regardless of individual assignments.

Application of national security law involves the rapid review and identification of legal issues embedded in policy options, policy decisions, and policy statements. At the NSC, for example, counsel traditionally coordinates the provision of advice to meetings of the Principals and Deputies Committees, among other tasks, and, where appropriate, attend such meetings to field questions and identify issues. However, this role appears to have varied in texture depending on whether the NSC staff are viewed as facilitators of interagency process or sources of rival legal advice to department general counsel. It also depends on the national security role assumed by the counsel to the president. In addition, NSC counsel provide internal legal advice to the president, national security advisor, and NSC staff as well as review and write memoranda to the president, issue spotting and discussing the legal issues raised. However, these roles are not defined in statute and are, outside the confines of certain narrow spheres, not defined in directive. Rather, these roles are defined by practice and the adoption or modification of past practice by successor officials.

Lawyers serving in defined billets are more likely to find continuity in the form and method of practice, but not necessarily in the substance of practice. For example, the assistant attorney general for the Office of Legal Counsel and his or her deputies generally provide constitutional advice to the executive branch and arbitrate interagency legal disputes, usually through promulgation of formal (often classified) legal memoranda. They are consulted, but are usually less active on daily issues of national security implementation and NSC policy development.

Likewise, line attorneys, as well as programmatic attorneys, are more likely to specialize in particular areas of law and find defined and generally accepted roles. This description might apply, for example, to a line attorney at the State Department who reviews export control licenses, or the attorney at the Treasury Department who reviews financial transactions with foreign states, or a Justice Department lawyer who reviews FISA applications. These lawyers play critical national security roles, but are less likely to address the breadth of national security issues identified in this book. Their lanes are relatively clear and defined.

In addition, lawyers serving as agency general counsel, or their equivalent, perform or oversee the performance of myriad tasks generally associated with lawyers, such as drafting legal documents, reviewing legislation, overseeing litigation, and addressing matters of budget, personnel, and contracting. Rule of law and respect for law are often defined by these tasks. Do the lawyers apply the ethics rules with reason, care, and rigor? Are legislative and public document searches conducted in earnest? These everyday tasks help to define constitutional government, involving as they do the interplay between branches of government and between the government and the public.

Harder to define is the role lawyers should take involving matters where there is discretion as to the style of practice, where the lawyer might have a choice between a proactive, active, or reactive role. In role-playing, personality can be as important as intellectual capacity and training. Not every attorney is suited to a process of decision-making that can be rapid and is conducted under stress and often involves the application of law to uncertain or emerging facts. In this context, lawyers must know when to render their best advice and let go of an issue or when to hold an issue and request time for further review, or to buck the issue up the legal line. There is rarely time to double back for a second look. This may be difficult for lawyers who prefer the deliberative and careful speed of appellate work. It may also be difficult for lawyers who prefer practice areas oriented toward black-letter law and absolute answers. In short, national security practice requires a capacity to close on issues and make decisions, identifying nuance and caveats, if necessary.

National security practice also requires a capacity to compartmentalize work. This is true in a security sense. Lawyers operate under multiple constraints regarding what they can say and to whom based on the attorney-client, deliberative process, and state secrets privileges. (A sure way for a lawyer not to be in the right place at the right time is to garner a reputation for indiscretion.) However, by compartmentalization, I also mean an emotional and intellectual ability to move from one issue to another in rapid succession without getting stuck on just one issue. Policymakers must master this same skill. In contrast, subordinates assigned to specific issues are expected to devote their attention to a single policy issue and drive that issue up and down the chain of command.

As in other legal fields, national security lawyers should learn to subordinate matters of ego to the task of meaningfully applying the law. In doing so, they will have ample opportunity to learn the maxim that it is often the messenger who pays the price for the message. How common is the disapproving refrain, "Lawyers!" The refrain might be more aptly addressed—"Legislators!" "Democracy!" or "Benjamin Franklin!"—unless, of course, it is the lawyer who has delayed decision or diluted decision out of undue
caution or concern. Lawyers must also appreciate that while steady and
faithful application of the law is a hallmark of constitutional government,
in most bureaucratic and substantive contexts they are a supporting arm to
the policy process. Outside the Department of Justice, success is associated
with the policy and not the legal work that supports the policy.

Lawyers are also subject to having their advice tested, as they should.
That is part of the national security process and an essential part of inter-
nal and external appraisal. Does the lawyer understand the facts? Does the
lawyer understand the law? Has the lawyer distinguished between law and
legal policy? However, style varies. Where the stakes are high the distinc-
tion between understanding, testing, and bullying may be lost. Policymak-
ers have a duty to push. Policymakers do not become policy generals by
sitting back and waiting for events to unfold or opportunities to come their
way. Boot camp, it turns out, is sound training for national security lawyers.
National security lawyers will be tested and pushed, as they should be when
national security is at stake. The lawyers will know when a bad idea has
encountered a better idea and they must have the courage to adjust their
views; but they will also know when they have been under pressure, know-
ing the difference between a good faith argument and an inability to hold a
line.

The practice of national security law, like many areas of law, requires
endurance. However, in private practice the client has usually come to the
counsel and now expects hard and constant effort. National security law
requires comparable effort, but a different kind of endurance. Lawyers are
not always invited into the decision-making room. This reluctance reflects
concerns about secrecy, delay, and "lawyer creep" (the legal version of "mis-
sion creep," whereby one legal question becomes seventeen, requiring not
one lawyer but forty-three to answer). Of course, decisionmakers may also
feel that the lawyer may say no to something the policymaker wants to do.
Rule of law often depends on the lawyer being at the right place at the right
time to render advice. This is achieved by reading agendas, attending staff
meetings, and ensuring that they and not the policymaker or the secretariat
define what it is the lawyer needs to see.

National security process is never designed to convenience the lawyer.
Sometimes it is specifically designed to avoid the lawyer. Endurance means
having fresh legs in the middle of the night as well as first thing in the
morning. Some officials will wait until the late night or the weekend to
move their memo, noting "not available" for a legal clearance. The lawyer
avoids such traps by meeting deadlines, negating silent consent, and where
necessary by laying out tripwires, alerting the executive secretary of issues
they need to see, sending timely e-mail prompting inclusion in discussions,
and meeting each policy staff member one-on-one to establish expectations
and confidence.

Most important, counsel should gain the support of the principal official
engaged. This is done by adding value to the process and articulating for
the decisionmaker why lawyers should have a seat at the table (or in the
Situation Room, along the wall). Counsel keeps that seat through effective
practice that is proactive, entailing the same zeal in overcoming legal and
bureaucratic obstacles as they show in identifying them. A lawyer engaged
at the advent of policy development is more likely to influence and guide
than one that clears the final memorandum to the decisionmaker, where
policy advisors have already committed to both the substance of decision
and means of execution. Moreover, if the lawyer waits for issues, or is perused
as an obstacle rather than a source of value, the lawyer will find he or she
is only contributing to decisions where legal review is mandated and then
only as the last stop on the bureaucratic bus route.

Lawyers can advance the application of law in a number of ways. First, by
understanding national security process, counsel can better identify where
decisions are formed and made and thus where legal input is most useful.
Second, by understanding the military and intelligence instruments counsel
can better apply the law to fact. For example, military lawyers can hardly
apply the principles of proportionality, discrimination, and necessity to tar-
gets without having an understanding of the weapons, munitions, and tactics
that inform judgments about necessity and proportionality. Likewise, coun-
sel addressing the use of force should understand the qualitative and quanti-
tative limits of intelligence, distinguishing between evidence, inference, and
intelligence in the process. Third, counsel must understand bureaucracy,
knowing when and how to provide advice in person, via memo, and through
e-mail, without losing sight that each written communication is a record no
matter how informal, and that tone and demeanor can get lost in e-mail.

Finally, counsel should master and proactively recommend legal methods
for overcoming bureaucratic inertia and resistance. Such methods include
(a) presidential directives, (b) agency directives, (c) interagency or intra-
agency memoranda of understanding, (d) lead agency designations, (e) the
conduct of exercises, (f) formal adjustments that defer or eliminate con-
cerns, or (g) just the force of personality or diplomacy. Concerns about the
deployment of armed forces in civil context might be addressed through
requests to any one of these methodologies or by textually limiting the scope,
with the executive director to which the forces might be used. Such limitations
might be put in the president's action memorandum, in the executive order,
or in the rules of engagement. Alternative process may work as well, such
as resorting to biweekly meetings of the agency heads, in an effort to take
issues up and over bureaucratic obstacles, or holding weekly luncheons of the
sort that Mr. Carlini and Mr. Berger found effective.

When lawyers are being used to dress policy disagreements up in deter-
nominative legal clothing — "my lawyer says this is illegal" — good legal process
can allow decisionmakers to focus on the policy issues at hand. Legal issues should be culled from policy agendas and intra- or inter-agency legal meetings held in advance to review options. This allows an opportunity to send issues up the legal chain rather than letting them linger, and possibly sidetrack deliberations. Moreover, just as policymakers forum shop for “can do” lawyers, or perhaps afﬁliate lawyers, lawyers do the same, looking for lawyers who are problem solvers and do not shoot from the hip.

As in other areas of law, preparation is essential. This means reading agendas, consulting with relevant experts on an intra-agency and inter-agency basis, and taking issues up the legal chain of command in advance of meetings so that the lawyer can speak authoritatively when presented with the opportunity to do so. The opportunity may not come again.

Lawyers should also craft, and ﬁguratively or actually, carry walk-about books to address national security issues as they arise. There is no excuse, for example, if the Northern Command staff judge advocate or counsel to the president does not have draft declarations “in the case” to address virtually every homeland security scenario. One purpose of tabletop exercises is to alert policymakers and lawyers to legal obstacles that lie ahead so that lawyers might ﬁnd the means of circumnavigation before the crisis.

Preparation also entails educating the policymaker. Absent groundwork, the policymaker may respond at the moment of crisis by seeing the law only as something that allows or does not allow the policymaker to do what he wants. Contextual advice built on a foundation already laid is readily absorbed and accepted and will add greater value to the national security mission. A 3 AM conference call is no time to explain for the ﬁrst time the principles of proportionality, necessity, and discrimination in targeting. Nor is the immediate aftermath of a natural disaster or terrorist attack the optimal time to explain for the ﬁrst time the delicate legal issues raised by the deployment of U.S. military personnel in a civil context. In addition, the policymaker will understand in a live situation that the lawyer is applying “hard law” — speciﬁc, well established, and sanctioned — and not kibitzing on policy or operational matters.

Advance education also helps establish lines of communication and a common vocabulary of stance between lawyer and policymaker before the crisis. A policymaker who hears a good brief on civil-military deployment will be sure his or her lawyer fully participates in any subsequent decisional process. A large and layered bureaucracy, where the lawyer may be less proximate to the decisionmaker, and cannot count on immediate access, the teaching process is equally important in deﬁning roles as well as legal expectations; however, it is more likely to occur through submission of written memoranda.

National security law also entails the application of legal policy; however, lawyers must take care to distinguish between what is law and what is legal policy. The identiﬁcation of a preferred course as between lawful options is legal policy. The identiﬁcation of a better argument among available arguments is legal policy. Identiﬁcation of the long-term and short-term impact of legal arguments is legal policy. For example, will other states assert the same right to act as the United States asserts, and if so, what are the long-term costs and beneﬁts of the United States asserting such authority? If a constitutional argument is legally available to the president, will it nonetheless generate a congressional or public response disproportionate to the beneﬁts of using the argument?

The reality is that many national security law questions are not yes or no questions. Just as many national security policy decisions represent 51-49 judgments, legal judgments may be close calls; legal policy helps to identify the pros and cons of taking alternative positions. This is particularly the case where legal policy is national security policy as well; for example, where foreign reaction to U.S. legal choices may help or hinder alliances, or where reciprocal applications of law may harm U.S. national security.

Finally, lawyers, like policymakers, must return to appraise their work. Has the ground truth shifted in a manner that alters the legal basis for an action in either a permissive or restrictive manner? Has the president’s directive been implemented in the manner intended? Do the ROE provide adequate protection and ﬂexibility for U.S. forces? Has process been implemented in a manner that facilitates or that impedes rapid decision or the identiﬁcation of policy options?

In summary, the national security lawyer must consider not only the substance of the law but also the process and process of law and the essential decisional skills that bear on the practice of national security law. In the end, however, most senior executive branch lawyers serve at the direction and sometimes discretion of the department counsel, department head, and ultimately the president. Chances are, if the policymaker is not satisﬁed with the manner, method, or substance of advice he will replace his counsel, seek his reassignment, or work around counsel to work with other lawyers. Whether he is satisﬁed will not only depend on the performance of the lawyer but also on whether they share common expectations of how to deﬁne the duties of the national security lawyer.

B. THE DUTY OF THE NATIONAL SECURITY LAWYER

Academics and practitioners sometimes deﬁne the roles and responsibilities of lawyers through identiﬁcation of the client and the client’s interests. Thus, in this context, the ABA Model Rules of Professional Conduct state:

A lawyer must act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client’s behalf.4
It is the client who must decide critical questions of strategy and it is to the client to whom the attorney owes a duty of loyalty and confidentiality.

The client-based private model, however, is least apt in identifying and defining the responsibilities of the national security lawyer: To start, in government context, there are differing views on what is the "client." Scholars and practitioners have identified both animate and conceptual candidates, including the president, the agency, the public interest, and the Constitution. Consider that there are at least five possible and distinct facets to the president as client alone. At any given time the president may function as chief executive, party leader, commander in chief, the embodiment of the institution of the office of the president, or the president in his personal capacity. Each facet potentially represents distinct interests and responsibilities. While the national security lawyer certainly owes the president dedication and commitment as commander in chief, he does not necessarily owe the president as party leader the same zeal. Indeed, he may be legally barred under the Hatch Act from exercising any zeal at all.

In a related manner, there are differing perspectives, or models, on how national security lawyers should practice law, which reflect but are not necessarily determined by the identification of the "client." In the judicial model, for example, the lawyer is expected to render neutral detached views on the law, as a judge might, ultimately rendering a decision as to what the law is. The advocacy model posits that the attorney will render advice on legally available options. The advocacy model, perhaps, is closest in paralleling the private model, with the attorney serving to guide the client's preferred outcomes and then defending the client's actions. It might be said that with the judicial model the attorney works with both hands, presenting both sides of each issue. In the client-based or advocate model, the attorney works with one hand, finding a legal basis for what is the client wishes to accomplish.

Such models bring structure to consideration of the practice of national security law and may serve as a point of departure in describing the duties of the national security lawyer. However, in the daily mix of practice, most national security lawyers do not relate their conduct back to specific theories of ethical responsibility and conflict of interest analysis, as a government or private practitioner might do in criminal practice. This reflects the nature of most national security practice. The provision of advice regarding the Foreign Assistance Act, for example, does not require identification of the client, but rather the competent official who can authorize use of the authority. This may vary depending on the section of law and internal agency process. When the assistant secretary asks whether the United States can provide aid, the question is not, who is the client? - it is whether the Act authorizes such aid and, if so, subject to what substantive and procedural thresholds.

Likewise, judge advocates in the field do not ask, who is the client? - they ask, which commander has the authority to issue the lawful order to attack?

Even where issues present what look like traditional private legal ethical questions, for example, in cases involving the waiver of a privilege, the question is not resolved through identification of the client - for example, the agency or agency head - but rather through knowledge of the substance of law and process. In the case of executive privilege the answer is the president. In the case of classified information the answer is found in some combination of the originating agency, the DNI, and the president. And in the litigation context, the answer may vary depending on who can ultimately speak for the government on the specific issue presented.

Moreover, attorneys need not resort to ethics or academic models to define their role, when so much of the role is already defined in law, and in particular in the Constitution. First, in Article II the president is charged with taking "Care that the Laws be faithfully executed." Second,

Before he enter on the Execution of his Office, he shall take the following Oath or Affirmation:

"I do solemnly swear (or affirm) that I will faithfully execute the Office of President of the United States, and will to the best of my ability, preserve, protect and defend the Constitution of the United States."

Third, Article VI requires that "all executive and judicial Officers, both of the United States and of the several States, shall be bound by Oath or Affirmation, to support this Constitution." As a matter of statute, government officials, including attorneys, also undertake an oath of office tied to the Constitution.

An individual, except the president, elected or appointed to an office of honor or profit in the civil service or uniformed services, shall take the following oath:

"I, , do solemnly swear (or affirm) that I will support and defend the Constitution of the United States against all enemies, foreign or domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God."

This section does not affect other oaths required by law. As is clear from the statutory text, the oath is not exclusive, but is applied in conjunction with other ethical obligations. Thus, in context, attorneys may well have to consider questions pertaining to the identification of the client. A judge advocate, for example, must adhere to his constitutional oath and to applicable bar codes pertaining to the representation of criminal law clients.
The point is that in the private context where academics and practitioners might reasonably debate to whom the attorney owes loyalty, the government attorney takes one oath and that is to the Constitution and not to a client. Further, that oath and the Constitution require faithful application of the law. That starts with faithful application of the Constitution, its structure and its substance, in the common defense of security and liberty.

Finally, the “client,” used here to identify the official with authority to decide an issue, as well as the role of the national security attorney, will vary in context. There are more than 40,000 lawyers in the government. Only a fraction of this number practice national security law. In each context, the “client” may be different. Moreover, within each setting the lawyer will (or should) play each role described above: advisor, counselor, advocate, and judge. The practice is also sufficiently contextual that the answer as to which role is appropriate is found not in identifying the client or a particular model of practice, but in the facts. The skill and art is in knowing when and how to play each role.

Consider the following hypothetical, presenting a preemption scenario likely to occur in the future. The president’s attorney is asked in the middle of the night to review a prospective target for a missile strike. For reasons of operational security, a “black list” is in place. It does not include the attorney general. The target is a suspected WMD weapons facility in a restricted country, but one with which the United States is nominally at peace. The facility is operating under cover as a legitimate commercial enterprise. The target is in play because of intelligence suggesting, but not confirming, that the plant is linked to Al Qaeda affiliates.

For sound operational reasons, an up or down decision on attacking is needed within two hours, or sooner, to avoid the risk that the enemy will disperse extant WMD weapons. However, it turns out that at the staff level there is disagreement on whether the intelligence linking the target to terrorist actors or even clandestine activities is credible and persuasive. There are also differences of view as to whether additional methods of intelligence gathering may improve U.S. knowledge, although there is general agreement that the target is a hard target and that any disclosure of U.S. interest in the facility could lead to the rapid dispersal of existing WMD stockpiles (if any).

What is the role and the duty of the attorney, and is that role defined by identification of the client or application of a judicial, advocacy, or advisory model of practice?

In the advocate model, the attorney might determine that he or she will defend the president’s decision regardless of how the factual dispute is resolved, or for that matter whether it is resolved. Thus, the attorney might advise that so long as the president believes he is defending the country he has the legal authority to do so and counsel will support the decision under U.S. and international law.

In a judicial model, the attorney might ask additional questions. What is the potential for collateral consequences? And, what is the basis for the difference in intelligence opinion? He would then apply the law to the facts as they are known to determine whether a strike is lawful under U.S. and international law. To the extent the attorney believes the target is “lawful” under U.S. law he would indicate so, and if necessary, advise the president that he could not in good faith approve the target.

Under an advocacy model, the attorney might advise the president as to the legal standard and defer to the president’s judgment on the application of law to fact. Under the public interest model, the attorney might consider what is in the best interest of the United States or the public. Presumably this interest would revolve around getting the facts right, but also taking all measures necessary to defend the country, erring on the side of security.

The attorney should play all of these roles. First, under any rubric the attorney has a duty to resolve the factual ambiguity. Arguably, under an advocacy model, the attorney might sit back and defer to the president’s view of the law and facts and then defend both. However, it is not clear how such inaction would represent zealous or diligent representation. The president would still require knowledge of the facts and the law to faithfully execute his security functions. Moreover, under the advocacy model, even if the attorney were poised to validate the president’s judgment, he would still need to know the countermovements to better represent the president’s choice. Thus, the question is how best to do so in a manner that respects the role of the president as commander in chief and chief executive.

The hypothetical also illustrates the potential range of duties, functions, and choices the attorney might (and in my view should) address in a given scenario. The national security lawyer has a duty to guide decisionmakers toward legally available options. In performing this function in a timely and meaningful manner, the lawyer provides for our physical security. In doing it faithfully, based on honest belief on the application of law, he provides for the security of our way of life, which is to say, a process of decision founded on respect for the law and subject to law.

The hypothetical presents threshold questions of authority. Therefore, the attorney must consider whether the president has the constitutional authority to authorize the missile strike. As the president is also, in effect, approving a specific military target while authorizing the initial resort to force the attorney should run through a three-pronged substantive template:

(1) Does the president have the constitutional authority to use force, and is it subject to a statutory overlay? If so, must or should the president consult with the Congress, or notify the Congress in advance?
(2) Is the use of force a lawful exercise in self-defense, anticipatory self-defense, or preemption? Will such an assertion be viewed as controversial? And, what are the legal policy ramifications of U.S. decision?
(3) Is the president's selection of targets and the means and methods of attack consistent with the law of armed conflict as reflected in U.S. and international law?

The attorney should also consider a procedural template:

(1) Who must authorize the use of force?
(2) Must the attorney general be informed? Should the attorney general be informed? If not, if or if so, who must/may/should make that decision?
(3) Is the president aware of the factual dispute? If not, whose duty is it to inform him?
(4) Must the factual dispute be resolved before authorization may be given? If so, how can it be resolved in the timeline presented?

These questions present a mix of fact and law, law and legal policy, as well as substance and process. There are no textbook answers. There are as clearly wrong answers. There are as well, as a matter of legal policy, preferred answers. One solution: the lawyer can identify the parameters of the factual dispute and ensure that they are framed and communicated within any decisional documents going to the president. But it is two in the morning. The president has already made his decision, without knowing that the facts are sliding. One solution: the president's lawyer can call the national security advisor and identify the problem and a solution -- a conference call with the DNI, national security advisor, and the secretary of defense to determine if the facts are sliding or whether analysts are rehashing judgments already made at the top, without their knowledge. Does the DNI stand by the intelligence and intelligence judgment or not? And if there is any shift in fact or analysis, is the president and the military chain of command aware?

The scenario continues. With the input and concurrence of the attorney general, the DNI, and the secretary of defense, the president decides to authorize the strike. The lawyer now becomes advocate. He clears talking points for use with the Congress, the media, and foreign governments, conscious that the talking points, as opposed to the advice rendered in advance of decision, will shape outside perspectives on the validity of U.S. assertions of authority. As a matter of legal policy, will this be cast in the language of preemption, anticipatory self-defense, self-defense, or under some other rubric? In doing so, he considers what information if any can be disclosed in support of the intelligence link between the target and terrorism. He adds bullets on the legal basis for the strike, not as judge or advisor, reflecting the best arguments on both sides, but as advocate, presenting the arguments in support of action. Bigot list permitting, the lawyer ensures the State Department is generating an Article 51 report to the United Nations identifying the U.S. legal position as one of self-defense.

The strike occurs. The lawyer now shifts to the role of advisor appraising the process. What worked well and what didn't work well? Could the factual dispute have been resolved through alternative process, or was it only identified and forced to the surface through the presentation of decision? Should the president retain case-specific decision authority over comparable strikes, or authorize strikes in concept in the future and if so subject to what qualifications in policy, law, and legal policy? Is this a question of law, or of command preference that should be dictated by operational need and presidential style?

The hypothetical also illustrates the extent to which the application of national security law and process is dependent on culture, personality, and style. The president can direct legal review of his decisions, but if a national security advisor is not committed to such a review, it will not occur in a meaningful manner; it at all. The process would have failed if the lawyer did not make the call or if the national security advisor would not take the call. In short, it is not the presence of counsel at the NSC, the White House, or the Defense Department that upholds the law. It is the active presence of a president, a national security advisor, and department secretaries who insist on legal input in the decision-making process and lawyers who will place their integrity and careers on the line to provide it.

An indeterminate conflict, of indefinite duration, against unknown enemies and known enemies unless put uncommon strain on U.S. national security. It will also put uncommon strain on principles of liberty. If we meet this day's threats without destroying the fabric of our constitutional liberty it will be through the effective and meaningful application of national security law.

The sine qua non for broad national security authority is meaningful oversight. By oversight, I mean the considered application of constitutional structure, executive process, legal substance, and relevant reviews of decision-making -- all of which depend on the integrity and judgment of lawyers. It is lawyers who will help us find the right combination of broad executive authority to defeat terrorism with the considered application of law before action and subsequent appraisals to protect our liberty. So whether one likes law or not, it is central to national security. Lawyers and not just generals will decide the outcome of this conflict.

Lawyers reside at the intersection where physical safety and liberty merge. In this role they are indispensable to good process and should feel a duty to advocate good process. Good process permits the faithful application
of the law and the accomplishment of the security objectives. In any given context, the pressure of the moment may encourage short-term thinking and the adoption of process shortcuts. The lawyer alone may be sufficiently detached from the policy outcome to identify the enduring institutional consequences of a particular course of action. So too, the lawyer alone may be familiar, and may feel an obligation to be familiar, with applicable written procedures. Process is substance if it means critical actors and perspectives are omitted from the discussion table.

Good process is not antithetical to timely decisions, operational timelines, or to secrecy. Process must find the right balance between speed and strength, secrecy and input. But process can always meet deadlines. There is no excuse for shortcuts. Process can be made to work faster and smarter. By example, if legal review is warranted, the attorney general alone can review a matter and, if need be, do so while sitting next to the president in the Oval Office.

Third, process should be contextual. The legal and policy parameters for responding to terrorism are different from those for responding to a Balkan crisis. Clandestine and remote military operations against a hidden enemy will dictate different decision processes than NATO air operations against fixed targets, as the different political and policy parameters of both situations. One has to maintain situational awareness, to find the measure of process and approval that ensures law is applied in a manner that is faithful to constitutional, statutory, and executive dictates and that meets operational timelines. Therefore, there will always be some tension as to who should see what when.

Finally, lawyers support and defend the Constitution and not just the policies of their government. It is not clear how a president can faithfully apply the law without faithfully applying the constitutional principles identified in Chapters 3 and 4, including the separation of powers, and checks and balances. Constitutional faith recognizes that the Constitution is a national security document, which is the face of a WMD threat is appropriately read broadly and realistically. Constitutional faith also recognizes that liberty and the rule of law are national security values, which the Constitution is designed to preserve and to protect.

A definition of national security that includes constitutional values makes lawyers schooled in history, law, and ethics essential to the national security process. Being a lawyer in such a process is more than saying yes to a client's goals; it means guiding policymakers not just to lawful outcomes, but to outcomes addressing both aspects of national security by providing for security and preserving our sense of liberty. That is one reason this book places as much emphasis on the role of the lawyer as it does on the content of the law.

The National Security Lawyer

There are hard questions ahead in a time of homeland insecurity from which lawyers should not shy. Hamilton observed, 

The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions that have a tendency to destroy their civilian and political rights. To be more safe, they at length become willing to run the risk of being less free.

It is the national security lawyer's duty to alert policymakers to these tensions. The lawyer's duty is to show all sides to every issue while guiding policymakers and above all the president to lawful decisions that protect our security and our liberty. This is hardest to do when lives are at stake. But the Constitution was not designed to fail, to safeguard our security at the expense of our freedom, nor celebrate freedom at the expense of security. It is designed to underpin and protect us and our way of life. National security lawyers daily demonstrate how it can and must be done.

As a result, we should not begrudge democracy's adherence to law, but continue to find the best contextual process for its meaningful application. In war, and no more so than in addressing a threat where the terrorists' choice of weapons and targets may be unlimited, this means a substance, process, and practice of law that is both security effective and faithful to democratic values.

As Justice Brandeis reminded in Whitney,

Those who won independence believed that the final end of the state was to make men free to develop their faculties, and that, in its government the deliberative forces should prevail over the arbitrary. They believed liberty to be the secret of happiness and courage to be the secret of liberties. 

The law depends on the morality and courage of those who apply it. It depends on the moral courage of lawyers who raise tough questions, who dare to argue both sides of every issue, who insist upon being heard at the highest levels of decision-making, and who ultimately call the legal questions as they believe the Constitution dictates and not necessarily as policymakers may want at a moment in time. We do not live in a moment in time. We and our children live in perilous times.
Panel V:  

Emerging Technology and Executive Order 12333

Moderator:  
Mary Ellen Callahan
Executive Order 12333
United States Intelligence Activities
(As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1 Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts

1.1 Goals. The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

(1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

(2) Threats to the United States and its interests from terrorism; and

(3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 The National Security Council.

(a) Purpose. The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence,
counterintelligence, and covert action, and attendant policies and programs.

(b) **Covert Action and Other Sensitive Intelligence Operations.** The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 **Director of National Intelligence.** Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

1. Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

2. Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

1. Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived;

2. May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

3. Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

4. In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

   (A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

   (B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

   (C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

5. Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence
programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preemption, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head of the originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;
(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;
(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director’s exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director’s authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director’s intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head...
chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 The Intelligence Community. Consistent with applicable Federal law and with the other provisions of this order, and under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

(g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies. The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;
(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 Heads of Elements of the Intelligence Community. The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 Intelligence Community Elements. Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.
(a) THE CENTRAL INTELLIGENCE AGENCY. The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;

(3) Conduct counterintelligence activities;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;

(6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;
(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and
(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 The Department of State. In addition to the authorities exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

(a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 The Department of the Treasury. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 The Department of Defense. The Secretary of Defense shall:

(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;
(b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) through (i) above, and to support the Intelligence Community elements of the Department of Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (l) and, when the Coast Guard is operating as part of the Department of Defense, and above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 The Department of Homeland Security. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 The Department of Energy. In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.
1.13 *The Federal Bureau of Investigation.* In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and .7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

**PART 2 Conduct of Intelligence Activities**

2.1 **Need.** Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 **Purpose.** This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 **Collection of information.** Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.
In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 Collection Techniques. Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 Assistance to Law Enforcement and other Civil Authorities. Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 Contracting. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency With Other Laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 Human Experimentation. No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 Prohibition on Assassination. No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.12 Indirect Participation. No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 Limitation on Covert Action. No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 General Provisions

3.1 Congressional Oversight. The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 Implementation. The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.
3.3 Procedures. The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 References and Transition. References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 Definitions. For the purposes of this Order, the following terms shall have these meanings:

(a) Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) Covert action means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) Electronic surveillance means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) Employee means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) Foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) Intelligence includes foreign intelligence and counterintelligence.

(g) Intelligence activities means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) Intelligence Community and elements of the Intelligence Community refers to:

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;
(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) **National Intelligence and Intelligence Related to National Security** means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(ii) **The National Intelligence Program** means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) **United States person** means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 **Revocation.** Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 **General Provisions.**

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

(2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.
Statement for the Record

before the
Senate Homeland Security and
Governmental Affairs Committee

“Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration”

Statement of Corin R. Stone
Intelligence Community Information Sharing Executive
Office of the Director of National Intelligence

10 March 2011
Statement of Corin R. Stone
Intelligence Community Information Sharing Executive
before the
Senate Homeland Security and Governmental Affairs Committee
10 March 2011

Introduction
Chairman Lieberman, Ranking Member Collins, and Members of the Committee, thank you for the invitation to appear before you today to discuss the Intelligence Community’s (IC) progress and challenges in sharing information. I want to first recognize the Committee’s leadership on these important issues and thank you for your continued commitment to assisting us as we address the many questions associated with the need to both share information and to protect it.

Information Sharing
As the IC Information Sharing Executive (IC ISE), my main focus today concerns classified information – and, in particular, information that is derived from intelligence sources and methods, or information that is reflected in the analytic judgments and assessments that the IC produces. I want to be clear, though, that our concern for the protection of information is not restricted to the fragility of sources and methods, but extends as well to broader aspects of national security. We recognize, and will hear today, that the Departments of State and Defense, as well as other federal agencies, themselves originate classified national security information that is vital to the protection of our nation and conduct of our foreign relations, and this information is, like intelligence information, widely distributed and used throughout the government to achieve these objectives. As we have seen recently, the unauthorized disclosure of any form of classified national security information has serious implications for the policy and operational aspects of national security.

I am acutely aware that our major task is to find what the Director of National Intelligence (DNI) has termed the “sweet spot” between the two critical imperatives of sharing and protecting information. To ensure that we share and protect information effectively, we work to find the “sweet spot,” as the compelling need for information sharing remains a top priority for the DNI and the IC.

The need is compelling because information sharing is essential to provide quality intelligence support to such disparate activities as coalition warfare, counternarcotics, counterproliferation, homeland security, and cybersecurity. Intelligence judgments and reports that reflect our commitment to sharing information are also essential to support senior policymakers who must deal with matters of increasing complexity in a world that is interconnected and fast-paced. Every day, the talented collectors and analysts within the IC share vital information with each other, our partners, and customers, to provide critical support to senior policymakers across the Executive Branch and Congress. We have made great strides in the post-9/11 era, especially in the counterterrorism mission. The United States is safer because of the progress we have made –
as a Community and as a Government – in sharing information more effectively and raising “signals” from the “noise.”

Our efforts are not a matter of finding a “balance” between the need to share information and the need to protect; that term implies a “zero-sum” relationship that, as we increase sharing, for example, we also decrease protection. We believe it is more accurate to approach this relationship as one that requires coordinated increases in protecting and sharing information. In other words, as we increase information sharing, we must also increase the protections afforded to that information.

With that approach in mind, we are working to ensure that the IC has the policies, practices, and technologies in place to enable the Community to share information, while both protecting the information and safeguarding privacy and civil liberties. It is clear, for example, that a fundamentally important relationship exists between the parallel needs to share and protect information, and the IC’s technology systems and networks’ ability to securely store and handle that information. But we also recognize that some of the most complex matters that must be addressed as we increase the sharing of intelligence within and beyond the bounds of the IC largely relate to policy, legal, and cultural issues.

**IC Information Sharing Executive**

To provide additional emphasis in those areas (policy, legal, and cultural), and to move the center of gravity for the IC beyond technologies and systems, the DNI reassigned the IC ISE role from the IC Chief Information Officer to the ODNI’s Office of Policy and Strategy in October 2010. As the DNI’s appointed IC ISE, I am developing a coordinated and comprehensive plan for responsibly managing information sharing activities within the ODNI, across the IC, and with all of our mission partners.

To that end, I have established an internal governance process for ensuring a coordinated information sharing approach within the ODNI. I have also refashioned and reinvigorated the IC ISE’s engagement activities and governance across the IC to do the same, as well as to set IC-wide priorities and oversee their execution. In carrying out these functions and this mission, I am directly accountable to the Principal Deputy Director of National Intelligence. In addition, I have an excellent partnership with the Program Manager for the Information Sharing Environment (PM-ISE), who focuses on sharing information related to counterterrorism and homeland security across the entire U.S. Government. Our close working relationship helps me ensure that the information sharing activities we undertake in the IC related to those areas are consistent and interoperable with the steps being taken across the entire U.S. Government, as well as with our state, local, tribal, and private sector partners. In this partnership, we agree; responsible information sharing remains our top priority.

**Finding the “Sweet Spot”**

The IC’s work on the complicated questions related to access to intelligence, and the ways in which it can be a shared responsibility, pre-dates the recent unauthorized disclosures. The challenges associated with both sharing and protecting intelligence are not new and have been a
factor of major consideration in the Community for years. As this Committee knows all too well, it is one of the foundational principles underlying the Intelligence Reform and Terrorism Prevention Act of 2004, as well as the creation of the Office of the Director of National Intelligence. The latest unauthorized disclosures, however, underscored again the importance of a comprehensive approach to address those challenges.

Working within the broad Government effort that is underway to address the security of classified information in the context of information sharing, the IC’s strategy involves three interlocking elements:

• The first is ACCESS: ensuring that the right people can discover and access the networks and information they need to perform their duties, but not to information that they do not need. This is a complex matter that is centered on the principle of determining “Need to Know.”

• The second element is TECHNICAL PROTECTION: technically limiting the ability to misappropriate, manipulate, or transfer data, especially in large quantities, such as by disabling or prohibiting the use of removable media on classified networks, including thumb drives and CDs.

• The third area is AUDITING and MONITORING: taking actions to give the IC day-to-day confidence that the information access granted to our personnel is being properly used. This involves monitoring and auditing user activity on classified computer systems to identify anomalous activity, and following up accordingly.

We are also focused on additional measures to protect classified information from “Insider Threats.” Consequently, in concert with the three principal elements of our strategy, we must also sustain strong personnel security investigation and reinvestigation programs, ensure that we conduct effective security awareness training, and take or support action against those who disclose classified information without authorization.

Addressing the Insider Threat

The damage caused by the unauthorized disclosures of classified information stems from the actions of individuals and their malicious exploitation of the opportunities available to them in a classified environment. Over the course of our nation’s history, there have been spies among us, and the actions of those individuals have demonstrated how a trusted insider “gone wrong” can do grave damage to national security. It is clear that we must be vigilant and proactive in trying to detect, mitigate, and deter this threat.

To meet that challenge, the U.S. Government must have a comprehensive insider threat detection capability. The National Counterintelligence Executive (NCIX) has developed such a program for the IC, and we are working toward implementing its principles. Over the course of the last several months, agencies have worked together to support the development of an insider threat monitoring capability that can be deployed across the entire Government. There are different maturity levels across the Government, and, as a result, improvements will be phased throughout
implementation. Technology refresh is a vital part of this program and is being considered for emerging threats, as well as our technology platform, for sharing and protecting information. A robust insider threat detection program will allow departments and agencies to manage the risk caused by granting broader access to sensitive information in Government.

In structuring and implementing insider threat efforts, however, it is paramount that each department and agency ensures privacy protections are in place, and that access to insider threat detection information and activities are limited to authorized personnel performing counterintelligence, security, and other appropriate oversight missions.

It is also important to note that insider threat capabilities are not intended only to detect or deter potential bad actors. These capabilities are also critical to build and increase confidence that access to intelligence is being properly used and protected. That confidence is essential to building a culture that supports responsible information sharing.

Security

Executive Order 13526 established the Information Security Oversight Office (ISOO) of the National Archives and Records Administration as the oversight organization for safeguarding classified information in the federal government, and gave the DNI responsibility for the oversight of all classified national intelligence information. The ONCIX performs the security oversight function for the IC to ensure that its 17 agencies and elements have effective measures and mechanisms to protect classified national intelligence from unauthorized disclosure, and to ensure that any security barriers to information sharing are necessary.

There has not been a unified process to assess the counterintelligence, security, and information assurance postures within all Executive Branch departments and agencies. Departments and agencies currently assess their own performance and compliance with internal programs and regulations. In coordination with OMB, ISOO and ONCIX will evaluate and assist agencies in their assessments, and plan to use on-site reviews as part of that process.

Technology

A dual-pronged approach is needed to improving technology solutions in the classified information sharing environment: (1) enhancements to logical and physical security controls; and (2) incremental delivery of information sharing capabilities through prioritized mission needs from the intelligence, defense, and civilian agency communities.

Critical capabilities supported by technology – such as identity and access management, data protection and discoverability, and a reliable audit process – play an integral role in the steps we are taking to find the “sweet spot” between the need to share and the need to protect intelligence. In particular, technology can help regulate the availability of information. It can also help to identify and prevent the potential misappropriation, manipulation, or transfer of data; as well as the means by which such actions can be taken. Further, technology can record users’ actions and
support the investigation and prosecution of those who intentionally misappropriate classified information. The IC is working to provide end-to-end data management technology to ensure that sensitive intelligence data is appropriately protected throughout its life cycle (creation, use, transit, storage).

To enable strong network authentication and ensure that networks and systems can authoritatively identify who is accessing classified information, the IC CIO is implementing user authentication technologies and is working with the IC elements to achieve certificate issuance to eligible IC personnel in the first quarter of fiscal year 2012. In addition to networks and systems, the IC is working to advance the authentication standards to applications in order to better protect data. Identity management for both networks and applications represent the foundational capability required to enable access management decisions and ultimately the recording or audit of users’ actions with attribution.

The IC plans to increase access control to critical IC information resources, based on Data Protection Models in fiscal year 2011-2012. To that end, the IC CIO is standardizing a Data Protection Model based on current and evolving protection requirements and identity attributes. This approach will allow for several levels of protection; from open access through highly restricted availability. The appropriate protection level will vary based on factors such as data sensitivity, environment, mission criticality, and systems capabilities. Important elements in this approach include authentication techniques and the use of attributes (such as clearance level) to determine identities and support mission-based access to intelligence. Access control capabilities ensure that information content is only accessible by those individuals who possess the appropriate need, as validated by their management.

For higher levels of protection, technology can be used to control usage and limit user capabilities to perform activities such as copying, printing, or exporting data to a device. At this level, access requires strong user identification and authentication for system access along with the use of one or more attributes such as clearance level, digital identifier, role, or Community of Interest.

Data discoverability is another vital component to enable sharing while appropriately restricting access to information content. In the event that a user is inadvertently denied access to information needed to perform the mission, yet does not possess the appropriate attributes (for example clearance level, organization, or “Need to Know”), this capability will allow that user to discover the existence of, and request access to, the information.

Finally, audit and monitoring technologies are necessary to ensure that employees’ access to intelligence information is recorded and anomalies are detectable. Implementation of audit and monitoring technologies, by providing a reliable record of users’ actions, will support our ability to identify and react to apparently inconsistent activities, while also affording a means of deterring errant user behavior. During fiscal year 2012, the IC CIO will leverage an Enterprise Audit Framework to enhance the sharing of audit data across the IC elements.

In addition to these critical technologies – identity and access management, data protection and discoverability, and a reliable audit – the IC CIO continues to look at ways to leverage additional
technologies, such as digital management and data loss prevention, to find the “sweet spot” between sharing and protecting intelligence.

Conclusion

The IC is fully committed to giving policymakers, warfighters, law enforcement officers, and our other partners the best intelligence and analytic insight we can provide. This support is essential to enable all those we serve to make the decisions, and take the actions that will protect American lives and American interests, here and around the world.

To carry out that critical mission, it remains vitally important to both share and protect networks, intelligence, and associated information – and the systems and networks that support them. As we continue to increase sharing, we must also increase the protections put in place to heighten confidence that the intelligence and information that is being shared is being properly used and protected. This is a matter of managing risk; and people, policies, processes, and technology all play important and interconnected roles in managing that risk.

Appropriate policies must be aligned across many information sharing constituencies to include, federal, military, state, local, tribal, private sector, and international partners. These policies must also be consistent with the law, and appropriately address civil liberties and privacy concerns. Cultural attitudes and behaviors must reflect these priorities, and be shaped through appropriate training and incentives. Work on the next generation information sharing environment must begin now and be collaboratively developed with the IC and other stakeholder agencies.

Whether classified information is acquired via a computer system, a classified document, or simply heard in a briefing or meeting, we have had “bad apples” who have misused such information before and, unfortunately, we will see them again. That does not mean we should err on the side of not sharing intelligence or information – the risk caused by not sharing the information we have with those who need it is simply too great. Rather, we must put all proper safeguards in place, continue to be forward leaning to find the threat before disclosures occur, be mindful of the risks, and manage those risks in the light of the importance of our mission.
June 16, 2015

Privacy and Civil Liberties Oversight Board
General Services Administration
Regulatory Secretariat Division (MVCB)
ATTN: Ms. Hada Flowers
1800 F Street N.W., 2nd floor
Washington, DC 20405

Re: Notice PCLOB-2015-01, Comments on the Board’s Plan for Examination of EO 12333
Activities

To the members of the Privacy and Civil Liberties Oversight Board:

Thank you for the opportunity to submit comments on the Board’s plans to examine various
counterterrorism-related activities conducted under Executive Order (“EO”) 12333.

While declassified documents show that a large proportion of electronic surveillance activities
are conducted under EO 12333, little information about these activities is publicly available.¹
Our comments contain a list of questions and issues that we urge you to address during your
examination of EO 12333 activities. Answers to these questions will provide the public with a
much-needed understanding of how the government interprets and exercises its powers to
conduct electronic surveillance and other intelligence gathering activities under the Order.

Please note that when our comments mention the terms “acquire” and “collect,” these are not
used interchangeably. The U.S. persons’ procedures under EO 12333 have distinguished between
the acquisition or gathering of information on one hand, and “collection” on the other. For
example, the Department of Defense considers that “collection” occurs only when information

¹ NATIONAL SECURITY AGENCY, LEGAL FACT SHEET: EXECUTIVE ORDER 12333 (2013), available at
https://www.aclu.org/files/assets/foi12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf
has been “processed into intelligible form.” Accordingly, when we use the term “collect” or “collection” below, we are referring to the government’s definition of “collection.” When we use “acquire” or “acquisition”, we are referring to the ordinary process of gathering or obtaining a particular communication or piece of information.

Finally, while we understand that the Board intends to make public its overview of the legal framework established by EO 12333, we urge the Board also to seek declassification of its studies of two counterterrorism-related activities governed by EO 12333, with only those redactions that are truly necessary. In particular, the Board should do everything in its power to ensure that any analysis of applicable laws and statutes are made public.

### List of Issues and Questions Concerning EO 12333 Activities

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>QUESTIONS FOR OVERVIEW REPORT</th>
<th>QUESTIONS FOR IN-DEPTH REPORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General Legal Questions</td>
<td>Has the NSA, CIA, ODNI, DOJ, White House Counsel, National Security Council or any other federal agency or department created any opinion, memorandum or document analyzing: (1) Whether and how EO 12333 or activities conducted under it are consistent with the relevant provisions of the Constitution and/or statutory law; and (2) whether and how EO 12333 or activities conducted under it are consistent with the U.S.'s obligations under international law, including the ICCPR? Please seek declassification of all such documents, or at least the public release of a summary of the legal analysis contained in these documents.</td>
<td>Has the NSA, CIA, ODNI, DOJ, White House Counsel, National Security Council or any other federal agency or department created any opinion, memorandum or document analyzing whether and how the program under review is consistent with: (1) the relevant provisions of the Constitution and/or statutory law, and (2) international law? Please seek declassification of all such documents, or at least the public release of a summary of the legal analysis contained in these documents.</td>
</tr>
<tr>
<td>2. EO 12333 vs. domestic statutory authorities</td>
<td>Under what circumstances, if any, are communications and other data acquired inside the U.S. under EO 12333? If intelligence activities are carried out inside the U.S. under the Order, what are the rules governing such activities?</td>
<td>Does any part of the program under review acquire communications and other data within the U.S.? If so, what is the legal basis for such activity and what are the rules governing such activity?</td>
</tr>
<tr>
<td>3. Congressional Oversight</td>
<td>What does the congressional oversight regime for EO 12333 look like? For instance, how frequently are (a) the House Permanent Select Committee on Intelligence (&quot;HPSCI&quot;) and the Senate Select Committee on Intelligence (&quot;SSCI&quot;), (b) subsets of those committees, or any other committees or groupings of Congress (e.g., &quot;Gang of Four&quot; or &quot;Gang of Eight&quot;); and (c) Congress as a whole, briefed on surveillance activities conducted under EO 12333? What kinds of information about EO 12333 surveillance are shared only with HPSCI, SSCI or smaller groups of members? In cases where only</td>
<td>How has congressional oversight of the program under review functioned? In particular, how frequently are the members or relevant committees of Congress briefed on the program under review, and which members or committees are briefed? Is knowledge about the program under review restricted to HPSCI, SSCI or smaller groups of members? What are the kinds of reviews, assessments or investigations that HPSCI and SSCI have conducted, if any, to ensure that the program under review complies with the Constitution and any domestic or international</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>4. Funding</strong></td>
<td>HPSCI, SSCI or smaller groups have been briefed, how often have these committees or groups shared information with other members, and how have they done so? Has any committee, subset or grouping of Congress conducted any review, assessment or investigation of the constitutionality and/or legality of EO 12333 surveillance activities? What were their findings and conclusions? legal obligations? What action have HPSCI and SSCI taken, if any, to remedy or deter any privacy or legal violations arising from the program under review?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How does Congress allocate funds for intelligence activities conducted under EO 12333? Have these programs been audited, and what were the results?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How much funding is allocated to the program under review? Has the program been audited, and what were the results?</td>
<td></td>
</tr>
<tr>
<td><strong>5. Intelligence Outsourcing</strong></td>
<td>What kinds of intelligence activities conducted under EO 12333 are outsourced to private contractors? What rules and regulations are in place to ensure that these contractors respect privacy, civil liberties, and relevant U.S. and international laws when they conduct such activities? How is oversight of these contractors conducted? Have there been any instances of fraud, waste or abuse involving contractors that conduct such activities?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What role(s), if any, do private contractors have in conducting the program under review? What rules and regulations are in place to ensure that these contractors respect privacy, civil liberties, and relevant U.S. and international laws when they conduct activities under the program? How is oversight of these contractors conducted? Have there been any instances of fraud, waste or abuse involving contractors that conduct activities under the program?</td>
<td></td>
</tr>
<tr>
<td><strong>6. Internal Oversight</strong></td>
<td>How frequently is compliance with EO 12333 and relevant privacy procedures and policies reviewed internally (i.e., within the executive branch), and which entities perform such reviews? What is the nature and frequency of incidents of non-compliance, and what recommendations have the relevant oversight bodies made to prevent future incidents and to otherwise ensure respect for privacy and civil liberties? Have these recommendations been implemented, and if so, has their effectiveness been measured or studied? How do the President’s Intelligence Advisory Board (“PIAB”) and its</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How frequently is the program’s compliance with EO 12333 and relevant privacy procedures or policies reviewed internally (i.e., within the executive branch), and which entities perform such reviews? What is the nature and frequency of incidents of non-compliance, and what recommendations have the relevant oversight bodies made to prevent future incidents and to otherwise ensure that the program respects privacy and civil liberties? Have these recommendations been implemented, and if so, has their effectiveness been measured or studied? How do</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>Intelligence Oversight Board (&quot;IOB&quot;) conduct oversight of intelligence activities under EO 12333?</td>
<td>the PIAB and the IOB oversee the program under review?</td>
<td></td>
</tr>
<tr>
<td>7. Effectiveness</td>
<td>How is the effectiveness of intelligence activities conducted under EO 12333 assessed, which government entities conduct these assessments, and how frequently do such assessments occur? What metrics are used to measure effectiveness? Has any surveillance operation, program or activity under EO 12333 been terminated because it was deemed ineffective? Has there been any surveillance operation, program or activity that has yielded intelligence or information that could have been obtained using more targeted or privacy-protective methods?</td>
<td>How is the effectiveness of the program under review assessed, which government entities conduct these assessments, how frequently do such assessments occur, and what metrics are used? Could the intelligence or information obtained from the program under review have been obtained using more targeted or privacy-protective methods?</td>
</tr>
<tr>
<td>8. Acquisition vs. Collection</td>
<td>DoD 5240.1-R, the DoD's U.S. persons' procedures under EO 12333, considers data acquired by electronic means to be &quot;collected&quot; only when &quot;it has been processed into intelligible form.&quot; On the other hand, USSID 18, the NSA's signals intelligence directive, states that &quot;collection&quot; is the &quot;intentional tasking or selection of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.&quot; Are these definitions intended to have the same meaning? What does &quot;intelligible form&quot; mean? Can the Board provide examples of when &quot;collection&quot; takes place under these definitions?</td>
<td></td>
</tr>
<tr>
<td>9. PPD-28 and Information</td>
<td>How has the establishment of PPD-28 and the agencies' supplemental procedures affected how</td>
<td>How has the establishment of PPD-28 and the agencies' supplemental procedures affected how</td>
</tr>
</tbody>
</table>

3 Id.

<table>
<thead>
<tr>
<th>Acquistion and Collection</th>
<th>information is (a) acquired, and (b) collected under EO 12333? Although the ODNI has pledged that the Intelligence Community will no longer retain or disseminate information solely because of a person’s foreign status,(^5) there appears to be no similar limitation with respect to acquisition or collection. Are any agencies acquiring and/or collecting data under EO 12333 solely based on the foreign status of those targeted or affected?</th>
<th>information is (a) acquired, and (b) collected under the program under review? Does the program under review acquire and/or collect data under EO 12333 based solely on the foreign status of those targeted or affected?</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. “Bulk” collection vs. “targeted” collection</td>
<td>What percentage or proportion of EO 12333 surveillance operations or programs involve “bulk” (versus “targeted”) collection as defined under Footnote 5 of PPD-28?(^6)</td>
<td>Is the program under review a “bulk” or “targeted” collection program?</td>
</tr>
<tr>
<td>11. Joint information acquisition / collection efforts with foreign governments</td>
<td>What rules and regulations apply to intelligence gathering activities that are conducted jointly with foreign governments? A senior intelligence official has stated that the Intelligence Community cannot ask its foreign partners to spy on targets or communications it is legally prohibited to spy on, but acknowledged that it can accept information from other governments it cannot legally acquire or collect.(^7) If this is an accurate description, how does this principle work in practice?</td>
<td>What role, if any, do foreign intelligence agencies and other relevant foreign government entities have in acquiring, collecting, or processing information under the program under review? What rules and regulations are in place to ensure that the foreign entity respects privacy, civil liberties, and relevant U.S. and international laws when it conducts such activities under the program?</td>
</tr>
</tbody>
</table>


<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12. <strong>Search terms</strong></td>
<td>What types of search terms are used to acquire and/or collect information under EO 12333 (e.g. specific, known personal identifiers, names of organizations, geographical regions, general topics, terms that target communications because of their encrypted nature, etc.)? Which types of search terms are most commonly used, and how much information does each type of search term acquire and/or collect?</td>
<td>What types of search terms does the program under review use to acquire and/or collect information? Which types of search terms are most commonly used, and how much information does each type of search term acquire and/or collect?</td>
</tr>
<tr>
<td>13. <strong>Impact on U.S. persons’ communications</strong></td>
<td>To what extent do intelligence activities conducted under EO 12333 acquire and/or collect: (1) communications between U.S. persons and non-U.S. persons; and (2) wholly domestic communications between U.S. persons? Please request that the relevant agencies provide estimates, based on sampling if necessary.</td>
<td>To what extent does the program under review acquire and/or collect: (1) communications between U.S. persons and non-U.S. persons; and (2) wholly domestic communications between U.S. persons? Please request that the relevant agencies provide estimates, based on sampling if necessary.</td>
</tr>
<tr>
<td>14. <strong>Religious profiling</strong></td>
<td>Under what circumstances are an individual or organization’s racial, religious, or ethnic affiliation a relevant characteristic that may be taken into account in conducting intelligence collection under EO 12333? Has information collected under EO 12333 been used to map the demographics, travel, associations, and financial activities of Muslim, South Asian and Arab communities in the U.S.? What type of training do analysts and other personnel who conduct EO 12333 surveillance receive on these matters?</td>
<td>Have there been any incidents where the program under review was used to target individuals or organizations on the basis of their racial, religious or ethnic affiliation? What measures were taken, if any, to address the privacy and civil liberties violations arising from such incidents?</td>
</tr>
</tbody>
</table>
| 15. **Minimization** | What are the relevant minimization rules and how are they implemented in practice, and how have the rules and/or practice changed since the establishment of PPD-28? In particular, please address the following questions:  - The ODNI has pledged that the Intelligence | What are the rules for disseminating and retaining data acquired and/or collected under the program under review, and how are these rules implemented in practice? How much of the information collected under the program under review is deemed exempt from the default 5-year retention limit? How often has the relevant agency }
Community will no longer retain or disseminate information solely because of a person’s foreign status.\(^8\) The NSA’s PPD-28 Procedures expressly incorporate this limitation with respect to dissemination, but not retention.\(^9\) (In contrast, the CIA’s PPD-28 Procedures apply this limitation to both activities.)\(^10\) Could the Board clarify whether the NSA still asserts the authority to retain information solely because of a person’s foreign status?

- How has the principle that information will no longer be retained or disseminated based solely on a person’s foreign status been implemented? What additional criteria are used in deciding whether to retain or disseminate data?
- Does the executive branch adhere to the default 5-year retention limit established by Congress,\(^11\) and if so, how much of the information collected is deemed exempt from that default?
- How often do agencies mask or delete data before the 5-year retention limit is reached, and is this done before or after dissemination?
- Has non-U.S. persons’ data collected under masked or deleted data before the 5-year retention limit is reached? Has non-U.S. persons’ data collected under the program under review ever been minimized?

---

\(^8\) Supra, n. 5.
| 16. Use of EO 12333-collected information during criminal proceedings | Are there any criminal cases where prosecutors have relied on evidence (a) directly obtained or (b) derived from EO 12333 surveillance? How many of these cases exist, and how many or what proportion of them resulted in conviction? Can the Board make public statistics on how many of these cases concerned crimes other than those that are “likely to affect national security, defense or foreign relations of the United States” as defined in Section VII(A)(2) of the MOU on the Reporting of Information Concerning Federal Crimes? Are defendants notified when information obtained or derived through EO 12333 activities is used against them? | Are there any criminal cases where prosecutors have relied on evidence (a) directly obtained or (b) derived from the program under review? How many of these cases exist, and how many or what proportion of them resulted in conviction, and how many of these cases concerned crimes other than those that likely to affect U.S. national security, defense or foreign relations? |
| 17. Use of EO 12333-collected information during immigration and other proceedings | Are there any deportation or exclusion proceedings where the government has relied on evidence (a) directly obtained, or (b) derived from EO 12333 surveillance? How many of these cases exist, and how many or what proportion of them have led to deportation or exclusion? Are there any other kinds of legal or administrative proceedings where the government has relied on evidence directly obtained or derived from EO 12333 surveillance? Are parties to these proceedings notified when information obtained or derived through EO 12333 activities is used against them? | Are there any deportation or exclusion proceedings where the government has relied on evidence (a) directly obtained, or (b) derived from the program under review? How many of these cases exist, and how many or what proportion of them have led to deportation or exclusion? |
| 18. Use of EO 12333-collected information during | Has information obtained or derived from EO 12333 surveillance been used to support a targeted killing operation? How many or what proportion of targeted | Has information obtained or derived from the program under review been used to support a targeted killing operation? |

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>targeted killing operations</strong></td>
<td>Killing operations conducted by the U.S. have relied on information obtained or derived from EO 12333 surveillance?</td>
</tr>
<tr>
<td><strong>19. Information sharing with other agencies</strong></td>
<td>Do any agencies other than the collecting agency (e.g., the FBI or the DEA) have access to “raw,” unminimized EO 12333 data? If so, which agencies and under what circumstances? If not, when and how is processed information shared with other agencies?</td>
</tr>
<tr>
<td><strong>20. Information sharing with foreign governments</strong></td>
<td>What internal requirements exist for determining with whom data is shared, including how equities are weighed when sharing intelligence with governments that have a history of committing human rights abuses? What safeguards are included in information sharing agreements with foreign governments to ensure that the privacy of both U.S. persons and non-U.S. persons is adequately protected? Is the NSA, CIA, or any other element of the IC or USG aware of any human rights violations that were committed using information that was shared with the foreign government? Has information acquired/collected by U.S. intelligence been used in foreign prosecutions of U.S. persons?</td>
</tr>
</tbody>
</table>
SECTION 702 AND THE COLLECTION OF INTERNATIONAL TELEPHONE AND INTERNET CONTENT

LAURA K. DONOHUE

INTRODUCTION ................................................................. 119
I. THE EVOLUTION OF SECTION 702 .................................. 124
   A. The President’s Surveillance Program ...................... 125
   B. Redefinition of “Facility” under FISA .................... 128
   C. The Protect America Act ........................................ 135
   D. The FISA Amendments Act .................................... 137
      1. Section 702 .................................................. 139
      2. Sections 703 and 704 ....................................... 142
   E. Executive Order 12,333 ........................................... 144
      1. Shifting Communications and FISA Modernization ........ 147
      2. Executive Order 13,470 ..................................... 149
II. PROGRAMMATIC COLLECTION ....................................... 153
   A. Targeting .......................................................... 158
      1. Information To, From, and About Targets ............... 159
      2. Foreignness Determinations ................................ 165
      3. Foreign Intelligence Purpose Determination ............ 170
      4. Result of Statutory Interpretations ....................... 172
      5. Congressional Intent ......................................... 174
         a. Minimization and Explicit Limits .................... 174

* Professor of Law, Georgetown University Law Center. Thanks to Judge Morris Arnold, William Banks, Orin Kerr, and David Kris for comments on an earlier draft of this paper. This Article is Part Two of two-part series on NSA surveillance under the Foreign Intelligence Surveillance Act. For Part One, see Laura K. Donohue, Bulk Metadata Collection: Statutory and Constitutional Questions, 37 HARV. J.L. & PUB. POL’Y 757 (2014).
b. Potential Programmatic Collection
   As a Point of Opposition ................. 177
   c. Acquiescence.......................... 180

6. FISC Oversight of Targeting
   Procedures .................................. 190

7. Law as Written Versus Law as
   Applied .................................... 194

B. Post-Targeting Analysis .................... 195

C. Retention and Dissemination of Data ........ 199
   1. Retention of Encrypted
      Communications .......................... 199
   2. Use of Section 702 Data in Criminal
      Prosecution ............................ 202

III. FOREIGN INTELLIGENCE AND THE FOURTH
     AMENDMENT ................................ 202

A. Application of the Warrant Clause in
   the United States .......................... 206
   1. Criminal Law Versus Domestic
      Security .................................. 207
   2. The Domestic Foreign Intelligence
      Exception ............................... 211
   3. Concurrent Authorities .................. 214
   4. FISA Replacement of the Warrant
      Exception ............................... 216
   5. Recognition of FISA as a
      Constitutional Limit ........................ 219

B. Application of the Fourth Amendment
   Overseas .................................. 222
   1. Meaningful Contact as a Precursor ...... 223
   2. Limits of the Warrant Clause Abroad ... 231

C. Foreign Intelligence, Criminal
   Prosecution ............................... 237
   1. Lawful Seizure and Subsequent
      Search of Data ......................... 238
   2. Database Construction .................. 241
   3. Use of Data as Fourth Amendment
      Consideration .......................... 243
   4. Notice and Section 702-derived
      Evidence .................................. 245
      a. Criminal Law Standard ............... 246
b. Notice Under the FAA: Theory and Practice ........................................... 248
D. Reasonableness Standard .................................................. 252
  1. Criminal Law Versus National Security Law ............................................. 255
  2. Incidental Interception .................................................. 259
IV. CONCLUSION .......................................................... 263

INTRODUCTION

On June 6, 2013, the Washington Post and the Guardian captured public attention by reporting that the intelligence community was collecting large amounts of information about U.S. citizens. The National Security Agency (NSA) and Federal Bureau of Investigation (FBI) were “tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person’s movements and contacts over time.”

In conjunction with the articles, the press published a series of PowerPoint slides attributed to the NSA, describing a program called “PRISM” (also known by its SIGAD, US-984XN). The title


3. PRISM/US-984XN Overview, April 2013, available at https://www.aclu.org/files/natsrc/nsa/20130816/PRISM%20Overview%20Powerpoint%20Slides.pdf [http://perma.cc/F5JZ-2GMD] [hereinafter PRISM SLIDES]. A Signals Intelligence Activity Designator (SIGAD) is an alphanumeric designator that identifies a facility used for collecting Signals Intelligence (SIGINT). The facilities may be terrestrial (for example, connected to internet cables), sea-borne (for example, intercept
The central difference between Sections 703 and 704 is that, in certain respects, less specificity is required under the latter. The government need not assert that the information to be obtained cannot be garnered via normal investigative means. Section 704 also requires that FISC approve the minimization procedures only in regard to the dissemination of acquired information, as opposed to Section 703, which requires minimization procedures to be applied with regard to both acquisition and retention.

Unlike traditional FISA, which requires that applications identify the facilities to be searched or subject to electronic surveillance, and probable cause that the facilities are or will be used by the target, Sections 703 and 704 have no such equivalent. And unlike Section 702, under Sections 703 and 704 only the government is authorized to appeal the determination of FISC either to FISCR or to the Supreme Court.

E. Executive Order 12,333

In 1978, Congress excluded three types of foreign intelligence collection from FISA: (1) electronic communications outside U.S. borders, (2) intelligence in the U.S. and overseas falling outside the statutory definition of "electronic communications," and (3) incidental collection of U.S. persons' communications.

95. Note, however, that the same standard of probable cause is required.
99. See H.R. REP. NO. 95-1283(I), at 50 (1978) ("[T]his bill does not afford protections to U.S. persons who are abroad, nor does it regulate the acquisition of the contents of international communications of U.S. persons who are in the United States, where the contents are acquired unintentionally. The committee does not believe that this bill is the appropriate vehicle for addressing this area.") S. REP. NO. 95-701, at 7 & n.2, 34-35 & n.16 (1978). In 1978 the definition of "electronic surveillance" limited FISA to four types of collection. First, the acquisition of the contents of any wire or radio communication obtained by "intentionally targeting" a particular, known U.S. person located within domestic bounds. 50 U.S.C. § 1801(f)(1) (2012). Second, the acquisition of the contents of a wire communication to or from someone located in the United States, where the collection takes place on domestic soil. 50 U.S.C. § 1801(f)(2) (2012). Third, the intentional collection of the contents of some radio communications where "the sender and all intended recipients are located within the United States." 50 U.S.C. § 1801(f)(3) (2012). Fourth, the installation and use of other surveillance devices, on U.S. soil, directed at monitoring or acquiring information other than wire or radio communications. 50 U.S.C. § 1801(f)(4) (2012).
explained, "[T]he standards and procedures for overseas surveillance may have to be different than those provided in this bill for electronic surveillance within the United States or targeted against U.S. persons who are in the United States." At the same time, the legislature was careful to hedge. HPSCI noted, at least with regard to intelligence community activities abroad:

The fact that S.1566 does not bring the overseas surveillance activities of the U.S. intelligence community within its purview . . . should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans. The committee merely recognizes at this point that such overseas surveillance activities are not covered by this bill.101

Instead, the framing for these foreign intelligence collection activities (foreign-to-foreign electronic communications, foreign intelligence collection at home and abroad outside of FISA's definition of "electronic communications," and the incidental collection of U.S. persons' communications) came from Executive Order 12,333.102 Issued by President Reagan in 1981, this order required each agency to establish procedures, approved by the Attorney General, to govern collection methods.103

The order offered heightened protections for U.S. persons. It required that the Attorney General "approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes."104 Surveillance could only be undertaken where the Attorney General had "determined in each case that there [was] probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power."105 For the military, for instance, to engage in foreign intelligence collection on U.S. persons, an application to the Attorney General must be made consistent with DOD

101. Id.
103. Id.
104. Id. at § 2.5.
105. Id.
regulations. Procedural procedures adopted in the early 1980s required that
the applicant include a statement of facts demonstrating probable
cause and necessity, as well as the period for which surveillance
was being sought.

All electronic surveillance had to take place consistent with
FISA and Executive Order 12,333. The order directed the intelligence
community to “use the least intrusive collection techniques feasible
within the United States or directed against United States
persons abroad.” The physical surveillance of U.S. persons
overseas for foreign intelligence purposes, in turn, could only be
conducted where the purpose was “to obtain significant infor-
mation” that otherwise could not reasonably be acquired.

The order included institutional protections. It prohibited the
CIA from conducting electronic surveillance within domestic
bounds (outside of counterintelligence investigations of military
personnel). Within the United States, the FBI had the lead,
“provided that no foreign intelligence collection by such agencies
may be undertaken for the purpose of acquiring information con-
cerning the domestic activities of United States persons.” And
all domestic physical surveillance of U.S. persons had to be under-
taken by the FBI.

One of the chief complaints of the Bush Administration that
spurred the introduction of the PAA and, subsequently, the FAA,
was that changes in telecommunications technologies meant that
communications that had previously fallen under the less restric-
tive contours of Executive Order 12,333 had gradually been
brought within FISA. In 2006, the Director of National Intelli-
gence, Admiral Mike McConnell, argued that, as a result, the in-
telligence community was not collecting some two-thirds of the

106. U.S. Dep’t of Def. Dir. 5247.1-R, Procedures Governing the Activities of DOD
Intelligence Components that Affect United States Persons, Proc. 5, Pt. 2.3 (1982).
107. Id.
109. Id. at § 2.4.
110. Id. at § 2.4(d).
111. See id. at § 2.4(a). The order also excepted searches of non-U.S. person
property lawfully in the CIA’s possession. Id. at § 2.4(b)(2).
112. Id. at § 2.3(b).
113. See id. at § 2.4(c). But note the exception of government employee-related
investigations. Id.
foreign intelligence information that it had collected before. The resulting FAA supplanted Executive Order 12,333, in some ways, with a statutory framing. In other ways, it left the existing 12,333 authorities intact. The end result is relevant to analyzing the scope of the FAA and the NSA’s programs under Section 702.

1. Shifting Communications and FISA Modernization

The arguments put forward in support of modernizing FISA are of varying strength. The strongest claim relates to the nature of e-mail communications. Congress explicitly exempted foreign-to-foreign wire communications from FISA’s remit. The exclusion made sense: the voice transmission of a British subject in London, calling a French citizen in Paris, at no point crossed U.S. borders. It would be impractical and cumbersome to expect the intelligence community to obtain court approval for every interception of foreign intelligence between foreign nationals overseas. By grounding the exception in territorial limits, Congress thus acted consistently with Fourth Amendment doctrine—reserving, in the process, the potential to act where U.S. persons’ privacy might be at stake.

The same types of communications exempted from FISA, however, in the modern age of e-mail, had begun to fall within traditional FISA. For instance, U.S. Internet Service Providers (ISPs) store e-mail on servers in the United States. The same British subject, if she accesses her email from London (pulling it from a server within the United States), suddenly falls within FISA—even when the e-mail she is retrieving is sent by the same French citizen in Paris. In other words, merely by using an American ISP,

non-citizens could obtain the protections of the more rights-
protective FISA framework—even where such persons had no
other ties to the United States and presented a classic foreign in-
elligence threat (and would otherwise be covered by the less rigor-
ous contours of Executive Order 12,333). Exacerbating the prob-
lem was the difficulty of determining where the user was
located—inside the U.S. or on foreign soil—a consideration cru-
cial to determining whether the intelligence community must first
approach FISC for an order.

The other two arguments put forward in support of moderniz-
ing FISA were less robust. First, the government argued that the
transition from satellite to fiber optic cables for trans-oceanic
communications meant that international communications, pre-
viously carried by radio waves (exempted from FISA unless the
target was a particular, known, U.S. person on domestic soil),
began to fall within FISA’s wire communications provisions.117
While accurate in its assertion that fiber optic cable commu-
nications came within FISA’s remit, it was an exaggeration to say
that Congress did not expressly contemplate this in 1978. The Com-
mittee explained at the time: “It is the committee’s intent that ac-
quision of the contents of a wire communication, without the
consent of any party thereto, would clearly be included” in the
definition of “wire communication.” It continued, “Excluded
would be . . . commercial broadcasts, as well as ham radio and
citizen band radio broadcasts.”118 Also exaggerated was the claim
that most communications at the time of FISA’s enactments were
carried on radio waves, as opposed to fiber optic cables.119 The
government further over-emphasized the change in terms of the
trend.120

Second, the government argued that the difference of a mile
or two should not matter with regard to whether the U.S. inter-
cepted communications offshore or within U.S. borders.121 The
intelligence community might need the assistance of a U.S.

117. KRIS & WILSON, NSIAP, § 16.3.
119. See KRIS & WILSON, NSIAP, § 16.3, citing § 16.4 (“A review of telecommunica-
tions history . . . shows this claim to be exaggerated: the transition from satellite to
cable was neither as dramatic, nor as unanticipated, as the government argued.”).
120. Id.
121. For discussion of this point, see KRIS & WILSON, NSIAP, § 16.5.
company. The location of the actual intercept was a matter of accident, not design—and entirely outside the government's control. The location turned on where the company had chosen to concentrate the flow of traffic. So, where previously the wiretap offshore would not trigger the protections of traditional FISA, the same wiretap just inside US borders would—even where the same conversation or communication was being obtained. The problem with this argument is that it was precisely the point of FISA to draw a line at the border of the country. Trying to move that line a matter of feet and call it a day fell short of understanding the point of the statute.

In light of all three arguments, Members of Congress began to focus on the need to "modernize" FISA.\textsuperscript{122} The FAA, however, still only reaches electronic communications as defined in FISA. Other forms of foreign intelligence collection continue to be governed by executive order.

2. **Executive Order 13,470**

Executive Order 12,333 has thrice been amended.\textsuperscript{123} The most recent, in July 2008, drew attention to areas outside the traditional foreign intelligence emphasis.\textsuperscript{124}

The new order emphasized that intelligence collection should be conducted in a manner consistent with the intelligence priorities set by the President, with "[s]pecial emphasis" given to detecting and countering not just espionage, but "[t]hreats to the

\textsuperscript{122} See, e.g., 154 CONG. REC. S6379 (daily ed. July 8, 2008) (statement of Sen. Cardin) ("Congress must indeed make needed changes to FISA to account for changes in technology and rulings from the FISA Court involving purely international communications that pass through telecommunications routes in the United States."); 154 CONG. REC. H5759 (daily ed. June 20, 2008) (statement of Sen. Blunt) ("We modernized the law to adapt to changes in technology since the 1978 FISA statute. The bill would accomplish all this while adding new protections and strengthening the individual liberties and privacy protections of Americans."); 154 CONG. REC. H5767 (daily ed. June 20, 2008) (statement of Rep. Pelosi) ("[W]e all recognize the changes in technology necessitate a change in the legislation, and this legislation today modernizes our intelligence-gathering system by recognizing and responding to technological developments that have occurred since the original FISA Act in 1978.").


United States and its interests from terrorism; and [t]hreats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction."125 The amendments directed the intelligence community to take into account state, local, and private sector responsibilities and requirements "when undertaking the collection and dissemination of information and intelligence."126 In addition, the new order incorporated the Director of National Intelligence into the intelligence infrastructure.127

Some of the language signaled a shift in how the NSA would be using its authority under the FAA. Where previously the order prohibited the dissemination of unminimized Signals Intelligence (SIGINT) pertaining to U.S. persons, the new order allowed dissemination subject to procedures developed by the DNI in coordination with the Secretary of Defense and approved by the Attorney General.128 This change enabled other agencies to obtain SIGINT to ascertain whether the information could be kept, at which point it becomes subject to that agency’s U.S. person rules (pursuant to the first part of Executive Order 12,333, Section 2.3).129 The sharing and evaluation of unminimized SIGINT data thus appears to create an internal process that can be thought of as a form of intelligence "discovery." Although the previous order required that intelligence be collected in a manner consistent with the restrictions in FISA and Executive Order 12,333, the amendments only required that information be collected subject to restrictions in FISA.130 This change made a differ-

125. Id. at § 2, Pt. 1.1(d).
126. Id. at § 2, Pt. 1.1(f).
127. See id. at § 2, Pts. 1.3–1.6.
129. The relevant DNI/DOD/AG procedures, if they have been developed, have not been declassified.
130. Compare Exec. Order No. 12,333, 3 C.F.R. 200, § 2.5 ("Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.")., with Exec. Order No. 13,470, 73 Fed. Reg. 45,325, § 3(y) (deleting sentence quoted in prior citation and replacing with: "The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.").
ence. The FAA, for instance, amended FISA to allow for U.S. person data to be retained to protect life and property, and for the NSA to retain encrypted communications. Under Executive Order 12,333’s more general guidelines, these practices would not have been allowed; however, they appear now to fall within the scope of intelligence agencies’ authorities.

Some of the regulations implementing Executive Order 12,333 have been made publicly available. But many of the guidelines, and the programs conducted under the order, remain veiled from public scrutiny. Even Congress has limited view. Although the procedures approved by the Attorney General under the order must be provided to the Congressional intelligence committees, SSCI Chairman, Senator Dianne Feinstein, has acknowledged that the committee does not conduct extensive oversight of intelligence gathering conducted under the order’s auspices.

The Snowden documents provide some detail on different ways in which the order appears to be interpreted and used. Accessing social network data or stored information (for example, address book contacts, “buddy lists,” and draft e-mails) may fall within Executive Order 12,333, insofar as FISA does not apply.


132. Exec. Order No. 12,333, 3 C.F.R. 200, § 3.3.


134. For slides detailing collection of this data and released by Edward Snowden, see Barton Gellman & Matt DeLong, The NSA’s Problem? Too Much Data,
For example, Section 703 applies to stored electronic data acquired in the United States in the process of targeting U.S. persons overseas. It would thus cover the acquisition of U.S. persons’ buddy lists on U.S. soil. FISA would not, however, govern the overseas acquisition of buddy lists of non-U.S. persons located abroad. This acquisition would come within Executive Order 12,333. Similarly, to the extent that social network information, such as Instagram postings, fall outside FISA’s definition of electronic surveillance or stored communications, regardless of whether a U.S. person is located inside or outside the country, collection would be governed by the weaker restrictions of Executive Order 12,333.

These other types of programs can potentially yield significant amounts of information. The NSA appears to be collecting e-mail address books for most major webmail companies, and storing the information in multiple databases. According to the Washington Post, the yield is “hundreds of millions of contact lists from personal e-mail and instant messaging accounts around the world.” On any representative day, in turn, the NSA appears to collect approximately half a million buddy lists and inboxes (which frequently include the first part of the messages that have been sent).

Another example of collection under Executive Order 12,333 is the interception of content flowing between data centers overseas. In October 2013, the Washington Post reported that the NSA was collecting hundreds of millions of records, ranging from metadata to content, transiting fiber optics cables between Google and Yahoo data centers. The principal tool used to analyze the infor-

136. See Gellman & DeLong, supra note 134, at slide on p. 3. MARINA centers on Internet metadata; MAINWAY focuses on telephone metadata for contact chaining; and PINWALE concentrates on written content. Id.
139. Gellman & Soltani, NSA Infiltrates Links, supra note 133.
mation, MUSCULAR, appears to be operated jointly with the U.K.'s Government Communications Headquarters (GCHQ). The collection of information held on the cloud, outside U.S. borders, shifts the program outside the FISA framework.

With GCHQ in mind, it is worth noting an additional exception to both FISA and Executive Order 12,333: to the extent that it is not the United States engaged in the collection of information, but, rather, one of our allies, rules that otherwise limit the U.S. intelligence community may not apply. From the language of the order, it appears that the United States may receive or benefit from other countries' collection of information on U.S. citizens, where it does not actively participate in the collection or specifically request other countries to carry out the collection at its behest. In turn, the United States can provide information about foreign citizens to their governments that their intelligence agencies, under their domestic laws, might otherwise be unable to collect. To the extent that the programs underway are extended to the dosely allied “Five Eyes” (Australia, Canada, the United Kingdom, the United States, and New Zealand), structural demarcations offer a way around the legal restrictions otherwise enacted to protect citizen rights in each region.

II. PROGRAMMATIC COLLECTION

Almost immediately after passage of the FAA, members of Congress, scholars, and others began criticizing Section 702 be-

140. Id.
141. Id.
142. The order states with regard to indirect participation, “No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.” Exec. Order No. 12,333, 3 C.F.R. 200, § 2.12 (1982), as amended by Exec. Order No. 13,470, 73 Fed. Reg. 45,325, § 3(ii) (July 30, 2008). This prohibits the intelligence community from actively participating in collection, or requesting other countries to engage in collection, outside the confines of the order; however, it does not appear to prohibit the intelligence community from simply receiving or benefiting from other countries’ actions in this regard.

143. By “programmatic collection” I refer to a method of collection involving indiscriminate surveillance. The scanning of e-mail communications for reference to selectors, targets, or key words, is thus programmatic. It is not limited to the communications of particular individuals but, rather, monitors the communications of all individuals passing through particular points.
cause of the potential for the government to use the authorities to engage in programmatic surveillance.\textsuperscript{144}

In 2009 prominent national security law Professor William Banks explained, “the FAA targets do not have to be suspected of being an agent of a foreign power or, for that matter, they do not have to be suspected of terrorism or any national security offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance.”\textsuperscript{145} Surveillance could be directed at a person, organization, e-mail address, or even “an entire ISP or area code.”\textsuperscript{146} He noted, “the surveillance permitted under the FAA does not require that the Government identify a particular known facility where the intercepted communications occur.”\textsuperscript{147} These provisions represented a sea change from how FISA had previously worked (albeit introducing, for the first time, statutory restrictions in an area previously governed by Executive Order). U.S. persons’ communications now could be incidentally collected under the statute, on a large scale, without many of the protections in traditional FISA.\textsuperscript{148}

Banks presciently pointed out the most likely way in which the new authorities would be used:

Although details of the implementation of the program . . . are not known, a best guess is the Government uses a broad vacuum cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then the NSA engages in a more particularized collection of content after analyzing mined data . . . [A]ccidental or incidental acquisition of U.S. persons inside the United States [will] surely occur[, especially in light of the difficulty of ascertaining a target’s location.\textsuperscript{149}

For Professor Banks, part of the problem was that the nature of international information flows meant that it would be impossible

---

\textsuperscript{144} See, e.g., Banks, supra note 52.
\textsuperscript{145} Id. at 5013–14.
\textsuperscript{146} Id.
\textsuperscript{147} Id.
\textsuperscript{148} Id. at 5014.
\textsuperscript{149} Id. at 5014–15.
THE STATE OF PLAY: RETOOLING UNCLE SAM SINCE 9/11

MODERATOR:
JOEL BRENNER
Forty Years After Church-Pike: What’s Different Now?

This is the Henry F. Schorrack Memorial Lecture that I delivered at the National Security Agency

May 15, 2015

About ten years ago, when I was the inspector general here, I found myself one day in Hawaii, under the Pineapples, and by coincidence there was at the same time a conference nearby of the agency’s training staff from all over the Pacific region. And one of them came to me and said, We do all this training about the legal restrictions on our activities — USSID 18 and Executive Order 12333 and all that — and we know it’s a big deal, but none of the people we’re training know why we’re doing it. And then after a pause she said: And frankly, we’re not sure either.

I had lived through the upheaval of the late ‘sixties and the ‘seventies – the Vietnam War, the intelligence scandals, the Nixon impeachment, and the implementation of the legislative and regulatory framework that we impliedly refer to every time we say that this agency operates under law. Younger people had not.

We Americans don’t take instructions well if we don’t understand the reasons for them. And so I decided it was incumbent on us to tell and re-tell the story of how and why the United States became the first nation on earth to turn intelligence into a regulated industry. But the story isn’t entirely behind us. It continues. And so this morning I’m not only going to recount what happened in the ‘seventies; I’m also going to address the Agency’s position in the wake of the Snowden leaks, and how we got here. Because insofar as NSA has again been in the public’s doghouse (It is certainly not in the policymakers’ dog house), it is for very different reasons from those in 1976, and that difference is worth reflecting on.

Let’s go back to January 1970, when a former Army captain in military intelligence, Christopher Pyle, disclosed in the Washington Monthly that the U.S. Army intelligence had more than a thousand plainclothes agents surveilling every significant political demonstration in the United States.[2] According to Pyle’s account, the Army kept “files on the membership, ideology, programs, and practices of virtually every activist political group in the country . . . including . . . the Southern Christian Leadership Conference, Clergy and Laymen United Against the War in Vietnam, the American Civil Liberties Union, Women Strike for Peace, and the National Association for the Advancement of Colored People.”[3] It also kept a “Blacklist” of “people who might cause trouble for the Army.”[4] There had been violent, destructive race riots in Los Angeles in 1965, in Detroit in 1967, and then in April 1968 in Washington after Rev. Martin Luther King, Jr. was assassinated. Two months later, Bobby Kennedy was assassinated. That same year, the Soviet Army moved into Prague, the Fifth Republic in France nearly fell as a result of massive domestic unrest, and Chicago during the 1968 Democratic National Convention
was the scene of serious street violence. Lest anyone forget, we were also deep in the Cold War, early in the Brezhnev years, and the antiwar movement unquestionably included a small but violent far-left element. Stability was a genuine concern of sober people.

The scope of the Army’s domestic spying was nevertheless unauthorized in law, out of control, and plainly political. In the Army’s eyes, dangerous people included Coretta Scott King, Georgia State Representative Julian Bond, folk singer Arlo Guthrie, and former military officers who opposed the Vietnam War. In Colorado Springs, the leader of a church youth group attended a peaceful antiwar protest; in response, the Army infiltrated his church. In Kansas City, the Army asked local high schools and colleges to turn over the names of ‘potential trouble makers’ and anyone who was ‘too far left or too far right.’” Classroom statements by teachers and students found their way into police and Army files.[5] Based on Pyle’s account, Senator Sam Ervin, a conservative southern Democrat from North Carolina and chairman of the Senate Judiciary Committee, opened hearings, but they ran into a wall because the Executive Branch, citing executive privilege and “national security,” declined to provide much information. This episode nevertheless opened the first, small wedge into a system of government secrecy that had been little questioned since 1941.

The Army hearings were not the beginning of the American public’s distrust of government, but by 1970, trust was running out on a strong ebb tide. Just to color the picture a bit brighter, in April 1970, the United States secretly expanded the Vietnam War into Cambodia, but the operation was leaked and produced vehement opposition. On May 4, frightened and undisciplined Ohio National Guard troops fired into a crowd of student demonstrators at Kent State University, killing four and wounding nine. In July, a cabal of radicals blew up the Army Math Research Center at the University of Wisconsin, killing a graduate student. The Weather Underground planned further bombings.

The sense of anxiety and pessimism was profound, and lots of people really did seem to believe, as the song said, that we were on the eve of destruction. (That song was actually written in 1964, but it had long legs.)

On December 22, 1974, the New York Times published a front-page story by Seymour Hersh about a CIA program called “family jewels.” It began this way:

The Central Intelligence Agency, directly violating its charter, conducted a massive, illegal domestic intelligence operation during the Nixon Administration against the antiwar movement and other dissident groups in the United States, according to well-placed Government sources.

An extensive investigation by The New York Times has established that intelligence files on at least 10,000 American citizens were maintained by a special unit of the C.I.A. that was reporting directly to Richard Helms, then the Director of Central Intelligence . . .

This article is worth your reading, or re-reading after forty-one years – and not only for the mood of the country and the revelations themselves. It also lays out the unbelievably bad blood between the FBI and the CIA and the intentional freezing of cooperation between them. The seeds of the next generation’s intelligence problem were there to see, unnoticed in plain view.
Just two weeks after Hersh’s article, in January 1975, the Senate convened a Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church of Idaho. The Committee’s work had support from both sides of the aisle. A similar committee convened in the House under Rep. Otis G. Pike of New York, but the Senate version under Church was the more significant. It published fourteen reports in 1975-76 on intelligence agency activities, probably the most such comprehensive reports in history, in any country. The reports detailed the CIA’s habit of opening our mail, NSA’s domestic interception programs, and CIA’s human subject research – including a notorious instance of LSD administered to an unwitting subject who, in a hallucinating fit, jumped out a window to his death. They also went deeply into intelligence activities overseas as well as at home, disclosing assassination plots against the Diem brothers of Vietnam, Patrice Lumumba in the Congo, General René Schneider in Chile, and Rafael Trujillo in the Dominican Republic, as we as the failed plan to use the Sicilian Mafia to kill Fidel Castro. Coups against the governments of Arbenz in Guatemala and Mosadegh in Iran were also exposed.

The country was stunned by the systematic domestic surveillance, and shocked to learn that assassination was a tool of American foreign policy. It was as if we Americans had eaten of the fruit of the Tree of Knowledge. We had lost our innocence and the belief in the purity of our methods as well as our intentions.

Revelations about the FBI were, if possible, even more stunning. For 17 years, from 1956 to 1973, the Bureau under J. Edgar Hoover had run a covert program called COINTELPRO, for Counterintelligence Program. It had antecedents at least back to World War I. Its initial purpose was to assess the activities of the Communist Party of the U.S., but it eventually included surveillance of Senators Howard Baker and Church (who were the ranking member and chairman of the Senate Foreign Relations Committee), the women’s movement, nearly all groups opposing the Vietnam War, Albert Einstein, and many civil rights leaders. Hoover loathed Martin Luther King, Jr., and after the March on Washington in 1963, he called King “the most dangerous Negro of the future in this nation from the standpoint of communism, the Negro, and national security.” The FBI systematically bugged King’s home and hotel rooms. By the way, much of the surveillance was personally approved by Attorney General Robert F. Kennedy – who later discovered he too had been a target of FBI surveillance.

On November 21, 1964, the FBI sent an anonymous package to King that contained audio recordings of his sexual indiscretions together with a letter that said: “There is only one way out for you. You better take it before your filthy, abnormal, fraudulent self is bared to the nation.” The FBI was encouraging King to commit suicide.

Hoover, by the way, was regarded by several presidents as too powerful to remove from office because he was known or believed to have dossiers on them with embarrassing information.

NSA, meanwhile, was running two projects called SHAMROCK and MINARET. SHAMROCK began in August 1945 – the month Japan surrendered – and involved the collection by NSA’s predecessor, the Armed Forces Security Agency and then by NSA, of all telegraphic traffic entering or leaving the United States. Western Union, RCA, and ITT gave the agency direct daily access to microfilm copies of this traffic – up to 150,000 messages per month. There was
wartime precedent for this, but the scope of the collection, and its conduct in peacetime, was a different story.

MINARET was a related project by which NSA intercepted electronic communications of 1,650 people who were on a watch list. There were no warrants and no judicial oversight of these activities, which were simply assumed to be the normal activities of a foreign intelligence agency. The targets included Senators Church and Baker, many critics of the Vietnam War, King, Whitney Young, Muhammad Ali, Tom Wicker of the New York Times, and Washington Post columnist Art Buchwald. After the Church Committee disclosed these programs, then-NSA Director Lew Allen shut them down. The director’s testimony before the Committee was the first time since NSA’s founding in 1952 that any director had publicly testified before Congress; it was also the first time that NSA’s existence was publicly acknowledged. Before then, NSA really did stand for “No Such Agency.” (Now it stands for “Not Secret Anymore.”)

I think it fair to say, and important to say, that everyone associated with these various programs thought that he was a patriot acting in the national interest. Which is precisely why subjective notions of patriotism and national security are insufficient guides for people and agencies that claim to operate under law in a democratic republic. (Snowden and Hoover actually represent converse instances of unmoored, egotistical arrogance to oneself of the right to determine the public good. The comparison will annoy their respective admirers. So much the better. They should think about it.)

The Church-Pike hearings were watershed events in our nation’s history, psychologically as well as politically, and they led directly to the legal structures you operate under today. President Ford’s Executive Order 11905, later modified and reissued by President Reagan as E.O. 12333 in substantially the form we now know it; the creation of the House and Senate permanent select committees on intelligence; the Foreign Intelligence Surveillance Act of 1978; the Inspector General Act of 1978; and USSID 18 (originally issued in 1980) – not to mention drastic budget cuts in intelligence – all these were the direct product of the Church-Pike hearings and reports.

Because of the hearings whose anniversary we celebrate today, the men and women of the intelligence community operate with a profoundly different mindset. You take orders from a democratically elected government, and you answer to an independent judiciary. This is the “why.” This is the answer to the question put to me that day in Hawaii. This is the history we must teach to our successors.

I’m glad to say that NSA did not repeat the mistakes of the period that led to the Church-Pike hearings. Okay, then, so how did we get in the doghouse this time?

The seed of the problem was planted shortly after 9/11, when the White House determined to undertake certain collection outside the FISA regime under a highly classified, but now mostly declassified, program called STELLAR WIND. That program was not SAP’ed, because the creation of a new special access program requires Congressional notification, but it was run directly by the Office of the Vice President and put under the direct personal control of the Vice President’s counsel, David Addington. Under periodically renewed Presidential orders, NSA collected two kinds of intelligence: First, the contents of communications between a person
outside the United States with a known connection to Al Qaeda or certain affiliated organizations, and a person inside the country; and second, bulk metadata in order to chain off the domestic link. In my judgment, any President who had failed to order such surveillance on an emergency basis immediately after 9/11 would have been derelict. The President’s first duty is to protect the nation, and the fear of further attack was palpable. You could smell it. But under statute, the interceptions were not permissible without a FISA order because they were taken from a wire inside the United States; and FISA did not permit metadata collection at all. Under prevailing law, metadata, which is analogous to the information on the outside of a mailed envelope, may have had no Constitutional protection. But the bulk collection of that data was a watershed political event in the history of American intelligence and in American politics. As an emergency matter, there’s no question in my mind that the President had the power under Article II of the Constitution to order this collection – both kinds. But how long does an emergency last? (An emergency usually doesn’t come with a specific expiration date like a quart of milk, but claims of emergency do get sour.)

Now, it was the view in the White House that the President did have the power to collect this intelligence on a permanent basis. And I am persuaded that the White House, and certainly the Office of the Vice President, believed that FISA was an unconstitutional limitation on the President’s Article II power in all circumstances. This was an odd view, because Article I, Section 8 of the Constitution gives Congress the power to regulate interstate and foreign commerce, and that includes telecommunications. Under well-settled law, Congress cannot exercise its power in a manner that makes it impossible for the Executive to carry out its Constitutional duties, but it can regulate that exercise in a reasonable manner.

Both the NSA General Counsel at the time, Bob Deitz, and I looked for guidance in this situation to one of the more famous passages of Twentieth Century Constitutional law, and I’m going to read you a short bit of it. It’s by Justice Robert Jackson, concurring in the Supreme Court’s decision striking down President Truman’s seizure of the steel mills on national security grounds. Jackson is talking about Presidential power in a divided government and the point at which law and politics cannot be separated. The President’s power fluctuates, Jackson observed, depending upon Congress’ exercise of its power. He saw three possibilities:[7]

1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate.

1. When the President acts in the absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. ...In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law.

1. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb ....
In my view, President Bush’s STELLAR WIND orders fell into the third category – at least, I thought they did after some fairly brief but indeterminate emergency. (This was not the Administration’s view. They thought the Authorization for Use of Military Force impliedly granted the power to implement STELLAR WIND. That was a serious argument, but it was based on debatable inferences; so even accepting that view, I thought the President was in the twilight zone.) You may know that after President Lincoln unilaterally suspended *habeas corpus* during the Civil War on the grounds that it was necessary to save the Union, he went to Congress to get his action ratified. President Bush chose not to do that. So I put the question to NSA’s senior leadership: Why don’t we amend FISA, which we could easily have done in the aftermath of 9/11, and do this collection under statute? This was actually an academic question, because policy was being driven, and driven hard, by Addington, who detested the FISA statute. “We’re one bomb away from getting rid of that obnoxious [FISA] court,” he would say. But the answer I got here at the Fort was interesting. It was that amending FISA would require a public debate; that the public debate would educate our adversaries; and that we would lose intelligence as a result. My response was that the program could not be kept secret forever, and that its eventual disclosure would create a firestorm and divide the country. The broad unity of the country behind the agency’s activities was a strategic asset; the loss of collection was likely to be tactical and temporary; and sacrificing a strategic asset for tactical advantage was as foolish in politics as it is in military operations. Better, I said, to amend the statute. But Inspectors General do not make policy, and they are not consulted about it, nor should they be.

Sooner or later this program’s cover was going to be blown, and on December 16, 2005, it happened: The *New York Times* exposed the interception part of the program (but not the bulk metadata portion), amid accusations that NSA was engaged in “domestic” spying because it was intercepting communications involving Americans. In my view that was a distorted description, but when you’re explaining, you’re losing. This was the beginning of a shift in public opinion that until then had, on the whole, been highly supportive of our intelligence agencies. Suddenly we faced a country that was seriously divided about our activities.

Most of the criticism actually had little to do with the merit of the interceptions, just the authority for it. Nor surprisingly, the inflammatory publicity attendant on the STELLAR WIND disclosure and the resulting damage to actual collection, to NSA’s reputation, and to our public support were far greater than any damage that would have occurred if the program, and the reasons for it, had been publicly discussed at the outset and the FISA statute amended.

Ladies and gentlemen, democracies distrust power and secrecy and are right to do so. Intelligence agencies are powerful and secret. Tosquare that circle, two conditions must be met: The rules under which they operate must be clear to the public and authorized by law, and the public must have reason to believe that the rules are being followed. STELLAR WIND failed to meet those requirements, and NSA paid for it in loss of public trust.

Again, a lesson was learned – but imperfectly. FISA was amended in 2008, but only after a rancorous public debate, and the statute is frankly a bit of a mess. Still, you follow that statute.

And then in 2013 came Mr. Snowden. Overseas, people were stunned to learn how extremely good NSA really is at its business – sometimes at their expense. You were being criticized for
being too good. And of course the dough of outrage rose higher and higher when leavened with the yeast of hypocrisy.

But why did the Snowden leaks hurt so badly here in our own country? There hasn’t been even a whiff of intelligence abuse for political purposes. This was the only intelligence scandal in history involving practices approved by Congress and the federal courts and the President, and subject to heavy oversight. How did this happen?

The answer, I think, goes back to the power-and-secrecy principle and to the evolution of our representative democracy in the digital age. NSA was operating under statute – but ordinary, intelligent, educated Americans could not have looked at that statute and understood that it meant what the FISA Court interpreted it to mean. The intelligence committees knew. Any member of Congress who wanted to know either did know or could have known. (I discount the hypocrisy from that quarter, and the Second Circuit Court of Appeals’ opinion last week is just wrong about that.) But it is true that the FISA Court’s expansive interpretation of the law was secret. So the argument that the Agency was operating under “secret law” had legs with the public, much of which is allergic to bulk collection and doubts its value.

We had amended FISA, yes, but our leaders had failed to absorb the transparency lesson. You now live in a glass house. How could anyone think the bulk collection program would remain secret? I’m not telling you there are no more secrets. You still have plenty of them. I am telling you that with instantaneous electronic communications, secrets are hard to keep; and that which can be kept secret does not stay secret for long. The idea that the broad rules governing your activities – not specific operations, but the broad rules – can be kept secret is a delusion. And they should not be kept secret. Leaders who do not understand this will continue to make strategic blunders. I do not state this as a policy preference. I state it as a fact of life that political leaders and intelligence agencies – I mean you – must take into account as you make decisions about what can be, and should be, kept secret – and about what activities you can and should undertake.

I should note that even if the general counsel or the Director had given different advice to President Obama about bulk collection, it would not have been followed. The fight in 2008 was bruising enough. The White House had no appetite for more FISA battles. In any case, that was the President’s call – not the Director’s. The Director was on the right side of the law. Would the program be unpopular? Maybe. But we do our work. We keep our heads down. Sometimes we take some punches for it. Besides, there’s always a political faction that doesn’t like us no matter what. Tough luck. If it’s legal, we do our work.

But in retrospect there’s a lesson to learn. The public, not just the three branches of government, must know what kinds of things we are allowed to collect domestically.

If you disagree with me on this, do your own damage assessment. In the wake of Snowden, our country has lost control of the geopolitical narrative; our companies have lost more than $100 billion in business and counting. Collection has surely suffered. The damage from the Snowden leaks to American foreign intelligence operations, to American prestige, and to American power – not to mention the damage to morale and to personnel retention right here at Fort Meade – has
unquestionably been vastly greater than if the Executive Branch had determined from the outset to amend FISA back in 2002 to permit the activities the White House felt necessary to protect the country.

Do you reply that the Congress in late 2001 or in 2002 might not have permitted NSA to do it? I doubt it. But even so, in a functioning representative democracy, this Agency cannot keep the nation safer than the nation, acting through its elected representatives, wants to be kept.

We learned the hard lessons of 1976. Let’s now think hard and learn this lesson too. And let’s teach it to those who come after us.

Thank you for the opportunity to address you. What you do is enormously important, and I count it a great privilege to have served among you.

[1] Joel Brenner was the Inspector General of the National Security Agency from 2002-2006; the National Counterintelligence Executive in the Office of the Director of National Intelligence from 2006-2009; and senior counsel at NSA from 2009-10. He now maintains a private law and consulting practice and is the Robert F. Wilhelm Fellow at the Massachusetts Institute for Technology’s Center for International Studies.


[4] Ibid.


[6] The orders themselves have not been declassified, so far as I know.


PUBLIC LAW 108–458—DEC. 17, 2004

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004
Public Law 108–458
108th Congress

An Act

To reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Intelligence Reform and Terrorism Prevention Act of 2004".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY

Sec. 1001. Short title.

Subtitle A—Establishment of Director of National Intelligence

Sec. 1011. Reorganization and improvement of management of intelligence community.

Sec. 1012. Revised definition of national intelligence.

Sec. 1013. Joint procedures for operational coordination between Department of Defense and Central Intelligence Agency.

Sec. 1014. Role of Director of National Intelligence in appointment of certain officials responsible for intelligence-related activities.

Sec. 1015. Executive Schedule matters.

Sec. 1016. Information sharing.

Sec. 1017. Alternative analysis of intelligence by the intelligence community.

Sec. 1018. Presidential guidelines on implementation and preservation of authorities.

Sec. 1019. Assignment of responsibilities relating to analytic integrity.

Sec. 1020. Safeguard of objectivity in intelligence analysis.

Subtitle B—National Counterterrorism Center, National Counter Proliferation Center, and National Intelligence Centers

Sec. 1021. National Counterterrorism Center.

Sec. 1022. National Counter Proliferation Center.

Sec. 1023. National intelligence centers.

Subtitle C—Joint Intelligence Community Council

Sec. 1031. Joint Intelligence Community Council.

Subtitle D—Improvement of Education for the Intelligence Community

Sec. 1041. Additional education and training requirements.

Sec. 1042. Cross-disciplinary education and training.

Sec. 1043. Intelligence Community Scholarship Program.

Subtitle E—Additional Improvements of Intelligence Activities

Sec. 1051. Service and national laboratories and the intelligence community.

Sec. 1052. Open-source intelligence.

Sec. 1053. National Intelligence Reserve Corps.

Subtitle F—Privacy and Civil Liberties

Sec. 1061. Privacy and Civil Liberties Oversight Board.

Dec. 17, 2004
[S. 2845]
Sec. 1062. Sense of Congress on designation of privacy and civil liberties officers.

Subtitle G—Conforming and Other Amendments
Sec. 1071. Conforming amendments relating to roles of Director of National Intelligence and Director of the Central Intelligence Agency.
Sec. 1072. Other conforming amendments.
Sec. 1074. Redesignation of National Foreign Intelligence Program as National Intelligence Program.
Sec. 1075. Repeal of superseded authority.
Sec. 1077. Conforming amendments relating to prohibiting dual service of the Director of the Central Intelligence Agency.
Sec. 1078. Authority to establish inspector general for the Office of the Director of National Intelligence.
Sec. 1079. Ethics matters.
Sec. 1080. Construction of authority of Director of National Intelligence to acquire and manage property and services.
Sec. 1081. General references.

Subtitle H—Transfer, Termination, Transition, and Other Provisions
Sec. 1091. Transfer of Community Management Staff.
Sec. 1092. Transfer of Terrorist Threat Integration Center.
Sec. 1093. Termination of positions of Assistant Directors of Central Intelligence.
Sec. 1094. Implementation plan.
Sec. 1095. Director of National Intelligence report on implementation of intelligence community reform.
Sec. 1096. Transitional authorities.
Sec. 1097. Effective dates.

Subtitle I—Other Matters
Sec. 1101. Study of promotion and professional military education school selection for military intelligence officers.
Sec. 1102. Extension and improvement of authorities of Public Interest Declassification Board.
Sec. 1103. Severability.

TITLE II—FEDERAL BUREAU OF INVESTIGATION
Sec. 2006. Federal Bureau of Investigation use of translators.

TITLE III—SECURITY CLEARANCES
Sec. 3001. Security clearances.

TITLE IV—TRANSPORTATION SECURITY
Subtitle A—National Strategy for Transportation Security

Subtitle B—Aviation Security
Sec. 4011. Provision for the use of biometric or other technology.
Sec. 4012. Advanced airline passenger prescreening.
Sec. 4013. Deployment and use of detection equipment at airport screening checkpoints.
Sec. 4014. Advanced airport checkpoint screening devices.
Sec. 4015. Improvement of screener job performance.
Sec. 4016. Federal air marshals.
Sec. 4017. International agreements to allow maximum deployment of Federal air marshals.
Sec. 4018. Foreign air marshal training.
Sec. 4019. In-line checked baggage screening.
Sec. 4020. Checked baggage screening area monitoring.
Sec. 4021. Wireless communication.
Sec. 4022. Improved pilot licenses.
Sec. 4023. Aviation security staffing.
118 STAT. 3640          PUBLIC LAW 108–458—DEC. 17, 2004

Sec. 4024. Improved explosive detection systems.
Sec. 4025. Prohibited items list.
Sec. 4026. Man-Portable Air Defense Systems (MANPADs).
Sec. 4027. Technical corrections.
Sec. 4028. Report on secondary flight deck barriers.
Sec. 4029. Extension of authorization of aviation security funding.

Subtitle C—Air Cargo Security

Sec. 4051. Pilot program to evaluate use of blast resistant cargo and baggage containers.
Sec. 4052. Air cargo security.
Sec. 4053. Air cargo security regulations.
Sec. 4054. Report on international air cargo threats.

Subtitle D—Maritime Security

Sec. 4071. Watch lists for passengers aboard vessels.
Sec. 4072. Deadlines for completion of certain plans, reports, and assessments.

Subtitle E—General Provisions

Sec. 4081. Definitions.
Sec. 4082. Effective date.

TITLE V—BORDER PROTECTION, IMMIGRATION, AND VISA MATTERS

Subtitle A—Advanced Technology Northern Border Security Pilot Program

Sec. 5101. Establishment.
Sec. 5102. Program requirements.
Sec. 5103. Administrative provisions.
Sec. 5104. Report.
Sec. 5105. Authorization of appropriations.

Subtitle B—Border and Immigration Enforcement

Sec. 5201. Border surveillance.
Sec. 5202. Increase in full-time Border Patrol agents.
Sec. 5203. Increase in full-time immigration and customs enforcement investigators.
Sec. 5204. Increase in detention bed space.

Subtitle C—Visa Requirements

Sec. 5301. In person interviews of visa applicants.
Sec. 5302. Visa application requirements.
Sec. 5303. Effective date.
Sec. 5304. Revocation of visas and other travel documentation.

Subtitle D—Immigration Reform

Sec. 5401. Bringing in and harboring certain aliens.
Sec. 5402. Deportation of aliens who have received military-type training from terrorist organizations.
Sec. 5403. Study and report on terrorists in the asylum system.

Subtitle E—Treatment of Aliens Who Commit Acts of Torture, Extrajudicial Killings, or Other Atrocities Abroad

Sec. 5501. Inadmissibility and deportability of aliens who have committed acts of torture or extrajudicial killings abroad.
Sec. 5502. Inadmissibility and deportability of foreign government officials who have committed particularly severe violations of religious freedom.
Sec. 5503. Waiver of inadmissibility.
Sec. 5504. Bar to good moral character for aliens who have committed acts of torture, extrajudicial killings, or severe violations of religious freedom.

Sec. 5505. Establishment of the Office of Special Investigations.
Sec. 5506. Report on implementation.

TITLE VI—TERRORISM PREVENTION

Subtitle A—Individual Terrorists as Agents of Foreign Powers

Sec. 6001. Individual terrorists as agents of foreign powers.
Sec. 6002. Additional semiannual reporting requirements under the Foreign Intelligence Surveillance Act of 1978.

Subtitle B—Money Laundering and Terrorist Financing

Sec. 6101. Additional authorization for FinCEN.
Sec. 6102. Money laundering and financial crimes strategy reauthorization.

Subtitle C—Money Laundering Abatement and Financial Antiterrorism Technical Corrections

Sec. 6201. Short title.
Sec. 6202. Technical corrections to Public Law 107–56.
Sec. 6203. Technical corrections to other provisions of law.
Sec. 6204. Repeal of review.
Sec. 6205. Effective date.

Subtitle D—Additional Enforcement Tools

Sec. 6301. Bureau of Engraving and Printing security printing.
Sec. 6302. Reporting of certain cross-border transmittal of funds.
Sec. 6303. Terrorism financing.

Subtitle E—Criminal History Background Checks

Sec. 6401. Protect Act.
Sec. 6402. Reviews of criminal records of applicants for private security officer employment.
Sec. 6403. Criminal history background checks.

Subtitle F—Grand Jury Information Sharing

Sec. 6501. Grand jury information sharing.

Subtitle G—Providing Material Support to Terrorism

Sec. 6601. Short title.
Sec. 6602. Receiving military-type training from a foreign terrorist organization.
Sec. 6603. Additions to offenses of providing material support to terrorism.
Sec. 6604. Financing of terrorism.

Subtitle H—Stop Terrorist and Military Hoaxes Act of 2004

Sec. 6701. Short title.
Sec. 6702. Hoaxes and recovery costs.
Sec. 6703. Obstruction of justice and false statements in terrorism cases.
Sec. 6704. Clarification of definition.

Subtitle I—Weapons of Mass Destruction Prohibition Improvement Act of 2004

Sec. 6801. Short title.
Sec. 6802. Weapons of mass destruction.
Sec. 6803. Participation in nuclear and weapons of mass destruction threats to the United States.

Subtitle J—Prevention of Terrorist Access to Destructive Weapons Act of 2004

Sec. 6901. Short title.
Sec. 6902. Findings and purpose.
Sec. 6903. Missile systems designed to destroy aircraft.
Sec. 6904. Atomic weapons.
Sec. 6905. Radiological dispersal devices.
Sec. 6906. Variola virus.
Sec. 6907. Interception of communications.
Sec. 6908. Amendments to section 2332d(g)(5)(b) of title 18, United States Code.
Sec. 6909. Amendments to section 1958c(e)(7)(d) of title 18, United States Code.
Sec. 6910. Export licensing process.
Sec. 6911. Clerical amendments.

Subtitle K—Pretrial Detention of Terrorists

Sec. 6951. Short title.
Sec. 6952. Presumption for pretrial detention in cases involving terrorism.

TITLE VII—IMPLEMENTATION OF 9/11 COMMISSION RECOMMENDATIONS

Sec. 7001. Short title.

Subtitle A—Diplomacy, Foreign Aid, and the Military in the War on Terrorism

Sec. 7101. Findings.
Sec. 7102. Terrorist sanctuaries.
Sec. 7103. United States commitment to the future of Pakistan.
Sec. 7104. Assistance for Afghanistan.
Sec. 7105. The relationship between the United States and Saudi Arabia.
Sec. 7106. Efforts to combat Islamist terrorism.
Sec. 7107. United States policy toward dictatorships.
Sec. 7108. Promotion of free media and other American values.
Sec. 7109. Public diplomacy responsibilities of the Department of State.
Sec. 7110. Public diplomacy training.
Sec. 7111. Promoting democracy and human rights at international organizations.
Sec. 7112. Expansion of United States scholarship and exchange programs in the Islamic world.
Sec. 7113. Pilot program to provide grants to American-sponsored schools in predominantly Muslim countries to provide scholarships.
Sec. 7114. International Youth Opportunity Fund.
Sec. 7115. The use of economic policies to combat terrorism.
Sec. 7116. Middle East partnership initiative.
Sec. 7117. Comprehensive coalition strategy for fighting terrorism.
Sec. 7118. Financing of terrorism.
Sec. 7119. Designation of foreign terrorist organizations.
Sec. 7120. Report to Congress.
Sec. 7121. Case-Zablocki Act requirements.
Sec. 7122. Effective date.

Subtitle B—Terrorist Travel and Effective Screening
Sec. 7201. Counterterrorist travel intelligence.
Sec. 7202. Establishment of human smuggling and trafficking center.
Sec. 7203. Responsibilities and functions of consular officers.
Sec. 7204. International agreements to track and curtail terrorist travel through the use of fraudulently obtained documents.
Sec. 7205. International standards for transliteration of names into the Roman alphabet for international travel documents and name-based watchlist systems.
Sec. 7206. Immigration security initiative.
Sec. 7207. Certification regarding technology for visa waiver participants.
Sec. 7208. Biometric entry and exit data system.
Sec. 7209. Travel documents.
Sec. 7210. Exchange of terrorist information and increased preinspection at foreign airports.
Sec. 7211. Minimum standards for birth certificates.
Sec. 7212. Driver's licenses and personal identification cards.
Sec. 7213. Social security cards and numbers.
Sec. 7214. Prohibition of the display of social security account numbers on driver's licenses or motor vehicle registrations.
Sec. 7215. Terrorist travel program.
Sec. 7216. Increase in penalties for fraud and related activity.
Sec. 7217. Study on allegedly lost or stolen passports.
Sec. 7218. Establishment of visa and passport security program in the Department of State.
Sec. 7219. Effective date.
Sec. 7220. Identification standards.

Subtitle C—National Preparedness
Sec. 7301. The incident command system.
Sec. 7302. National capital region mutual aid.
Sec. 7303. Enhancement of public safety communications interoperability.
Sec. 7304. Regional model strategic plan pilot projects.
Sec. 7305. Private sector preparedness.
Sec. 7306. Critical infrastructure and readiness assessments.
Sec. 7307. Northern command and defense of the United States homeland.
Sec. 7308. Effective date.

Subtitle D—Homeland Security
Sec. 7401. Sense of Congress on first responder funding.
Sec. 7402. Coordination of industry efforts.
Sec. 7403. Study regarding nationwide emergency notification system.
Sec. 7404. Pilot study to move warning systems into the modern digital age.
Sec. 7405. Required coordination.
Sec. 7406. Emergency preparedness compacts.
Sec. 7407. Responsibilities of counternarcotics office.
Sec. 7408. Use of counternarcotics enforcement activities in certain employee performance appraisals.

Subtitle E—Public Safety Spectrum
Sec. 7501. Digital television conversion deadline.
Sec. 7502. Studies on telecommunications capabilities and requirements.
Subtitle F—Presidential Transition

Sec. 7601. Presidential transition.

Subtitle G—Improving International Standards and Cooperation to Fight Terrorist Financing

Sec. 7701. Improving international standards and cooperation to fight terrorist financing.
Sec. 7702. Definitions.
Sec. 7703. Expanded reporting and testimony requirements for the Secretary of the Treasury.
Sec. 7704. Coordination of United States Government efforts.

Subtitle H—Emergency Financial Preparedness

Sec. 7801. Delegation authority of the Secretary of the Treasury.
Sec. 7802. Treasury support for financial services industry preparedness and response and consumer education.
Sec. 7804. Private sector preparedness.

TITLE VIII—OTHER MATTERS

Subtitle A—Intelligence Matters

Sec. 8101. Intelligence community use of National Infrastructure Simulation and Analysis Center.

Subtitle B—Department of Homeland Security Matters

Sec. 8201. Homeland security geospatial information.

Subtitle C—Homeland Security Civil Rights and Civil Liberties Protection

Sec. 8301. Short title.
Sec. 8303. Officer for Civil Rights and Civil Liberties.
Sec. 8304. Protection of civil rights and civil liberties by Office of Inspector General.
Sec. 8305. Privacy officer.

Subtitle D—Other Matters

Sec. 8401. Amendments to Clinger-Cohen Act provisions to enhance agency planning for information security needs.
Sec. 8402. Enterprise architecture.
Sec. 8403. Financial disclosure and records.
Sec. 8404. Extension of requirement for air carriers to honor tickets for suspended air passenger service.

TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY

SEC. 1001. SHORT TITLE.

This title may be cited as the “National Security Intelligence Reform Act of 2004”.

Subtitle A—Establishment of Director of National Intelligence

SEC. 1011. REORGANIZATION AND IMPROVEMENT OF MANAGEMENT OF INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 402 et seq.) is amended by striking sections 102 through 104 and inserting the following new sections:
"DIRECTOR OF NATIONAL INTELLIGENCE

SEC. 102. (a) DIRECTOR OF NATIONAL INTELLIGENCE.—(1) There is a Director of National Intelligence who shall be appointed by the President, by and with the advice and consent of the Senate. Any individual nominated for appointment as Director of National Intelligence shall have extensive national security expertise.

(2) The Director of National Intelligence shall not be located within the Executive Office of the President.

(b) PRINCIPAL RESPONSIBILITY.—Subject to the authority, direction, and control of the President, the Director of National Intelligence shall—

(1) serve as head of the intelligence community;

(2) act as the principal adviser to the President, to the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; and

(3) consistent with section 1018 of the National Security Intelligence Reform Act of 2004, oversee and direct the implementation of the National Intelligence Program.

(c) PROHIBITION ON DUAL SERVICE.—The individual serving in the position of Director of National Intelligence shall not, while so serving, also serve as the Director of the Central Intelligence Agency or as the head of any other element of the intelligence community.

RESPONSIBILITIES AND AUTHORITIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE

SEC. 102A. (a) PROVISION OF INTELLIGENCE.—(1) The Director of National Intelligence shall be responsible for ensuring that national intelligence is provided—

(A) to the President;

(B) to the heads of departments and agencies of the executive branch;

(C) to the Chairman of the Joint Chiefs of Staff and senior military commanders;

(D) to the Senate and House of Representatives and the committees thereof; and

(E) to such other persons as the Director of National Intelligence determines to be appropriate.

(2) Such national intelligence should be timely, objective, independent of political considerations, and based upon all sources available to the intelligence community and other appropriate entities.

(b) ACCESS TO INTELLIGENCE.—Unless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence.

(c) BUDGET AUTHORITIES.—(1) With respect to budget requests and appropriations for the National Intelligence Program, the Director of National Intelligence shall—

(A) based on intelligence priorities set by the President, provide to the heads of departments containing agencies or organizations within the intelligence community, and to the
heads of such agencies and organizations, guidance for developing the National Intelligence Program budget pertaining to such agencies and organizations;

"(B) based on budget proposals provided to the Director of National Intelligence by the heads of agencies and organizations within the intelligence community and the heads of their respective departments and, as appropriate, after obtaining the advice of the Joint Intelligence Community Council, develop and determine an annual consolidated National Intelligence Program budget; and

"(C) present such consolidated National Intelligence Program budget, together with any comments from the heads of departments containing agencies or organizations within the intelligence community, to the President for approval.

"(2) In addition to the information provided under paragraph (1)(B), the heads of agencies and organizations within the intelligence community shall provide the Director of National Intelligence such other information as the Director shall request for the purpose of determining the annual consolidated National Intelligence Program budget under that paragraph.

"(3)(A) The Director of National Intelligence shall participate in the development by the Secretary of Defense of the annual budgets for the Joint Military Intelligence Program and for Tactical Intelligence and Related Activities.

"(B) The Director of National Intelligence shall provide guidance for the development of the annual budget for each element of the intelligence community that is not within the National Intelligence Program.

"(4) The Director of National Intelligence shall ensure the effective execution of the annual budget for intelligence and intelligence-related activities.

"(5)(A) The Director of National Intelligence shall be responsible for managing appropriations for the National Intelligence Program by directing the allotment or allocation of such appropriations through the heads of the departments containing agencies or organizations within the intelligence community and the Director of the Central Intelligence Agency, with prior notice (including the provision of appropriate supporting information) to the head of the department containing an agency or organization receiving any such allocation or allotment or the Director of the Central Intelligence Agency.

"(B) Notwithstanding any other provision of law, pursuant to relevant appropriations Acts for the National Intelligence Program, the Director of the Office of Management and Budget shall exercise the authority of the Director of the Office of Management and Budget to apportion funds, at the exclusive direction of the Director of National Intelligence, for allocation to the elements of the intelligence community through the relevant host executive departments and the Central Intelligence Agency. Department comptrollers or appropriate budget execution officers shall allot, allocate, reprogram, or transfer funds appropriated for the National Intelligence Program in an expeditious manner.

"(C) The Director of National Intelligence shall monitor the implementation and execution of the National Intelligence Program by the heads of the elements of the intelligence community that manage programs and activities that are part of the National Intelligence Program, which may include audits and evaluations.
"(6) Apportionment and allotment of funds under this subsection shall be subject to chapter 13 and section 1517 of title 31, United States Code, and the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 621 et seq.).

"(7)(A) The Director of National Intelligence shall provide a semi-annual report, beginning April 1, 2005, and ending April 1, 2007, to the President and the Congress regarding implementation of this section.

"(B) The Director of National Intelligence shall report to the President and the Congress not later than 15 days after learning of any instance in which a departmental controller acts in a manner inconsistent with the law (including permanent statutes, authorization Acts, and appropriations Acts), or the direction of the Director of National Intelligence, in carrying out the National Intelligence Program.

"(d) ROLE OF DIRECTOR OF NATIONAL INTELLIGENCE IN TRANSFER AND REPROGRAMMING OF FUNDS.—(1)(A) No funds made available under the National Intelligence Program may be transferred or reprogrammed without the prior approval of the Director of National Intelligence, except in accordance with procedures prescribed by the Director of National Intelligence.

"(B) The Secretary of Defense shall consult with the Director of National Intelligence before transferring or reprogramming funds made available under the Joint Military Intelligence Program.

"(2) Subject to the preceding provisions of this subsection, the Director of National Intelligence may transfer or reprogram funds appropriated for a program within the National Intelligence Program to another such program.

"(3) The Director of National Intelligence may only transfer or reprogram funds referred to in subparagraph (A)—

"(A) with the approval of the Director of the Office of Management and Budget; and

"(B) after consultation with the heads of departments containing agencies or organizations within the intelligence community to the extent such agencies or organizations are affected, and, in the case of the Central Intelligence Agency, after consultation with the Director of the Central Intelligence Agency.

"(4) The amounts available for transfer or reprogramming in the National Intelligence Program in any given fiscal year, and the terms and conditions governing such transfers and reprogrammings, are subject to the provisions of annual appropriations Acts and this subsection.

"(5)(A) A transfer or reprogramming of funds or personnel may be made under this subsection only if—

"(i) the funds are being transferred to an activity that is a higher priority intelligence activity;

"(ii) the transfer or reprogramming supports an emergent need, improves program effectiveness, or increases efficiency;

"(iii) the transfer or reprogramming does not involve a transfer or reprogramming of funds to a Reserve for Contingencies of the Director of National Intelligence or the Reserve for Contingencies of the Central Intelligence Agency;

"(iv) the transfer or reprogramming results in a cumulative transfer or reprogramming of funds out of any department or agency, as appropriate, funded in the National Intelligence Program in a single fiscal year—
“(I) that is less than $150,000,000, and
“(II) that is less than 5 percent of amounts available to a department or agency under the National Intelligence Program; and
“(v) the transfer or reprogramming does not terminate an acquisition program.
“(B) A transfer or reprogramming may be made without regard to a limitation set forth in clause (iv) or (v) of subparagraph (A) if the transfer has the concurrence of the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency). The authority to provide such concurrence may only be delegated by the head of the department or agency involved to the deputy of such officer.
“(6) Funds transferred or reprogrammed under this subsection shall remain available for the same period as the appropriations account to which transferred or reprogrammed.
“(7) Any transfer or reprogramming of funds under this subsection shall be carried out in accordance with existing procedures applicable to reprogramming notifications for the appropriate congressional committees. Any proposed transfer or reprogramming for which notice is given to the appropriate congressional committees shall be accompanied by a report explaining the nature of the proposed transfer or reprogramming and how it satisfies the requirements of this subsection. In addition, the congressional intelligence committees shall be promptly notified of any transfer or reprogramming of funds made pursuant to this subsection in any case in which the transfer or reprogramming would not have otherwise required reprogramming notification under procedures in effect as of the date of the enactment of this subsection.
“(e) Transfer of Personnel.—(1)(A) In addition to any other authorities available under law for such purposes, in the first twelve months after establishment of a new national intelligence center, the Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in consultation with the congressional committees of jurisdiction referred to in subparagraph (B), may transfer not more than 100 personnel authorized for elements of the intelligence community to such center.
“(B) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—
“(i) the congressional intelligence committees;
“(ii) the Committees on Appropriations of the Senate and the House of Representatives;
“(iii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and
“(iv) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.
“(C) The Director shall include in any notice under subparagraph (B) an explanation of the nature of the transfer and how it satisfies the requirements of this subsection.
“(2) (A) The Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in accordance with procedures to be developed by the Director of National Intelligence and the heads of the departments and agencies
concerned, may transfer personnel authorized for an element of the intelligence community to another such element for a period of not more than 2 years.

"(B) A transfer of personnel may be made under this paragraph only if—

"(i) the personnel are being transferred to an activity that is a higher priority intelligence activity; and

"(ii) the transfer supports an emergent need, improves program effectiveness, or increases efficiency.

"(C) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

"(i) the congressional intelligence committees;

"(ii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and

"(iii) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

"(D) The Director shall include in any notice under subparagraph (C) an explanation of the nature of the transfer and how it satisfies the requirements of this paragraph.

"(3) It is the sense of Congress that—

"(A) the nature of the national security threats facing the United States will continue to challenge the intelligence community to respond rapidly and flexibly to bring analytic resources to bear against emerging and unforeseen requirements;

"(B) both the Office of the Director of National Intelligence and any analytic centers determined to be necessary should be fully and properly supported with appropriate levels of personnel resources and that the President's yearly budget requests adequately support those needs; and

"(C) the President should utilize all legal and administrative discretion to ensure that the Director of National Intelligence and all other elements of the intelligence community have the necessary resources and procedures to respond promptly and effectively to emerging and unforeseen national security challenges.

"(f) TASKING AND OTHER AUTHORITIES.—(1)(A) The Director of National Intelligence shall—

"(i) establish objectives, priorities, and guidance for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination (including access by users to collected data consistent with applicable law and, as appropriate, the guidelines referred to in subsection (b) and analytic products generated by or within the intelligence community) of national intelligence;

"(ii) determine requirements and priorities for, and manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community, including—

"(I) approving requirements (including those requirements responding to needs provided by consumers) for collection and analysis; and
“(II) resolving conflicts in collection requirements and in the tasking of national collection assets of the elements of the intelligence community; and
“(iii) provide advisory tasking to intelligence elements of those agencies and departments not within the National Intelligence Program.
“(B) The authority of the Director of National Intelligence under subparagraph (A) shall not apply—
“(i) insofar as the President so directs;
“(ii) with respect to clause (ii) of subparagraph (A), insofar as the Secretary of Defense exercises tasking authority under plans or arrangements agreed upon by the Secretary of Defense and the Director of National Intelligence; or
“(iii) to the direct dissemination of information to State government and local government officials and private sector entities pursuant to sections 201 and 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482).
“(2) The Director of National Intelligence shall oversee the National Counterterrorism Center and may establish such other national intelligence centers as the Director determines necessary.
“(3)(A) The Director of National Intelligence shall prescribe, in consultation with the heads of other agencies or elements of the intelligence community, and the heads of their respective departments, personnel policies and programs applicable to the intelligence community that—
“(i) encourage and facilitate assignments and details of personnel to national intelligence centers, and between elements of the intelligence community;
“(ii) set standards for education, training, and career development of personnel of the intelligence community;
“(iii) encourage and facilitate the recruitment and retention by the intelligence community of highly qualified individuals for the effective conduct of intelligence activities;
“(iv) ensure that the personnel of the intelligence community are sufficiently diverse for purposes of the collection and analysis of intelligence through the recruitment and training of women, minorities, and individuals with diverse ethnic, cultural, and linguistic backgrounds;
“(v) make service in more than one element of the intelligence community a condition of promotion to such positions within the intelligence community as the Director shall specify; and
“(vi) ensure the effective management of intelligence community personnel who are responsible for intelligence community-wide matters.
“(B) Policies prescribed under subparagraph (A) shall not be inconsistent with the personnel policies otherwise applicable to members of the uniformed services.
“(4) The Director of National Intelligence shall ensure compliance with the Constitution and laws of the United States by the Central Intelligence Agency and shall ensure such compliance by other elements of the intelligence community through the host executive departments that manage the programs and activities that are part of the National Intelligence Program.
“(5) The Director of National Intelligence shall ensure the elimination of waste and unnecessary duplication within the intelligence community.
"(6) The Director of National Intelligence shall establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for national intelligence purposes, except that the Director shall have no authority to direct or undertake electronic surveillance or physical search operations pursuant to that Act unless authorized by statute or Executive order.

"(7) The Director of National Intelligence shall perform such other functions as the President may direct.

"(8) Nothing in this title shall be construed as affecting the role of the Department of Justice or the Attorney General under the Foreign Intelligence Surveillance Act of 1978.

"(g) INTELLIGENCE INFORMATION SHARING.—(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

(A) establish uniform security standards and procedures;

(B) establish common information technology standards, protocols, and interfaces;

(C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

(D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; and

(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program.

(2) The President shall ensure that the Director of National Intelligence has all necessary support and authorities to fully and effectively implement paragraph (1).

(3) Except as otherwise directed by the President or with the specific written agreement of the head of the department or agency in question, a Federal agency or official shall not be considered to have met any obligation to provide any information, report, assessment, or other material (including unevaluated intelligence information) to that department or agency solely by virtue of having provided that information, report, assessment, or other material to the Director of National Intelligence or the National Counterterrorism Center.

(4) Not later than February 1 of each year, the Director of National Intelligence shall submit to the President and to the Congress an annual report that identifies any statute, regulation, policy, or practice that the Director believes impedes the ability of the Director to fully and effectively implement paragraph (1).

(h) ANALYSIS.—To ensure the most accurate analysis of intelligence is derived from all sources to support national security needs, the Director of National Intelligence shall—

(1) implement policies and procedures—
“(A) to encourage sound analytic methods and tradecraft throughout the elements of the intelligence community;

“(B) to ensure that analysis is based upon all sources available; and

“(C) to ensure that the elements of the intelligence community regularly conduct competitive analysis of analytic products, whether such products are produced by or disseminated to such elements;

“(2) ensure that resource allocation for intelligence analysis is appropriately proportional to resource allocation for intelligence collection systems and operations in order to maximize analysis of all collected data;

“(3) ensure that differences in analytic judgment are fully considered and brought to the attention of policymakers; and

“(4) ensure that sufficient relationships are established between intelligence collectors and analysts to facilitate greater understanding of the needs of analysts.

“(i) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—

(1) The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.

“(2) Consistent with paragraph (1), in order to maximize the dissemination of intelligence, the Director of National Intelligence shall establish and implement guidelines for the intelligence community for the following purposes:

“(A) Classification of information under applicable law, Executive orders, or other Presidential directives.

“(B) Access to and dissemination of intelligence, both in final form and in the form when initially gathered.

“(C) Preparation of intelligence products in such a way that source information is removed to allow for dissemination at the lowest level of classification possible or in unclassified form to the extent practicable.

“(3) The Director may only delegate a duty or authority given the Director under this subsection to the Principal Deputy Director of National Intelligence.

“(j) UNIFORM PROCEDURES FOR SENSITIVE COMPARTMENTED INFORMATION.—The Director of National Intelligence, subject to the direction of the President, shall—

“(1) establish uniform standards and procedures for the grant of access to sensitive compartmented information to any officer or employee of any agency or department of the United States and to employees of contractors of those agencies or departments;

“(2) ensure the consistent implementation of those standards and procedures throughout such agencies and departments;

“(3) ensure that security clearances granted by individual elements of the intelligence community are recognized by all elements of the intelligence community, and under contracts entered into by those agencies; and

“(4) ensure that the process for investigation and adjudication of an application for access to sensitive compartmented information is performed in the most expeditious manner possible consistent with applicable standards for national security.

“(k) COORDINATION WITH FOREIGN GOVERNMENTS.—Under the direction of the President and in a manner consistent with section
207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director of National Intelligence shall oversee the coordination of the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

(I) ENHANCED PERSONNEL MANAGEMENT.—(A) The Director of National Intelligence shall, under regulations prescribed by the Director, provide incentives for personnel of elements of the intelligence community to serve—

(i) on the staff of the Director of National Intelligence;

(ii) on the staff of the national intelligence centers;

(iii) on the staff of the National Counterterrorism Center;

and

(iv) in other positions in support of the intelligence community management functions of the Director.

(B) Incentives under subparagraph (A) may include financial incentives, bonuses, and such other awards and incentives as the Director considers appropriate.

(2)(A) Notwithstanding any other provision of law, the personnel of an element of the intelligence community who are assigned or detailed under paragraph (1)(A) to service under the Director of National Intelligence shall be promoted at rates equivalent to or better than personnel of such element who are not so assigned or detailed.

(B) The Director may prescribe regulations to carry out this section.

(3)(A) The Director of National Intelligence shall prescribe mechanisms to facilitate the rotation of personnel of the intelligence community through various elements of the intelligence community in the course of their careers in order to facilitate the widest possible understanding by such personnel of the variety of intelligence requirements, methods, users, and capabilities.

(B) The mechanisms prescribed under subparagraph (A) may include the following:

(i) The establishment of special occupational categories involving service, over the course of a career, in more than one element of the intelligence community.

(ii) The provision of rewards for service in positions undertaking analysis and planning of operations involving two or more elements of the intelligence community.

(iii) The establishment of requirements for education, training, service, and evaluation for service involving more than one element of the intelligence community.

(C) It is the sense of Congress that the mechanisms prescribed under this subsection should, to the extent practical, seek to duplicate for civilian personnel within the intelligence community the joint officer management policies established by chapter 38 of title 10, United States Code, and the other amendments made by title IV of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99–433).

(4)(A) Except as provided in subparagraph (B) and subparagraph (D), this subsection shall not apply with respect to personnel of the elements of the intelligence community who are members of the uniformed services.
“(B) Mechanisms that establish requirements for education and training pursuant to paragraph (3)(B)(iii) may apply with respect to members of the uniformed services who are assigned to an element of the intelligence community funded through the National Intelligence Program, but such mechanisms shall not be inconsistent with personnel policies and education and training requirements otherwise applicable to members of the uniformed services.

“(C) The personnel policies and programs developed and implemented under this subsection with respect to law enforcement officers (as that term is defined in section 5541(3) of title 5, United States Code) shall not affect the ability of law enforcement entities to conduct operations or, through the applicable chain of command, to control the activities of such law enforcement officers.

“(D) Assignment to the Office of the Director of National Intelligence of commissioned officers of the Armed Forces shall be considered a joint-duty assignment for purposes of the joint officer management policies prescribed by chapter 38 of title 10, United States Code, and other provisions of that title.

“(m) ADDITIONAL AUTHORITY WITH RESPECT TO PERSONNEL.—

(1) In addition to the authorities under subsection (f)(3), the Director of National Intelligence may exercise with respect to the personnel of the Office of the Director of National Intelligence any authority of the Director of the Central Intelligence Agency with respect to the personnel of the Central Intelligence Agency under the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.), and other applicable provisions of law, as of the date of the enactment of this subsection to the same extent, and subject to the same conditions and limitations, that the Director of the Central Intelligence Agency may exercise such authority with respect to personnel of the Central Intelligence Agency.

“(2) Employees and applicants for employment of the Office of the Director of National Intelligence shall have the same rights and protections under the Office of the Director of National Intelligence as employees of the Central Intelligence Agency have under the Central Intelligence Agency Act of 1949, and other applicable provisions of law, as of the date of the enactment of this subsection.

“(n) ACQUISITION AUTHORITIES.—(1) In carrying out the responsibilities and authorities under this section, the Director of National Intelligence may exercise the acquisition and appropriations authorities referred to in the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.) other than the authorities referred to in section 8(b) of that Act (50 U.S.C. 403j(b)).

“(2) For the purpose of the exercise of any authority referred to in paragraph (1), a reference to the head of an agency shall be deemed to be a reference to the Director of National Intelligence or the Principal Deputy Director of National Intelligence.

“(3)(A) Any determination or decision to be made under an authority referred to in paragraph (1) by the head of an agency may be made with respect to individual purchases and contracts or with respect to classes of purchases or contracts, and shall be final.

“(B) Except as provided in subparagraph (C), the Director of National Intelligence or the Principal Deputy Director of National Intelligence may, in such official's discretion, delegate to any officer or other official of the Office of the Director of National Intelligence any authority to make a determination or decision as the head of the agency under an authority referred to in paragraph (1),
“(C) The limitations and conditions set forth in section 3(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403c(d)) shall apply to the exercise by the Director of National Intelligence of an authority referred to in paragraph (1).

“(D) Each determination or decision required by an authority referred to in the second sentence of section 3(d) of the Central Intelligence Agency Act of 1949 shall be based upon written findings made by the official making such determination or decision, which findings shall be final and shall be available within the Office of the Director of National Intelligence for a period of at least six years following the date of such determination or decision.

“(o) CONSIDERATION OF VIEWS OF ELEMENTS OF INTELLIGENCE COMMUNITY.—In carrying out the duties and responsibilities under this section, the Director of National Intelligence shall take into account the views of a head of a department containing an element of the intelligence community and of the Director of the Central Intelligence Agency.

“(p) RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING THE DEPARTMENT OF DEFENSE.—Subject to the direction of the President, the Director of National Intelligence shall, after consultation with the Secretary of Defense, ensure that the National Intelligence Program budgets for the elements of the intelligence community that are within the Department of Defense are adequate to satisfy the national intelligence needs of the Department of Defense, including the needs of the Chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands, and wherever such elements are performing Government-wide functions, the needs of other Federal departments and agencies.

“(q) ACQUISITIONS OF MAJOR SYSTEMS.—(1) For each intelligence program within the National Intelligence Program for the acquisition of a major system, the Director of National Intelligence shall—

“(A) require the development and implementation of a program management plan that includes cost, schedule, and performance goals and program milestone criteria, except that with respect to Department of Defense programs the Director shall consult with the Secretary of Defense;

“(B) serve as exclusive milestone decision authority, except that with respect to Department of Defense programs the Director shall serve as milestone decision authority jointly with the Secretary of Defense or the designee of the Secretary; and

“(C) periodically—

“(i) review and assess the progress made toward the achievement of the goals and milestones established in such plan; and

“(ii) submit to Congress a report on the results of such review and assessment.

“(2) If the Director of National Intelligence and the Secretary of Defense are unable to reach an agreement on a milestone decision under paragraph (1)(B), the President shall resolve the conflict.

“(3) Nothing in this subsection may be construed to limit the authority of the Director of National Intelligence to delegate to any other official any authority to perform the responsibilities of the Director under this subsection.

“(4) In this subsection:
“(A) The term ‘intelligence program’, with respect to the acquisition of a major system, means a program that—
   “(i) is carried out to acquire such major system for an element of the intelligence community; and
   “(ii) is funded in whole out of amounts available for the National Intelligence Program.
   “(B) The term ‘major system’ has the meaning given such term in section 4(9) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 403(9)).

“(r) PERFORMANCE OF COMMON SERVICES.—The Director of National Intelligence shall, in consultation with the heads of departments and agencies of the United States Government containing elements within the intelligence community and with the Director of the Central Intelligence Agency, coordinate the performance by the elements of the intelligence community within the National Intelligence Program of such services as are of common concern to the intelligence community, which services the Director of National Intelligence determines can be more efficiently accomplished in a consolidated manner.

“OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

“SEC. 103. (a) Office of Director of National Intelligence.—There is an Office of the Director of National Intelligence.

“(b) Function.—The function of the Office of the Director of National Intelligence is to assist the Director of National Intelligence in carrying out the duties and responsibilities of the Director under this Act, the National Security Act of 1947 (50 U.S.C. 401 et seq.), and other applicable provisions of law, and to carry out such other duties as may be prescribed by the President or by law.

“(c) Composition.—The Office of the Director of National Intelligence is composed of the following:
   “(1) The Director of National Intelligence.
   “(2) The Principal Deputy Director of National Intelligence.
   “(3) Any Deputy Director of National Intelligence appointed under section 103A.
   “(4) The National Intelligence Council.
   “(5) The General Counsel.
   “(6) The Civil Liberties Protection Officer.
   “(7) The Director of Science and Technology.
   “(8) The National Counterintelligence Executive (including the Office of the National Counterintelligence Executive).
   “(9) Such other offices and officials as may be established by law or the Director may establish or designate in the Office, including national intelligence centers.

“(d) Staff.—(1) To assist the Director of National Intelligence in fulfilling the duties and responsibilities of the Director, the Director shall employ and utilize in the Office of the Director of National Intelligence a professional staff having an expertise in matters relating to such duties and responsibilities, and may establish permanent positions and appropriate rates of pay with respect to that staff.

   “(2) The staff of the Office of the Director of National Intelligence under paragraph (1) shall include the staff of the Office of the Deputy Director of Central Intelligence for Community Management that is transferred to the Office of the Director of
National Intelligence under section 1091 of the National Security Intelligence Reform Act of 2004.

"(e) LIMITATION ON CO-LOCATION WITH OTHER ELEMENTS OF INTELLIGENCE COMMUNITY.—Commencing as of October 1, 2008, the Office of the Director of National Intelligence may not be co-located with any other element of the intelligence community.

"DEPUTY DIRECTORS OF NATIONAL INTELLIGENCE

"SEC. 103A. (a) PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE.—(1) There is a Principal Deputy Director of National Intelligence who shall be appointed by the President, by and with the advice and consent of the Senate.

"(2) In the event of a vacancy in the position of Principal Deputy Director of National Intelligence, the Director of National Intelligence shall recommend to the President an individual for appointment as Principal Deputy Director of National Intelligence.

"(3) Any individual nominated for appointment as Principal Deputy Director of National Intelligence shall have extensive national security experience and management expertise.

"(4) The individual serving as Principal Deputy Director of National Intelligence shall not, while so serving, serve in any capacity in any other element of the intelligence community.

"(5) The Principal Deputy Director of National Intelligence shall assist the Director of National Intelligence in carrying out the duties and responsibilities of the Director.

"(6) The Principal Deputy Director of National Intelligence shall act for, and exercise the powers of, the Director of National Intelligence during the absence or disability of the Director of National Intelligence or during a vacancy in the position of Director of National Intelligence.

"(b) DEPUTY DIRECTORS OF NATIONAL INTELLIGENCE.—(1) There may be not more than four Deputy Directors of National Intelligence who shall be appointed by the Director of National Intelligence.

"(2) Each Deputy Director of National Intelligence appointed under this subsection shall have such duties, responsibilities, and authorities as the Director of National Intelligence may assign or are specified by law.

"(c) MILITARY STATUS OF DIRECTOR OF NATIONAL INTELLIGENCE AND PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE.—(1) Not more than one of the individuals serving in the positions specified in paragraph (2) may be a commissioned officer of the Armed Forces in active status.

"(2) The positions referred to in this paragraph are the following:

"(A) The Director of National Intelligence.

"(B) The Principal Deputy Director of National Intelligence.

"(3) It is the sense of Congress that, under ordinary circumstances, it is desirable that one of the individuals serving in the positions specified in paragraph (2)—

"(A) be a commissioned officer of the Armed Forces, in active status; or

"(B) have, by training or experience, an appreciation of military intelligence activities and requirements.

"(4) A commissioned officer of the Armed Forces, while serving in a position specified in paragraph (2)—
“(A) shall not be subject to supervision or control by the Secretary of Defense or by any officer or employee of the Department of Defense;

“(B) shall not exercise, by reason of the officer’s status as a commissioned officer, any supervision or control with respect to any of the military or civilian personnel of the Department of Defense except as otherwise authorized by law; and

“(C) shall not be counted against the numbers and percentages of commissioned officers of the rank and grade of such officer authorized for the military department of that officer.

“(5) Except as provided in subparagraph (A) or (B) of paragraph (4), the appointment of an officer of the Armed Forces to a position specified in paragraph (2) shall not affect the status, position, rank, or grade of such officer in the Armed Forces, or any emolument, perquisite, right, privilege, or benefit incident to or arising out of such status, position, rank, or grade.

“(6) A commissioned officer of the Armed Forces on active duty who is appointed to a position specified in paragraph (2), while serving in such position and while remaining on active duty, shall continue to receive military pay and allowances and shall not receive the pay prescribed for such position. Funds from which such pay and allowances are paid shall be reimbursed from funds available to the Director of National Intelligence.

“NATIONAL INTELLIGENCE COUNCIL

“Sec. 103B. (a) National Intelligence Council.—There is a National Intelligence Council.

“(b) Composition.—(1) The National Intelligence Council shall be composed of senior analysts within the intelligence community and substantive experts from the public and private sector, who shall be appointed by, report to, and serve at the pleasure of, the Director of National Intelligence.

“(2) The Director shall prescribe appropriate security requirements for personnel appointed from the private sector as a condition of service on the Council, or as contractors of the Council or employees of such contractors, to ensure the protection of intelligence sources and methods while avoiding, wherever possible, unduly intrusive requirements which the Director considers to be unnecessary for this purpose.

“(c) Duties and Responsibilities.—(1) The National Intelligence Council shall—

“(A) produce national intelligence estimates for the United States Government, including alternative views held by elements of the intelligence community and other information as specified in paragraph (2);

“(B) evaluate community-wide collection and production of intelligence by the intelligence community and the requirements and resources of such collection and production; and

“(C) otherwise assist the Director of National Intelligence in carrying out the responsibilities of the Director under section 102A.

“(2) The Director of National Intelligence shall ensure that the Council satisfies the needs of policymakers and other consumers of intelligence.

“(d) Service as Senior Intelligence Advisers.—Within their respective areas of expertise and under the direction of the Director
of National Intelligence, the members of the National Intelligence Council shall constitute the senior intelligence advisers of the intelligence community for purposes of representing the views of the intelligence community within the United States Government.

"(e) AUTHORITY TO CONTRACT.—Subject to the direction and control of the Director of National Intelligence, the National Intelligence Council may carry out its responsibilities under this section by contract, including contracts for substantive experts necessary to assist the Council with particular assessments under this section.

"(f) STAFF.—The Director of National Intelligence shall make available to the National Intelligence Council such staff as may be necessary to permit the Council to carry out its responsibilities under this section.

"(g) AVAILABILITY OF COUNCIL AND STAFF.—(1) The Director of National Intelligence shall take appropriate measures to ensure that the National Intelligence Council and its staff satisfy the needs of policymaking officials and other consumers of intelligence.

"(2) The Council shall be readily accessible to policymaking officials and other appropriate individuals not otherwise associated with the intelligence community.

"(h) SUPPORT.—The heads of the elements of the intelligence community shall, as appropriate, furnish such support to the National Intelligence Council, including the preparation of intelligence analyses, as may be required by the Director of National Intelligence.

"(i) NATIONAL INTELLIGENCE COUNCIL PRODUCT.—For purposes of this section, the term ‘National Intelligence Council product’ includes a National Intelligence Estimate and any other intelligence community assessment that sets forth the judgment of the intelligence community as a whole on a matter covered by such product.

"GENERAL COUNSEL

"SEC. 103C. (a) GENERAL COUNSEL.—There is a General Counsel of the Office of the Director of National Intelligence who shall be appointed by the President, by and with the advice and consent of the Senate.

"(b) PROHIBITION ON DUAL SERVICE AS GENERAL COUNSEL OF ANOTHER AGENCY.—The individual serving in the position of General Counsel may not, while so serving, also serve as the General Counsel of any other department, agency, or element of the United States Government.

"(c) SCOPE OF POSITION.—The General Counsel is the chief legal officer of the Office of the Director of National Intelligence.

"(d) FUNCTIONS.—The General Counsel shall perform such functions as the Director of National Intelligence may prescribe.

"CIVIL LIBERTIES PROTECTION OFFICER

"SEC. 103D. (a) CIVIL LIBERTIES PROTECTION OFFICER.—(1) Within the Office of the Director of National Intelligence, there is a Civil Liberties Protection Officer who shall be appointed by the Director of National Intelligence.

"(2) The Civil Liberties Protection Officer shall report directly to the Director of National Intelligence.

"(b) DUTIES.—The Civil Liberties Protection Officer shall—

"(1) ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures
developed for and implemented by the Office of the Director of National Intelligence and the elements of the intelligence community within the National Intelligence Program;

(2) oversee compliance by the Office and the Director of National Intelligence with requirements under the Constitution and all laws, regulations, Executive orders, and implementing guidelines relating to civil liberties and privacy;

(3) review and assess complaints and other information indicating possible abuses of civil liberties and privacy in the administration of the programs and operations of the Office and the Director of National Intelligence and, as appropriate, investigate any such complaint or information;

(4) ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(5) ensure that personal information contained in a system of records subject to section 552a of title 5, United States Code (popularly referred to as the 'Privacy Act'), is handled in full compliance with fair information practices as set out in that section;

(6) conduct privacy impact assessments when appropriate or as required by law; and

(7) perform such other duties as may be prescribed by the Director of National Intelligence or specified by law.

(c) Use of Agency Inspectors General.—When appropriate, the Civil Liberties Protection Officer may refer complaints to the Office of Inspector General having responsibility for the affected element of the department or agency of the intelligence community to conduct an investigation under paragraph (3) of subsection (b).

"SEC. 103E. (a) DIRECTOR OF SCIENCE AND TECHNOLOGY.—There is a Director of Science and Technology within the Office of the Director of National Intelligence who shall be appointed by the Director of National Intelligence.

(b) REQUIREMENT RELATING TO APPOINTMENT.—An individual appointed as Director of Science and Technology shall have a professional background and experience appropriate for the duties of the Director of Science and Technology.

(c) DUTIES.—The Director of Science and Technology shall—

(1) act as the chief representative of the Director of National Intelligence for science and technology;

(2) chair the Director of National Intelligence Science and Technology Committee under subsection (d);

(3) assist the Director in formulating a long-term strategy for scientific advances in the field of intelligence;

(4) assist the Director on the science and technology elements of the budget of the Office of the Director of National Intelligence; and

(5) perform other such duties as may be prescribed by the Director of National Intelligence or specified by law.

(d) DIRECTOR OF NATIONAL INTELLIGENCE SCIENCE AND TECHNOLOGY COMMITTEE.—(1) There is within the Office of the Director of Science and Technology a Director of National Intelligence Science and Technology Committee.

(2) The Committee shall be composed of the principal science officers of the National Intelligence Program.
"(3) The Committee shall—
   "(A) coordinate advances in research and development related to intelligence; and
   "(B) perform such other functions as the Director of Science and Technology shall prescribe.

"NATIONAL COUNTERINTELLIGENCE EXECUTIVE"

"SEC. 103F. (a) NATIONAL COUNTERINTELLIGENCE EXECUTIVE.—

"(b) DUTIES.—The National Counterintelligence Executive shall perform the duties provided in the Counterintelligence Enhancement Act of 2002 and such other duties as may be prescribed by the Director of National Intelligence or specified by law.

"CENTRAL INTELLIGENCE AGENCY"

"SEC. 104. (a) CENTRAL INTELLIGENCE AGENCY.—There is a Central Intelligence Agency.

"(b) FUNCTION.—The function of the Central Intelligence Agency is to assist the Director of the Central Intelligence Agency in carrying out the responsibilities specified in section 104A(c).

"DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY"

"SEC. 104A. (a) DIRECTOR OF CENTRAL INTELLIGENCE AGENCY.— There is a Director of the Central Intelligence Agency who shall be appointed by the President, by and with the advice and consent of the Senate.

"(b) SUPERVISION.—The Director of the Central Intelligence Agency shall report to the Director of National Intelligence regarding the activities of the Central Intelligence Agency.

"(c) DUTIES.—The Director of the Central Intelligence Agency shall—
   "(1) serve as the head of the Central Intelligence Agency; and
   "(2) carry out the responsibilities specified in subsection (d).

"(d) RESPONSIBILITIES.—The Director of the Central Intelligence Agency shall—
   "(1) collect intelligence through human sources and by other appropriate means, except that the Director of the Central Intelligence Agency shall have no police, subpoena, or law enforcement powers or internal security functions;
   "(2) correlate and evaluate intelligence related to the national security and provide appropriate dissemination of such intelligence;
   "(3) provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the intelligence community authorized to undertake such collection and, in coordination with other departments, agencies, or elements of the United States Government which are authorized to undertake such collection, ensure that the most effective use is made of resources and that appropriate account is taken of the risks
to the United States and those involved in such collection; and

“(4) perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct.

“(e) Termination of Employment of CIA Employees.—(1) Notwithstanding the provisions of any other law, the Director of the Central Intelligence Agency may, in the discretion of the Director, terminate the employment of any officer or employee of the Central Intelligence Agency whenever the Director deems the termination of employment of such officer or employee necessary or advisable in the interests of the United States.

“(2) Any termination of employment of an officer or employee under paragraph (1) shall not affect the right of the officer or employee to seek or accept employment in any other department, agency, or element of the United States Government if declared eligible for such employment by the Office of Personnel Management.

“(f) Coordination With Foreign Governments.—Under the direction of the Director of National Intelligence and in a manner consistent with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director of the Central Intelligence Agency shall coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

(b) Sense of Congress.—It is the sense of Congress that—

(1) the human intelligence officers of the intelligence community have performed admirably and honorably in the face of great personal dangers;

(2) during an extended period of unprecedented investment and improvements in technical collection means, the human intelligence capabilities of the United States have not received the necessary and commensurate priorities;

(3) human intelligence is becoming an increasingly important capability to provide information on the asymmetric threats to the national security of the United States;

(4) the continued development and improvement of a robust and empowered and flexible human intelligence work force is critical to identifying, understanding, and countering the plans and intentions of the adversaries of the United States; and

(5) an increased emphasis on, and resources applied to, enhancing the depth and breadth of human intelligence capabilities of the United States intelligence community must be among the top priorities of the Director of National Intelligence.

(c) Transformation of Central Intelligence Agency.—The Director of the Central Intelligence Agency shall, in accordance with standards developed by the Director in consultation with the Director of National Intelligence—

(1) enhance the analytic, human intelligence, and other capabilities of the Central Intelligence Agency;

(2) develop and maintain an effective language program within the Agency;
(3) emphasize the hiring of personnel of diverse backgrounds for purposes of improving the capabilities of the Agency;
(4) establish and maintain effective relationships between human intelligence and signals intelligence within the Agency at the operational level; and
(5) achieve a more effective balance within the Agency with respect to unilateral operations and liaison operations.
(d) REPORT.—(1) Not later than 180 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall submit to the Director of National Intelligence and the congressional intelligence committees a report setting forth the following:
   (A) A strategy for improving the conduct of analysis (including strategic analysis) by the Central Intelligence Agency, and the progress of the Agency in implementing that strategy.
   (B) A strategy for improving the human intelligence and other capabilities of the Agency, and the progress of the Agency in implementing that strategy.
(2)(A) The information in the report under paragraph (1) on the strategy referred to in paragraph (1)(B) shall—
   (i) identify the number and types of personnel required to implement that strategy;
   (ii) include a plan for the recruitment, training, equipping, and deployment of such personnel; and
   (iii) set forth an estimate of the costs of such activities.
   (B) If as of the date of the report under paragraph (1), a proper balance does not exist between unilateral operations and liaison operations, such report shall set forth the steps to be taken to achieve such balance.

SEC. 1012. REVISED DEFINITION OF NATIONAL INTELLIGENCE.

Paragraph (5) of section 3 of the National Security Act of 1947 (50 U.S.C. 401a) is amended to read as follows:
“(5) The terms ‘national intelligence’ and ‘intelligence related to national security’ refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—
   “(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and
   “(B) that involves—
   “(i) threats to the United States, its people, property, or interests;
   “(ii) the development, proliferation, or use of weapons of mass destruction; or
   “(iii) any other matter bearing on United States national or homeland security.”.

SEC. 1013. JOINT PROCEDURES FOR OPERATIONAL COORDINATION BETWEEN DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY.

(a) DEVELOPMENT OF PROCEDURES.—The Director of National Intelligence, in consultation with the Secretary of Defense and the Director of the Central Intelligence Agency, shall develop joint procedures to be used by the Department of Defense and the Central Intelligence Agency to improve the coordination and deconfliction
of operations that involve elements of both the Armed Forces and the Central Intelligence Agency consistent with national security and the protection of human intelligence sources and methods. Those procedures shall, at a minimum, provide the following:

1. Methods by which the Director of the Central Intelligence Agency and the Secretary of Defense can improve communication and coordination in the planning, execution, and sustainment of operations, including, as a minimum—
   A. information exchange between senior officials of the Central Intelligence Agency and senior officers and officials of the Department of Defense when planning for such an operation commences by either organization; and
   B. exchange of information between the Secretary and the Director of the Central Intelligence Agency to ensure that senior operational officials in both the Department of Defense and the Central Intelligence Agency have knowledge of the existence of the ongoing operations of the other.

2. When appropriate, in cases where the Department of Defense and the Central Intelligence Agency are conducting separate missions in the same geographical area, a mutual agreement on the tactical and strategic objectives for the region and a clear delineation of operational responsibilities to prevent conflict and duplication of effort.

b. IMPLEMENTATION REPORT.—Not later than 180 days after the date of the enactment of the Act, the Director of National Intelligence shall submit to the congressional defense committees (as defined in section 101 of title 10, United States Code) and the congressional intelligence committees (as defined in section 3(7) of the National Security Act of 1947 (50 U.S.C. 401a(7))) a report describing the procedures established pursuant to subsection (a) and the status of the implementation of those procedures.

SEC. 1014. ROLE OF DIRECTOR OF NATIONAL INTELLIGENCE IN APPOINTMENT OF CERTAIN OFFICIALS RESPONSIBLE FOR INTELLIGENCE-RELATED ACTIVITIES.

Section 106 of the National Security Act of 1947 (50 U.S.C. 403–6) is amended by striking all after the heading and inserting the following:

"(a) RECOMMENDATION OF DNI IN CERTAIN APPOINTMENTS.—

1. In the event of a vacancy in a position referred to in paragraph (2), the Director of National Intelligence shall recommend to the President an individual for nomination to fill the vacancy.

2. Paragraph (1) applies to the following positions:

   (A) The Principal Deputy Director of National Intelligence.

   (B) The Director of the Central Intelligence Agency.

(b) CONCURRENCE OF DNI IN APPOINTMENTS TO POSITIONS IN THE INTELLIGENCE COMMUNITY.—(1) In the event of a vacancy in a position referred to in paragraph (2), the head of the department or agency having jurisdiction over the position shall obtain the concurrence of the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy. If the Director does not concur in the recommendation, the head of the department or agency concerned may not fill the vacancy or make the recommendation to the President (as the case may be). In the case in which the Director does not concur in such a recommendation, the Director and the head of the department..."
or agency concerned may advise the President directly of the intention to withhold concurrence or to make a recommendation, as the case may be.

Applicability.

"(2) Paragraph (1) applies to the following positions:

(A) The Director of the National Security Agency.

(B) The Director of the National Reconnaissance Office.

(C) The Director of the National Geospatial-Intelligence Agency.

(D) The Assistant Secretary of State for Intelligence and Research.

(E) The Director of the Office of Intelligence of the Department of Energy.

(F) The Director of the Office of Counterintelligence of the Department of Energy.

(G) The Assistant Secretary for Intelligence and Analysis of the Department of the Treasury.

(H) The Executive Assistant Director for Intelligence of the Federal Bureau of Investigation or any successor to that position.

(I) The Assistant Secretary of Homeland Security for Information Analysis.

(c) CONSULTATION WITH DNI IN CERTAIN POSITIONS.—(1) In the event of a vacancy in a position referred to in paragraph (2), the head of the department or agency having jurisdiction over the position shall consult with the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy.

(2) Paragraph (1) applies to the following positions:

(A) The Director of the Defense Intelligence Agency.

(B) The Assistant Commandant of the Coast Guard for Intelligence.”.

SEC. 1015. EXECUTIVE SCHEDULE MATTERS.

(a) EXECUTIVE SCHEDULE LEVEL I.—Section 5312 of title 5, United States Code, is amended by adding at the end the following new item:

"Director of National Intelligence.”.

(b) EXECUTIVE SCHEDULE LEVEL II.—Section 5313 of title 5, United States Code, is amended by adding at the end the following new items:

"Principal Deputy Director of National Intelligence.

"Director of the National Counterterrorism Center.

"Director of the National Counter Proliferation Center.”.

(c) EXECUTIVE SCHEDULE LEVEL IV.—Section 5315 of title 5, United States Code, is amended—

(1) by striking the item relating to the Assistant Directors of Central Intelligence; and

(2) by adding at the end the following new item:

"General Counsel of the Office of the National Intelligence Director.”.

6 USC 485.

SEC. 1016. INFORMATION SHARING.

(a) DEFINITIONS.—In this section:

(1) INFORMATION SHARING COUNCIL.—The term “Information Sharing Council” means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).
Public Law 107–296
107th Congress

An Act

To establish the Department of Homeland Security, and for other purposes. [H.R. 5005]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Homeland Security Act of 2002”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Construction; severability.
Sec. 4. Effective date.

TITLE I—DEPARTMENT OF HOMELAND SECURITY

Sec. 101. Executive department; mission.
Sec. 102. Secretary; functions.
Sec. 103. Other officers.

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Directorate for Information Analysis and Infrastructure Protection; Access to Information

Sec. 201. Directorate for Information Analysis and Infrastructure Protection.

Subtitle B—Critical Infrastructure Information

Sec. 211. Short title.
Sec. 212. Definitions.
Sec. 213. Designation of critical infrastructure protection program.
Sec. 214. Protection of voluntarily shared critical infrastructure information.
Sec. 215. No private right of action.

Subtitle C—Information Security

Sec. 221. Procedures for sharing information.
Sec. 222. Privacy Officer.
Sec. 223. Enhancement of non-Federal cybersecurity.
Sec. 224. Net guard.

Subtitle D—Office of Science and Technology

Sec. 231. Establishment of office; Director.
Sec. 232. Mission of office; duties.
Sec. 233. Definition of law enforcement technology.
Sec. 234. Abolishment of Office of Science and Technology of National Institute of Justice; transfer of functions.
Sec. 235. National Law Enforcement and Corrections Technology Centers.
Sec. 236. Coordination with other entities within Department of Justice.
Sec. 237. Amendments relating to National Institute of Justice.

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

Sec. 301. Under Secretary for Science and Technology.
Sec. 302. Responsibilities and authorities of the Under Secretary for Science and Technology.
Sec. 303. Functions transferred.
Sec. 304. Conduct of certain public health-related activities.
Sec. 305. Federally funded research and development centers.
Sec. 306. Miscellaneous provisions.
Sec. 308. Conduct of research, development, demonstration, testing and evaluation.
Sec. 309. Utilization of Department of Energy national laboratories and sites in support of homeland security activities.
Sec. 310. Transfer of Plum Island Animal Disease Center, Department of Agriculture.
Sec. 311. Homeland Security Science and Technology Advisory Committee.
Sec. 313. Technology clearinghouse to encourage and support innovative solutions to enhance homeland security.

TITLE IV—DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY

Subtitle A—Under Secretary for Border and Transportation Security
Sec. 401. Under Secretary for Border and Transportation Security.
Sec. 402. Responsibilities.
Sec. 403. Functions transferred.

Subtitle B—United States Customs Service
Sec. 411. Establishment; Commissioner of Customs.
Sec. 412. Retention of customs revenue functions by Secretary of the Treasury.
Sec. 413. Preservation of customs funds.
Sec. 414. Separate budget request for customs.
Sec. 415. Definition.
Sec. 416. GAO report to Congress.
Sec. 417. Allocation of resources by the Secretary.
Sec. 418. Reports to Congress.
Sec. 419. Customs user fees.

Subtitle C—Miscellaneous Provisions
Sec. 421. Transfer of certain agricultural inspection functions of the Department of Agriculture.
Sec. 422. Functions of Administrator of General Services.
Sec. 423. Functions of Transportation Security Administration.
Sec. 424.Preservation of Transportation Security Administration as a distinct entity.
Sec. 425. Explosive detection systems.
Sec. 426. Transportation security.
Sec. 427. Coordination of information and information technology.
Sec. 428. Visa issuance.
Sec. 429. Information on visa denials required to be entered into electronic data system.
Sec. 430. Office for Domestic Preparedness.

Subtitle D—Immigration Enforcement Functions
Sec. 441. Transfer of functions to Under Secretary for Border and Transportation Security.
Sec. 442. Establishment of Bureau of Border Security.
Sec. 443. Professional responsibility and quality review.
Sec. 444. Employee discipline.
Sec. 446. Sense of Congress regarding construction of fencing near San Diego, California.

Subtitle E—Citizenship and Immigration Services
Sec. 452. Citizenship and Immigration Services Ombudsman.
Sec. 453. Professional responsibility and quality review.
Sec. 454. Employee discipline.
Sec. 455. Effective date.
Sec. 456. Transition.
Sec. 457. Funding for citizenship and immigration services.
Sec. 458. Backlog elimination.
Sec. 459. Report on improving immigration services.
Sec. 460. Report on responding to fluctuating needs.
Sec. 461. Application of Internet-based technologies.
Sec. 462. Children's affairs.

Subtitle F—General Immigration Provisions
Sec. 471. Abolishment of INS.
Sec. 472. Voluntary separation incentive payments.
Sec. 473. Authority to conduct a demonstration project relating to disciplinary ac-
tion.
Sec. 474. Sense of Congress.
Sec. 475. Director of Shared Services.
Sec. 476. Separation of funding.
Sec. 477. Reports and implementation plans.
Sec. 478. Immigration functions.

TITLE V—EMERGENCY PREPAREDNESS AND RESPONSE
Sec. 501. Under Secretary for Emergency Preparedness and Response.
Sec. 502. Responsibilities.
Sec. 503. Functions transferred.
Sec. 504. Nuclear incident response.
Sec. 505. Conduct of certain public health-related activities.
Sec. 506. Definition.
Sec. 507. Role of Federal Emergency Management Agency.
Sec. 508. Use of national private sector networks in emergency response.
Sec. 509. Use of commercially available technology, goods, and services.

TITLE VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE
ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL
ORGANIZATIONS
Sec. 601. Treatment of charitable trusts for members of the Armed Forces of the
United States and other governmental organizations.

TITLE VII—MANAGEMENT
Sec. 701. Under Secretary for Management.
Sec. 702. Chief Financial Officer.
Sec. 703. Chief Information Officer.
Sec. 704. Chief Human Capital Officer.
Sec. 705. Establishment of Officer for Civil Rights and Civil Liberties.
Sec. 706. Consolidation and co-location of offices.

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR
GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL
PROVISIONS
Subtitle A—Coordination with Non-Federal Entities
Sec. 801. Office for State and Local Government Coordination.

Subtitle B—Inspector General
Sec. 811. Authority of the Secretary.
Sec. 812. Law enforcement powers of Inspector General agents.

Subtitle C—United States Secret Service
Sec. 821. Functions transferred.

Subtitle D—Acquisitions
Sec. 831. Research and development projects.
Sec. 832. Personal services.
Sec. 833. Special streamlined acquisition authority.
Sec. 834. Unsolicited proposals.
Sec. 835. Prohibition on contracts with corporate expatriates.

Subtitle E—Human Resources Management
Sec. 841. Establishment of Human Resources Management System.
Sec. 842. Labor-management relations.

Subtitle F—Federal Emergency Procurement Flexibility
Sec. 851. Definition.
Sec. 852. Procurements for defense against or recovery from terrorism or nuclear,
biological, chemical, or radiological attack.
Sec. 833. Increased simplified acquisition threshold for procurements in support of humanitarian or peacekeeping operations or contingency operations.

Sec. 854. Increased micro-purchase threshold for certain procurements.

Sec. 855. Application of certain commercial items authorities to certain procurements.

Sec. 856. Use of streamlined procedures.

Sec. 857. Review and report by Comptroller General.

Sec. 858. Identification of new entrants into the Federal marketplace.

Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002

Sec. 861. Short title.

Sec. 862. Administration.

Sec. 863. Litigation management.

Sec. 864. Risk management.

Sec. 865. Definitions.

Subtitle H—Miscellaneous Provisions

Sec. 871. Advisory committees.

Sec. 872. Reorganization.

Sec. 873. Use of appropriated funds.

Sec. 874. Future Year Homeland Security Program.

Sec. 875. Miscellaneous authorities.

Sec. 876. Military activities.

Sec. 877. Regulatory authority and preemption.

Sec. 878. Counternarcotics officers.

Sec. 879. Office of International Affairs.

Sec. 880. Prohibition of the Terrorism Information and Prevention System.

Sec. 881. Review of pay and benefit plans.

Sec. 882. Office for National Capital Region Coordination.

Sec. 883. Requirement to comply with laws protecting equal employment opportunity and providing whistleblower protections.

Sec. 884. Federal Law Enforcement Training Center.

Sec. 885. Joint Interagency Task Force.

Sec. 886. Sense of Congress reaffirming the continued importance and applicability of the Posse Comitatus Act.

Sec. 887. Coordination with the Department of Health and Human Services under the Public Health Service Act.

Sec. 888. Preserving Coast Guard mission performance.

Sec. 889. Homeland security funding analysis in President’s budget.

Sec. 890. Air Transportation Safety and System Stabilization Act.

Subtitle I—Information Sharing

Sec. 891. Short title; findings; and sense of Congress.

Sec. 892. Facilitating homeland security information sharing procedures.

Sec. 893. Report.

Sec. 894. Authorization of appropriations.

Sec. 895. Authority to share grand jury information.

Sec. 896. Authority to share electronic, wire, and oral interception information.

Sec. 897. Foreign intelligence information.

Sec. 898. Information acquired from an electronic surveillance.

Sec. 899. Information acquired from a physical search.

TITLE IX—NATIONAL HOMELAND SECURITY COUNCIL


Sec. 902. Function.

Sec. 903. Membership.

Sec. 904. Other functions and activities.

Sec. 905. Staff composition.

Sec. 906. Relation to the National Security Council.

TITLE X—INFORMATION SECURITY

Sec. 1001. Information security.

Sec. 1002. Management of information technology.

Sec. 1003. National Institute of Standards and Technology.

Sec. 1004. Information Security and Privacy Advisory Board.

Sec. 1005. Technical and conforming amendments.

Sec. 1006. Construction.

TITLE XI—DEPARTMENT OF JUSTICE DIVISIONS

Subtitle A—Executive Office for Immigration Review

Sec. 1101. Legal status of EOIR.
Sec. 1102. Authorities of the Attorney General.
Sec. 1103. Statutory construction.

Subtitle B—Transfer of the Bureau of Alcohol, Tobacco and Firearms to the
Department of Justice

Sec. 1111. Bureau of Alcohol, Tobacco, Firearms, and Explosives.
Sec. 1112. Technical and conforming amendments.
Sec. 1113. Powers of agents of the Bureau of Alcohol, Tobacco, Firearms, and
Explosives.
Sec. 1114. Explosives training and research facility.
Sec. 1115. Personnel management demonstration project.

Subtitle C—Explosives

Sec. 1121. Short title.
Sec. 1122. Permits for purchasers of explosives.
Sec. 1123. Persons prohibited from receiving or possessing explosive materials.
Sec. 1124. Requirement to provide samples of explosive materials and ammonium
nitrate.
Sec. 1125. Destruction of property of institutions receiving Federal financial assis-
tance.
Sec. 1126. Relief from disabilities.
Sec. 1127. Theft reporting requirement.
Sec. 1128. Authorization of appropriations.

TITLE XII—AIRLINE WAR RISK INSURANCE LEGISLATION

Sec. 1201. Air carrier liability for third party claims arising out of acts of terrorism.
Sec. 1202. Extension of insurance policies.
Sec. 1203. Correction of reference.
Sec. 1204. Report.

TITLE XIII—FEDERAL WORKFORCE IMPROVEMENT

Subtitle A—Chief Human Capital Officers

Sec. 1301. Short title.
Sec. 1302. Agency Chief Human Capital Officers.
Sec. 1303. Chief Human Capital Officers Council.
Sec. 1304. Strategic human capital management.
Sec. 1305. Effective date.

Subtitle B—Reforms Relating to Federal Human Capital Management

Sec. 1311. Inclusion of agency human capital strategic planning in performance
plans and programs performance reports.
Sec. 1312. Reform of the competitive service hiring process.
Sec. 1313. Permanent extension, revision, and expansion of authorities for use of
voluntary separation incentive pay and voluntary early retirement.
Sec. 1314. Student volunteer transit subsidy.

Subtitle C—Reforms Relating to the Senior Executive Service

Sec. 1321. Repeal of recertification requirements of senior executives.
Sec. 1322. Adjustment of limitation on total annual compensation.

Subtitle D—Academic Training

Sec. 1331. Academic training.
Sec. 1332. Modifications to National Security Education Program.

TITLE XIV—ARMING PILOTS AGAINST TERRORISM

Sec. 1401. Short title.
Sec. 1402. Federal Flight Deck Officer Program.
Sec. 1403. Crew training.
Sec. 1404. Commercial airline security study.
Sec. 1405. Authority to arm flight deck crew with less-than-lethal weapons.
Sec. 1406. Technical amendments.

TITLE XV—TRANSITION

Subtitle A—Reorganization Plan

Sec. 1501. Definitions.
Sec. 1502. Reorganization plan.
Sec. 1503. Review of congressional committee structures.

Subtitle B—Transitional Provisions

Sec. 1511. Transitional authorities.
Sec. 1512. Savings provisions.
Sec. 1513. Terminations.
Sec. 1514. National identification system not authorized.
Sec. 1515. Continuity of Inspector General oversight.
Sec. 1516. Incidental transfers.
Sec. 1517. Reference.

TITLE XVI—CORRECTIONS TO EXISTING LAW RELATING TO AIRLINE TRANSPORTATION SECURITY

Sec. 1601. Retention of security sensitive information authority at Department of Transportation.
Sec. 1602. Increase in civil penalties.
Sec. 1603. Allowing United States citizens and United States nationals as screeners.

TITLE XVII—CONFORMING AND TECHNICAL AMENDMENTS

Sec. 1702. Executive Schedule.
Sec. 1703. United States Secret Service.
Sec. 1704. Coast Guard.
Sec. 1705. Strategic national stockpile and smallpox vaccine development.
Sec. 1706. Transfer of certain security and law enforcement functions and authorities.
Sec. 1707. Transportation security regulations.
Sec. 1709. Collaboration with the Secretary of Homeland Security.
Sec. 1710. Railroad safety to include railroad security.
Sec. 1711. Hazmat safety to include hazmat security.
Sec. 1712. Office of Science and Technology Policy.
Sec. 1713. National Oceanographic Partnership Program.
Sec. 1714. Clarification of definition of manufacturer.
Sec. 1715. Clarification of definition of vaccine-related injury or death.
Sec. 1716. Clarification of definition of vaccine.
Sec. 1717. Effective date.

SEC. 2. DEFINITIONS.

In this Act, the following definitions apply:

(1) Each of the terms “American homeland” and “homeland” means the United States.

(2) The term “appropriate congressional committee” means any committee of the House of Representatives or the Senate having legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.

(3) The term “assets” includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

(4) The term “critical infrastructure” has the meaning given that term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).


(6) The term “emergency response providers” includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

(7) The term “executive agency” means an executive agency and a military department, as defined, respectively, in sections 105 and 102 of title 5, United States Code.

(8) The term “functions” includes authorities, powers, rights, privileges, immunities, programs, projects, activities, duties, and responsibilities.
(9) The term "key resources" means publicly or privately controlled resources essential to the minimal operations of the economy and government.

(10) The term "local government" means—

(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(C) a rural community, unincorporated town or village, or other public entity.

(11) The term "major disaster" has the meaning given in section 102(2) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(12) The term "personnel" means officers and employees.

(13) The term "Secretary" means the Secretary of Homeland Security.

(14) The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(15) The term "terrorism" means any activity that—

(A) involves an act that—

(i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and

(ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and

(B) appears to be intended—

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

(16)(A) The term "United States", when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

(B) Nothing in this paragraph or any other provision of this Act shall be construed to modify the definition of "United States" for the purposes of the Immigration and Nationality Act or any other immigration or nationality law.

SEC. 3. CONSTRUCTION; SEVERABILITY.

Any provision of this Act held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, shall be construed so as to give it the maximum effect permitted by
law, unless such holding shall be one of utter invalidity or unenforceability, in which event such provision shall be deemed severable from this Act and shall not affect the remainder thereof, or the application of such provision to other persons not similarly situated or to other, dissimilar circumstances.

SEC. 4. EFFECTIVE DATE.

This Act shall take effect 60 days after the date of enactment.

TITLE I—DEPARTMENT OF HOMELAND SECURITY

SEC. 101. EXECUTIVE DEPARTMENT; MISSION.

(a) ESTABLISHMENT.—There is established a Department of Homeland Security, as an executive department of the United States within the meaning of title 5, United States Code.

(b) MISSION.—

(1) IN GENERAL.—The primary mission of the Department is to—

(A) prevent terrorist attacks within the United States;
(B) reduce the vulnerability of the United States to terrorism;
(C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;
(D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;
(E) ensure that the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;
(F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland; and
(G) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

(2) RESPONSIBILITY FOR INVESTIGATING AND PROSECUTING TERRORISM.—Except as specifically provided by law with respect to entities transferred to the Department under this Act, primary responsibility for investigating and prosecuting acts of terrorism shall be vested not in the Department, but rather in Federal, State, and local law enforcement agencies with jurisdiction over the acts in question.

SEC. 102. SECRETARY; FUNCTIONS.

(a) SECRETARY.—

(1) IN GENERAL.—There is a Secretary of Homeland Security, appointed by the President, by and with the advice and consent of the Senate.

(2) HEAD OF DEPARTMENT.—The Secretary is the head of the Department and shall have direction, authority, and control over it.
(3) **FUNCTIONS VESTED IN SECRETARY.**—All functions of all officers, employees, and organizational units of the Department are vested in the Secretary.

(b) **FUNCTIONS.**—The Secretary—

(1) except as otherwise provided by this Act, may delegate any of the Secretary's functions to any officer, employee, or organizational unit of the Department;

(2) shall have the authority to make contracts, grants, and cooperative agreements, and to enter into agreements with other executive agencies, as may be necessary and proper to carry out the Secretary's responsibilities under this Act or otherwise provided by law; and

(3) shall take reasonable steps to ensure that information systems and databases of the Department are compatible with each other and with appropriate databases of other Departments.

(c) **COORDINATION WITH NON-FEDERAL ENTITIES.**—With respect to homeland security, the Secretary shall coordinate through the Office of State and Local Coordination (established under section 801) (including the provision of training and equipment) with State and local government personnel, agencies, and authorities, with the private sector, and with other entities, including by—

(1) coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities;

(2) coordinating and, as appropriate, consolidating, the Federal Government's communications and systems of communications relating to homeland security with State and local government personnel, agencies, and authorities, the private sector, other entities, and the public; and

(3) distributing or, as appropriate, coordinating the distribution of, warnings and information to State and local government personnel, agencies, and authorities and to the public.

(d) **MEETINGS OF NATIONAL SECURITY COUNCIL.**—The Secretary may, subject to the direction of the President, attend and participate in meetings of the National Security Council.

(e) **ISSUANCE OF REGULATIONS.**—The issuance of regulations by the Secretary shall be governed by the provisions of chapter 5 of title 5, United States Code, except as specifically provided in this Act, in laws granting regulatory authorities that are transferred by this Act, and in laws enacted after the date of enactment of this Act.

(f) **SPECIAL ASSISTANT TO THE SECRETARY.**—The Secretary shall appoint a Special Assistant to the Secretary who shall be responsible for—

(1) creating and fostering strategic communications with the private sector to enhance the primary mission of the Department to protect the American homeland;

(2) advising the Secretary on the impact of the Department's policies, regulations, processes, and actions on the private sector;

(3) interfacing with other relevant Federal agencies with homeland security missions to assess the impact of these agencies' actions on the private sector;
(4) creating and managing private sector advisory councils composed of representatives of industries and associations designated by the Secretary to—
   (A) advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges; and
   (B) advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations;
(5) working with Federal laboratories, federally funded research and development centers, other federally funded organizations, academia, and the private sector to develop innovative approaches to address homeland security challenges to produce and deploy the best available technologies for homeland security missions;
(6) promoting existing public-private partnerships and developing new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges; and
(7) assisting in the development and promotion of private sector best practices to secure critical infrastructure.

(g) STANDARDS POLICY.—All standards activities of the Department shall be conducted in accordance with section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. 272 note) and Office of Management and Budget Circular A–119.

6 USC 113.

SEC. 103. OTHER OFFICERS.

(a) DEPUTY SECRETARY; UNDER SECRETARIES.—There are the following officers, appointed by the President, by and with the advice and consent of the Senate:

   (1) A Deputy Secretary of Homeland Security, who shall be the Secretary's first assistant for purposes of subchapter III of chapter 5 of title 5, United States Code.
   (2) An Under Secretary for Information Analysis and Infrastructure Protection.
   (3) An Under Secretary for Science and Technology.
   (4) An Under Secretary for Border and Transportation Security.
   (6) A Director of the Bureau of Citizenship and Immigration Services.
   (7) An Under Secretary for Management.
   (8) Not more than 12 Assistant Secretaries.
   (9) A General Counsel, who shall be the chief legal officer of the Department.

(b) INSPECTOR GENERAL.—There is an Inspector General, who shall be appointed as provided in section 3(a) of the Inspector General Act of 1978.

(c) COMMANDANT OF THE COAST GUARD.—To assist the Secretary in the performance of the Secretary's functions, there is a Commandant of the Coast Guard, who shall be appointed as provided in section 44 of title 14, United States Code, and who shall report directly to the Secretary. In addition to such duties as may be provided in this Act and as assigned to the Commandant by the Secretary, the duties of the Commandant shall include those required by section 2 of title 14, United States Code.
(d) **OTHER OFFICERS.**—To assist the Secretary in the performance of the Secretary’s functions, there are the following officers, appointed by the President:

1. A Director of the Secret Service.
2. A Chief Information Officer.
3. A Chief Human Capital Officer.
5. An Officer for Civil Rights and Civil Liberties.

(e) **PERFORMANCE OF SPECIFIC FUNCTIONS.**—Subject to the provisions of this Act, every officer of the Department shall perform the functions specified by law for the official’s office or prescribed by the Secretary.

**TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION**

**Subtitle A—Directorate for Information Analysis and Infrastructure Protection; Access to Information**

**SEC. 201. DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.**

(a) **UNDER SECRETARY OF HOMELAND SECURITY FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.**—

1. **IN GENERAL.**—There shall be in the Department a Directorate for Information Analysis and Infrastructure Protection headed by an Under Secretary for Information Analysis and Infrastructure Protection, who shall be appointed by the President, by and with the advice and consent of the Senate.

2. **RESPONSIBILITIES.**—The Under Secretary shall assist the Secretary in discharging the responsibilities assigned by the Secretary.

(b) **ASSISTANT SECRETARY FOR INFORMATION ANALYSIS; ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.**—

1. **ASSISTANT SECRETARY FOR INFORMATION ANALYSIS.**—There shall be in the Department an Assistant Secretary for Information Analysis, who shall be appointed by the President.

2. **ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.**—There shall be in the Department an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President.

3. **RESPONSIBILITIES.**—The Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection shall assist the Under Secretary for Information Analysis and Infrastructure Protection in discharging the responsibilities of the Under Secretary under this section.

(c) **DISCHARGE OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.**—The Secretary shall ensure that the responsibilities of the Department regarding information analysis and infrastructure protection are carried out through the Under Secretary for Information Analysis and Infrastructure Protection.

(d) **RESPONSIBILITIES OF UNDER SECRETARY.**—Subject to the direction and control of the Secretary, the responsibilities of the
Under Secretary for Information Analysis and Infrastructure Protection shall be as follows:

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to—

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

(4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

(6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

(7) To administer the Homeland Security Advisory System, including—

(A) exercising primary responsibility for public advisories related to threats to homeland security; and

(B) in coordination with other agencies of the Federal Government, providing specific warning information, and advice about appropriate protective measures and countermeasures, to State and local government agencies and authorities, the private sector, other entities, and the public.
Executive Order 13467 of June 30, 2008

Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for Government employment, contractor employee fitness, and eligibility for access to classified information, while taking appropriate account of title III of Public Law 108–458, it is hereby ordered as follows:

PART I—POLICY, APPLICABILITY, AND DEFINITIONS

Section 1.1. Policy. Executive branch policies and procedures relating to suitability, contractor employee fitness, eligibility to hold a sensitive position, access to federally controlled facilities and information systems, and eligibility for access to classified information shall be aligned using consistent standards to the extent possible, provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our Nation's business and protect national security.

Sec. 1.2. Applicability. (a) This order applies to all covered individuals as defined in section 1.3(g), except that:

(i) the provisions regarding eligibility for physical access to federally controlled facilities and logical access to federally controlled information systems do not apply to individuals exempted in accordance with guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107–347) and Homeland Security Presidential Directive 12; and

(ii) the qualification standards for enlistment, appointment, and induction into the Armed Forces pursuant to title 10, United States Code, are unaffected by this order.

(b) This order also applies to investigations and determinations of eligibility for access to classified information for employees of agencies working in or for the legislative or judicial branches when those investigations or determinations are conducted by the executive branch.

Sec. 1.3. Definitions. For the purpose of this order:

(a) “Adjudication” means the evaluation of pertinent data in a background investigation, as well as any other available information, that is relevant and reliable, to determine whether a covered individual is:

(i) suitable for Government employment;

(ii) eligible for logical and physical access;

(iii) eligible for access to classified information;

(iv) eligible to hold a sensitive position; or

(v) fit to perform work for or on behalf of the Government as a contractor employee.

(b) “Agency” means any “Executive agency” as defined in section 105 of title 5, United States Code, including the “military departments,” as defined in section 102 of title 5, United States Code, and any other entity.
within the executive branch that comes into possession of classified information or has designated positions as sensitive, except such an entity headed by an officer who is not a covered individual.

(c) "Classified information" means information that has been determined pursuant to Executive Order 12958 of April 17, 1995, as amended, or a successor or predecessor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

(d) "Continuous evaluation" means reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.

(e) "Contractor" means an expert or consultant (not appointed under section 3109 of title 5, United States Code) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of an agency (but not a Federal employee).

(f) "Contractor employee fitness" means fitness based on character and conduct for work for or on behalf of the Government as a contractor employee.

(g) "Covered individual" means a person who performs work for or on behalf of the executive branch, or who seeks to perform work for or on behalf of the executive branch, but does not include:

(i) the President or (except to the extent otherwise directed by the President) employees of the President under section 105 or 107 of title 3, United States Code; or

(ii) the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under section 106 of title 3 or annual legislative branch appropriations acts.

(h) "End-to-end automation" means an executive branch-wide federated system that uses automation to manage and monitor cases and maintain relevant documentation of the application (but not an employment application), investigation, adjudication, and continuous evaluation processes.

(i) "Federally controlled facilities" and "federally controlled information systems" have the meanings prescribed in guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107–347) and Homeland Security Presidential Directive 12.

(j) "Logical and physical access" means access other than occasional or intermittent access to federally controlled facilities or information systems.

(k) "Sensitive position" means any position so designated under Executive Order 10450 of April 27, 1953, as amended.

(l) "Suitability" has the meaning and coverage provided in 5 CFR Part 731.

PART 2—ALIGNMENT, RECIPROCITY, AND GOVERNANCE

Sec. 2.1. Aligned System. (a) Investigations and adjudications of covered individuals who require a determination of suitability, eligibility for logical and physical access, eligibility to hold a sensitive position, eligibility for access to classified information, and, as appropriate, contractor employee fitness, shall be aligned using consistent standards to the extent possible. Each successively higher level of investigation and adjudication shall build upon, but not duplicate, the ones below it.

(b) The aligned system shall employ updated and consistent standards and methods, enable innovations with enterprise information technology capabilities and end-to-end automation to the extent practicable, and ensure that relevant information maintained by agencies can be accessed and shared.
rapidly across the executive branch, while protecting national security, protecting privacy-related information, ensuring resulting decisions are in the national interest, and providing the Federal Government with an effective workforce.

(c) Except as otherwise authorized by law, background investigations and adjudications shall be mutually and reciprocally accepted by all agencies. An agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination consistent with law, directive, or regulation) that exceed the requirements for suitability, contractor employee fitness, eligibility for logical or physical access, eligibility to hold a sensitive position, or eligibility for access to classified information without the approval of the Suitability Executive Agent or Security Executive Agent, as appropriate, and provided that approval to establish additional requirements shall be limited to circumstances where additional requirements are necessary to address significant needs unique to the agency involved or to protect national security.

Sec. 2.2. Establishment and Functions of Performance Accountability Council.
(a) There is hereby established a Suitability and Security Clearance Performance Accountability Council (Council).

(b) The Deputy Director for Management, Office of Management and Budget, shall serve as Chair of the Council and shall have authority, direction, and control over the Council's functions. Membership on the Council shall include the Suitability Executive Agent and the Security Executive Agent. The Chair shall select a Vice Chair to act in the Chair's absence. The Chair shall have authority to designate officials from additional agencies who shall serve as members of the Council. Council membership shall be limited to Federal Government employees and shall include suitability and security professionals.

(c) The Council shall be accountable to the President to achieve, consistent with this order, the goals of reform, and is responsible for driving implementation of the reform effort, ensuring accountability by agencies, ensuring the Suitability Executive Agent and the Security Executive Agent align their respective processes, and sustaining reform momentum.

(d) The Council shall:
   (i) ensure alignment of suitability, security, and, as appropriate, contractor employee fitness investigative and adjudicative processes;
   (ii) hold agencies accountable for the implementation of suitability, security, and, as appropriate, contractor employee fitness processes and procedures;
   (iii) establish requirements for enterprise information technology;
   (iv) establish annual goals and progress metrics and prepare annual reports on results;
   (v) ensure and oversee the development of tools and techniques for enhancing background investigations and the making of eligibility determinations;
   (vi) arbitrate disparities in procedures between the Suitability Executive Agent and the Security Executive Agent;
   (vii) ensure sharing of best practices; and
   (viii) advise the Suitability Executive Agent and the Security Executive Agent on policies affecting the alignment of investigations and adjudications.

(e) The Chair may, to ensure the effective implementation of the policy set forth in section 1.1 of this order and to the extent consistent with law, assign, in whole or in part, to the head of any agency (solely or jointly) any function within the Council's responsibility relating to alignment and improvement of investigations and determinations of suitability, contractor employee fitness, eligibility for logical and physical access, eligibility for access to classified information, or eligibility to hold a sensitive position.
Sec. 2.3. Establishment, Designation, and Functions of Executive Agents. (a) There is hereby established a Suitability Executive Agent and a Security Executive Agent.

(b) The Director of the Office of Personnel Management shall serve as the Suitability Executive Agent. As the Suitability Executive Agent, the Director of the Office of Personnel Management will continue to be responsible for developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access.

(c) The Director of National Intelligence shall serve as the Security Executive Agent. The Security Executive Agent:

(i) shall direct the oversight of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position made by any agency;

(ii) shall be responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position;

(iii) may issue guidelines and instructions to the heads of agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position;

(iv) shall serve as the final authority to designate an agency or agencies to conduct investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position;

(v) shall serve as the final authority to designate an agency or agencies to determine eligibility for access to classified information in accordance with Executive Order 12968 of August 2, 1995;

(vi) shall ensure reciprocal recognition of eligibility for access to classified information among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position; and

(vii) may assign, in whole or in part, to the head of any agency (solely or jointly) any of the functions detailed in (i) through (vi), above, with the agency’s exercise of such assigned functions to be subject to the Security Executive Agent’s oversight and with such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate.

(d) Nothing in this order shall be construed in a manner that would limit the authorities of the Director of the Office of Personnel Management or the Director of National Intelligence under law.

Sec. 2.4. Additional Functions. (a) The duties assigned to the Security Policy Board by Executive Order 12968 of August 2, 1995, to consider, coordinate, and recommend policy directives for executive branch security policies, procedures, and practices are reassigned to the Security Executive Agent.

(b) Heads of agencies shall:

(i) carry out any function assigned to the agency head by the Chair, and shall assist the Chair, the Council, the Suitability Executive Agent, and the Security Executive Agent in carrying out any function under sections 2.2 and 2.3 of this order;

(ii) implement any policy or procedure developed pursuant to this order;

(iii) to the extent permitted by law, make available to the Performance Accountability Council, the Suitability Executive Agent, or the Security

166
Executive Agent such information as may be requested to implement this order;

(iv) ensure that all actions taken under this order take account of the counterintelligence interests of the United States, as appropriate; and

(v) ensure that actions taken under this order are consistent with the President's constitutional authority to:
   (A) conduct the foreign affairs of the United States;
   (B) withhold information the disclosure of which could impair the foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties;
   (C) recommend for congressional consideration such measures as the President may judge necessary or expedient; and
   (D) supervise the unitary executive branch.

PART 3—MISCELLANEOUS

Sec. 3. General Provisions. (a) Executive Order 13381 of June 27, 2005, as amended, is revoked. Nothing in this order shall:

(i) supersede, impede, or otherwise affect:
   (A) Executive Order 10450 of April 27, 1953, as amended;
   (B) Executive Order 10577 of November 23, 1954, as amended;
   (C) Executive Order 12333 of December 4, 1981, as amended;
   (D) Executive Order 12829 of January 6, 1993, as amended; or
   (E) Executive Order 12958 of April 17, 1995, as amended; nor

(ii) diminish or otherwise affect the denial and revocation procedures provided to individuals covered by Executive Order 10865 of February 20, 1960, as amended.

(b) Executive Order 12968 of August 2, 1995 is amended:

(i) by inserting: “Sec. 3.5. Continuous Evaluation. An individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence.”; and

(ii) by striking “the Security Policy Board shall make recommendations to the President through the Assistant to the President for National Security Affairs” in section 6.3(a) and inserting in lieu thereof “the Director of National Intelligence shall serve as the final authority”;

(iii) by striking “Security Policy Board” and inserting in lieu thereof “Security Executive Agent” in each instance;

(iv) by striking “the Board” in section 1.1(j) and inserting in lieu thereof “the Security Executive Agent”; and

(v) by inserting “or appropriate automated procedures” in section 3.1(b) after “by appropriately trained adjudicative personnel”.

(c) Nothing in this order shall supersede, impede, or otherwise affect the remainder of Executive Order 12968 of August 2, 1995, as amended.

(d) Executive Order 12171 of November 19, 1979, as amended, is further amended by striking “The Center for Federal Investigative Services” in section 1–216 and inserting in lieu thereof “The Federal Investigative Services Division.”

(e) Nothing in this order shall be construed to impair or otherwise affect the:

(i) authority granted by law to a department or agency, or the head thereof; or

(ii) functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.
(g) Existing delegations of authority made pursuant to Executive Order 13381 of June 27, 2005, as amended, to any agency relating to granting eligibility for access to classified information and conducting investigations shall remain in effect, subject to the exercise of authorities pursuant to this order to revise or revoke such delegation.

(h) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(i) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its agencies, instrumentalities, or entities, its officers or employees, or any other person.

THE WHITE HOUSE,
June 30, 2008.

[FR Doc. 08–1409
Filed 7–1–08; 11:00 am]
Billing code 3195–W8–P
THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release January 17, 2014

January 17, 2014

PRESIDENTIAL POLICY DIRECTIVE/PPD-28

SUBJECT: Signals Intelligence Activities

The United States, like other nations, has gathered intelligence throughout its history to ensure that national security and foreign policy decisionmakers have access to timely, accurate, and insightful information.

The collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm. At the same time, signals intelligence activities and the possibility that such activities may be improperly disclosed to the public pose multiple risks. These include risks to: our relationships with other nations, including the cooperation we receive from other nations on law enforcement, counterterrorism, and other issues; our commercial, economic, and financial interests, including a potential loss of international trust in U.S. firms and the decreased willingness of other nations to participate in international data sharing, privacy, and regulatory regimes; the credibility of our commitment to an open, interoperable, and secure global Internet; and the protection of intelligence sources and methods.

In addition, our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

In determining why, whether, when, and how the United States conducts signals intelligence activities, we must weigh all of these considerations in a context in which information and communications technologies are constantly changing. The evolution of technology has created a world where communications important to our national security and the communications all of us make as part of our daily lives are transmitted through the same channels. This presents new and diverse opportunities for, and challenges with respect to, the collection of intelligence — and especially signals intelligence. The United States Intelligence Community (IC) has achieved remarkable success in developing enhanced capabilities to perform its signals intelligence mission in this rapidly changing world, and these enhanced capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment.¹ The

¹ For the purposes of this directive, the terms "Intelligence Community" and "elements of the Intelligence Community" shall have the same meaning as they do in Executive Order 12333 of December 4, 1981, as amended (Executive Order 12333).
United States must preserve and continue to develop a robust and technologically advanced signals intelligence capability to protect our security and that of our partners and allies. Our signals intelligence capabilities must also be agile enough to enable us to focus on fleeting opportunities or emerging crises and to address not only the issues of today, but also the issues of tomorrow, which we may not be able to foresee.

Advanced technologies can increase risks, as well as opportunities, however, and we must consider these risks when deploying our signals intelligence capabilities. The IC conducts signals intelligence activities with care and precision to ensure that its collection, retention, use, and dissemination of signals intelligence account for these risks. In light of the evolving technological and geopolitical environment, we must continue to ensure that our signals intelligence policies and practices appropriately take into account our alliances and other partnerships; the leadership role that the United States plays in upholding democratic principles and universal human rights; the increased globalization of trade, investment, and information flows; our commitment to an open, interoperable and secure global Internet; and the legitimate privacy and civil liberties concerns of U.S. citizens and citizens of other nations.

Presidents have long directed the acquisition of foreign intelligence and counterintelligence pursuant to their constitutional authority to conduct U.S. foreign relations and to fulfill their constitutional responsibilities as Commander in Chief and Chief Executive. They have also provided direction on the conduct of intelligence activities in furtherance of these authorities and responsibilities, as well as in execution of laws enacted by the Congress. Consistent with this historical practice, this directive articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes.

Section 1. Principles Governing the Collection of Signals Intelligence.

Signals intelligence collection shall be authorized and conducted consistent with the following principles:

(a) The collection of signals intelligence shall be authorized by statute or Executive Order, proclamation, or other Presidential directive, and undertaken in

2 For the purposes of this directive, the terms "foreign intelligence" and "counterintelligence" shall have the same meaning as they have in Executive Order 12333. Thus, "foreign intelligence" means "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists," and "counterintelligence" means "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities." Executive Order 12333 further notes that "[i]ntelligence includes foreign intelligence and counterintelligence."

3 Unless otherwise specified, this directive shall apply to signals intelligence activities conducted in order to collect communications or information about communications, except that it shall not apply to signals intelligence activities undertaken to test or develop signals intelligence capabilities.
accordance with the Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives.

(b) Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.

(c) The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.

(d) Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.

Sec. 2. Limitations on the Use of Signals Intelligence Collected in Bulk.

Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern global communications. The United States must consequently collect signals intelligence in bulk in certain circumstances in order to identify these threats. Routine communications and communications of national security interest increasingly transit the same networks, however, and the collection of signals intelligence in bulk may consequently result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value. The United States will therefore impose new limits on its use of signals intelligence collected in bulk. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.

In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data

4 Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage.

3 The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection. References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).
only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S. or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section. In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified in this section.

The Assistant to the President and National Security Advisor (APNSA), in consultation with the Director of National Intelligence (DNI), shall coordinate, on at least an annual basis, a review of the permissible uses of signals intelligence collected in bulk through the National Security Council Principals and Deputies Committee system identified in PPD-1 or any successor document. At the end of this review, I will be presented with recommended additions to or removals from the list of the permissible uses of signals intelligence collected in bulk.

The DNI shall maintain a list of the permissible uses of signals intelligence collected in bulk. This list shall be updated as necessary and made publicly available to the maximum extent feasible, consistent with the national security.

Sec. 3. Refining the Process for Collecting Signals Intelligence.

U.S. intelligence collection activities present the potential for national security damage if improperly disclosed. Signals intelligence collection raises special concerns, given the opportunities and risks created by the constantly evolving technological and geopolitical environment; the unique nature of such collection and the inherent concerns raised when signals intelligence can only be collected in bulk; and the risk of damage to our national security interests and our law enforcement, intelligence-sharing, and diplomatic relationships should our capabilities or activities be compromised. It is, therefore, essential that national security policymakers consider carefully the value of signals intelligence activities in light of the risks entailed in conducting these activities.

To enable this judgment, the heads of departments and agencies that participate in the policy processes for establishing signals intelligence priorities and requirements shall, on an annual basis, review any priorities or requirements identified by their departments or agencies and advise the DNI whether each should be maintained, with a copy of the advice provided to the APNSA.

Additionally, the classified Annex to this directive, which supplements the existing policy process for reviewing signals intelligence activities, affirms that determinations about whether and how to conduct signals intelligence activities must
carefully evaluate the benefits to our national interests and the risks posed by those activities.\textsuperscript{6}

Sec. 4. Safeguarding Personal Information Collected Through Signals Intelligence.

All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information.\textsuperscript{7} U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.\textsuperscript{8}

(a) Policies and Procedures. The DNI, in consultation with the Attorney General, shall ensure that all elements of the IC establish policies and procedures that apply the following principles for safeguarding personal information collected from signals intelligence activities. To the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality:\textsuperscript{9}

i. Minimization. The sharing of intelligence that contains personal information is necessary to protect our national security and advance our foreign policy interests, as it enables the United States to coordinate activities across our government. At the same time, however, by setting appropriate limits on such sharing, the United States takes legitimate privacy concerns into account and decreases the risks that personal information will be misused or mishandled. Relatedly, the significance to our national security of intelligence is not always apparent upon an initial review of information: intelligence must be retained for a sufficient period of time for the IC to understand its relevance and use

\textsuperscript{6} Section 3 of this directive, and the directive's classified Annex, do not apply to (1) signals intelligence activities undertaken by or for the Federal Bureau of Investigation in support of predicated investigations other than those conducted solely for purposes of acquiring foreign intelligence; or (2) signals intelligence activities undertaken in support of military operations in an area of active hostilities, covert action, or human intelligence operations.

\textsuperscript{7} Departments and agencies shall apply the term "personal information" in a manner that is consistent for U.S. persons and non-U.S. persons. Accordingly, for the purposes of this directive, the term "personal information" shall cover the same types of information covered by "information concerning U.S. persons" under section 2.3 of Executive Order 12333.

\textsuperscript{8} The collection, retention, and dissemination of information concerning "United States persons" is governed by multiple legal and policy requirements, such as those required by the Foreign Intelligence Surveillance Act and Executive Order 12333. For the purposes of this directive, the term "United States person" shall have the same meaning as it does in Executive Order 12333.

\textsuperscript{9} The policies and procedures of affected elements of the IC shall also be consistent with any additional IC policies, standards, procedures, and guidance the DNI, in coordination with the Attorney General, the heads of IC elements, and the heads of any other departments containing such elements, may issue to implement these principles. This directive is not intended to alter the rules applicable to U.S. persons in Executive Order 12333, the Foreign Intelligence Surveillance Act, or other applicable law.
it to meet our national security needs. However, long-term storage of personal information unnecessary to protect our national security is inefficient, unnecessary, and raises legitimate privacy concerns. Accordingly, IC elements shall establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities.

- **Dissemination**: Personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333.

- **Retention**: Personal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons. Information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States.

Additionally, within 180 days of the date of this directive, the DNI, in coordination with the Attorney General, the heads of other elements of the IC, and the heads of departments and agencies containing other elements of the IC, shall prepare a report evaluating possible additional dissemination and retention safeguards for personal information collected through signals intelligence, consistent with technical capabilities and operational needs.

ii. **Data Security and Access.** When our national security and foreign policy needs require us to retain certain intelligence, it is vital that the United States take appropriate steps to ensure that any personal information contained within that intelligence is secure. Accordingly, personal information shall be processed and stored under conditions that provide adequate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, Presidential directives, IC directives, and associated policies. Access to such personal information shall be limited to authorized personnel with a need to know the information to perform their mission, consistent with the personnel security requirements of relevant Executive Orders, IC directives, and associated policies. Such personnel will be provided appropriate and adequate training in the principles set forth in this directive. These persons may access and use the information consistent with applicable laws and Executive Orders and the principles of this directive; personal information for which no determination has been made that it can be permissibly disseminated or retained under section 4(a)(i) of this directive shall be accessed only in order to make such determinations.
(or to conduct authorized administrative, security, and oversight functions).

iii. Data Quality. IC elements strive to provide national security policymakers with timely, accurate, and insightful intelligence, and inaccurate records and reporting can not only undermine our national security interests, but also can result in the collection or analysis of information relating to persons whose activities are not of foreign intelligence or counterintelligence value. Accordingly, personal information shall be included in intelligence products only as consistent with applicable IC standards for accuracy and objectivity, as set forth in relevant IC directives. Moreover, while IC elements should apply the IC Analytic Standards as a whole, particular care should be taken to apply standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

iv. Oversight. The IC has long recognized that effective oversight is necessary to ensure that we are protecting our national security in a manner consistent with our interests and values. Accordingly, the policies and procedures of IC elements, and departments and agencies containing IC elements, shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information, to include periodic auditing against the standards required by this section.

The policies and procedures shall also recognize and facilitate the performance of oversight by the Inspectors General of IC elements, and departments and agencies containing IC elements, and other relevant oversight entities, as appropriate and consistent with their responsibilities. When a significant compliance issue occurs involving personal information of any person, regardless of nationality, collected as a result of signals intelligence activities, the issue shall, in addition to any existing reporting requirements, be reported promptly to the DNI, who shall determine what, if any, corrective actions are necessary. If the issue involves a non-United States person, the DNI, in consultation with the Secretary of State and the head of the notifying department or agency, shall determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel.

(b) Update and Publication. Within 1 year of the date of this directive, IC elements shall update or issue new policies and procedures as necessary to implement section 4 of this directive, in coordination with the DNI. To enhance public understanding of, and promote public trust in, the safeguards in place to protect personal information, these updated or newly issued policies and procedures shall be publicly released to the maximum extent possible, consistent with classification requirements.
(c) **Privacy and Civil Liberties Policy Official.** To help ensure that the legitimate privacy interests all people share related to the handling of their personal information are appropriately considered in light of the principles in this section, the APNSA, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy (OSTP) shall identify one or more senior officials who will be responsible for working with the DNI, the Attorney General, the heads of other elements of the IC, and the heads of departments and agencies containing other elements of the IC, as appropriate, as they develop the policies and procedures called for in this section.

(d) **Coordinator for International Diplomacy.** The Secretary of State shall identify a senior official within the Department of State to coordinate with the responsible departments and agencies the United States Government's diplomatic and foreign policy efforts related to international information technology issues and to serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States.

**Sec. 5. Reports.**

(a) Within 180 days of the date of this directive, the DNI shall provide a status report that updates me on the progress of the IC's implementation of section 4 of this directive.

(b) The Privacy and Civil Liberties Oversight Board is encouraged to provide me with a report that assesses the implementation of any matters contained within this directive that fall within its mandate.

(c) Within 120 days of the date of this directive, the President's Intelligence Advisory Board shall provide me with a report identifying options for assessing the distinction between metadata and other types of information, and for replacing the "need-to-share" or "need-to-know" models for classified information sharing with a Work-Related Access model.

(d) Within 1 year of the date of this directive, the DNI, in coordination with the heads of relevant elements of the IC and OSTP, shall provide me with a report assessing the feasibility of creating software that would allow the IC more easily to conduct targeted information acquisition rather than bulk collection.

**Sec. 6. General Provisions.**

(a) Nothing in this directive shall be construed to prevent me from exercising my constitutional authority, including as Commander in Chief, Chief Executive, and in the conduct of foreign affairs, as well as my statutory authority. Consistent with this principle, a recipient of this directive may at any time recommend to me, through the APNSA, a change to the policies and procedures contained in this directive.
(b) Nothing in this directive shall be construed to impair or otherwise affect the authority or responsibility granted by law to a United States Government department or agency, or the head thereof, or the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals. This directive is intended to supplement existing processes or procedures for reviewing foreign intelligence or counterintelligence activities and should not be read to supersede such processes and procedures unless explicitly stated.

(c) This directive shall be implemented consistent with applicable U.S. law and subject to the availability of appropriations.

(d) This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

# # #
PUBLIC LAW 109–177—MAR. 9, 2006

USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005
Public Law 109–177
109th Congress

An Act
To extend and modify authorities needed to combat terrorism, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.
(a) SHORT TITLE.—This Act may be cited as the “USA PATRIOT Improvement and Reauthorization Act of 2005”.
(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:
Sec. 1. Short title; table of contents.

TITLE I—USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT
Sec. 101. References to, and modification of short title for, USA PATRIOT Act.
Sec. 102. USA PATRIOT Act sunset provisions.
Sec. 103. Extension of sunset relating to individual terrorists as agents of foreign powers.
Sec. 104. Section 2332b and the material support sections of title 18, United States Code.
Sec. 105. Duration of FISA surveillance of non-United States persons under section 207 of the USA PATRIOT Act.
Sec. 106. Access to certain business records under section 215 of the USA PATRIOT Act.
Sec. 106A. Audit on access to certain business records for foreign intelligence purposes.
Sec. 107. Enhanced oversight of good-faith emergency disclosures under section 212 of the USA PATRIOT Act.
Sec. 108. Multipoint electronic surveillance under section 206 of the USA PATRIOT Act.
Sec. 109. Enhanced congressional oversight.
Sec. 110. Attacks against railroad carriers and mass transportation systems.
Sec. 111. Forfeiture.
Sec. 112. Section 2332b(g)(5)(B) amendments relating to the definition of Federal crime of terrorism.
Sec. 113. Amendments to section 2516(1) of title 18, United States Code.
Sec. 114. Delayed notice search warrants.
Sec. 115. Judicial review of national security letters.
Sec. 116. Confidentiality of national security letters.
Sec. 117. Violations of nondisclosure provisions of national security letters.
Sec. 118. Reports on national security letters.
Sec. 119. Audit of use of national security letters.
Sec. 120. Definition for forfeiture provisions under section 806 of the USA PATRIOT Act.
Sec. 121. Penal provisions regarding trafficking in contraband cigarettes or smokeless tobacco.
Sec. 122. Prohibition of narco-terrorism.
Sec. 123. Interfering with the operation of an aircraft.
Sec. 124. Sense of Congress relating to lawful political activity.
Sec. 125. Removal of civil liability barriers that discourage the donation of fire equipment to volunteer fire companies.
Sec. 126. Report on data-mining activities.
Sec. 127. Sense of Congress.
Sec. 128. USA PATRIOT Act section 214; authority for disclosure of additional information in connection with orders for pen register and trap and trace authority under FISA.
PUBLICATION LAW 109–177—MAR. 9, 2006

120 STAT. 193

TITLE II—TERRORIST DEATH PENALTY ENHANCEMENT

Sec. 201. Short title.

Subtitle A—Terrorist penalties enhancement Act

Sec. 211. Death penalty procedures for certain air piracy cases occurring before enactment of the Federal Death Penalty Act of 1994.

Sec. 212. Postrelease supervision of terrorists.

Subtitle B—Federal Death Penalty Procedures

Sec. 221. Elimination of procedures applicable only to certain Controlled Substances Act cases.

Sec. 222. Counsel for financially unable defendants.

TITLE III—REDUCING CRIME AND TERRORISM AT AMERICA'S SEAPORTS

Sec. 301. Short title.

Sec. 302. Entry by false pretenses to any seaport.

Sec. 303. Criminal sanctions for failure to heave to, obstruction of boarding, or providing false information.

Sec. 304. Criminal sanctions for violence against maritime navigation, placement of destructive devices.

Sec. 305. Transportation of dangerous materials and terrorists.

Sec. 306. Destruction of, or interference with, vessels or maritime facilities.

Sec. 307. Theft of interstate or foreign shipments or vessels.

Sec. 308. Stowaways on vessels or aircraft.

Sec. 309. Bribery affecting port security.

Sec. 310. Penalties for smuggling goods into the United States.

Sec. 311. Smuggling goods from the United States.

TITLE IV—COMBATING TERRORISM FINANCING

Sec. 401. Short title.

Sec. 402. Increased penalties for terrorism financing.

Sec. 403. Terrorism-related specified activities for money laundering.

Sec. 404. Assets of persons committing terrorist acts against foreign countries or international organizations.

Sec. 405. Money laundering through hawalas.

Sec. 406. Technical and conforming amendments relating to the USA PATRIOT Act.

Sec. 407. Cross reference correction.

Sec. 408. Amendment to mandatory language.

Sec. 409. Designation of additional money laundering predicate.

Sec. 410. Uniform procedures for criminal forfeiture.

TITLE V—MISCELLANEOUS PROVISIONS

Sec. 501. Residence of United States attorneys and assistant United States attorneys.

Sec. 502. Interim appointment of United States Attorneys.

Sec. 503. Secretary of Homeland Security in Presidential line of succession.

Sec. 504. Bureau of Alcohol, Tobacco and Firearms to the Department of Justice.

Sec. 505. Qualifications of United States Marshals.

Sec. 506. Department of Justice intelligence matters.

Sec. 507. Review by Attorney General.

TITLE VI—SECRET SERVICE

Sec. 601. Short title.

Sec. 602. Interference with national special security events.

Sec. 603. False credentials to national special security events.

Sec. 604. Forensic and investigative support of missing and exploited children cases.

Sec. 605. The Uniformed Division, United States Secret Service.

Sec. 606. Savings provisions.

Sec. 607. Maintenance as distinct entity.

Sec. 608. Exemptions from the Federal Advisory Committee Act.

TITLE VII—COMBAT METHAMPHETAMINE EPIDEMIC ACT OF 2005

Sec. 701. Short title.

Subtitle A—Domestic regulation of precursor chemicals

Sec. 711. Scheduled listed chemical products; restrictions on sales quantity, behind-the-counter access, and other safeguards.
TITLE I—USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT

SEC. 101. REFERENCES TO, AND MODIFICATION OF SHORT TITLE FOR, USA PATRIOT ACT.

(a) REFERENCES TO USA PATRIOT ACT.—A reference in this Act to the USA PATRIOT Act shall be deemed a reference to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001.

(b) MODIFICATION OF SHORT TITLE OF USA PATRIOT ACT.—Section 1(a) of the USA PATRIOT Act is amended to read as follows:

"(a) SHORT TITLE.—This Act may be cited as the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001' or the 'USA PATRIOT Act'.":

SEC. 102. USA PATRIOT ACT SUNSET PROVISIONS.

(a) IN GENERAL.—Section 224 of the USA PATRIOT Act is repealed.
§ 987. Anti-terrorist forfeiture protection

(a) Right to contest.—An owner of property that is confiscated under any provision of law relating to the confiscation of assets of suspected international terrorists, may contest that confiscation by filing a claim in the manner set forth in the Federal Rules of Civil Procedure (Supplemental Rules for Certain Admiralty and Maritime Claims), and asserting as an affirmative defense that—

“(1) the property is not subject to confiscation under such provision of law; or

“(2) the innocent owner provisions of section 983(d) of title 18, United States Code, apply to the case.

(b) Evidence.—In considering a claim filed under this section, a court may admit evidence that is otherwise inadmissible under the Federal Rules of Evidence, if the court determines that the evidence is reliable, and that compliance with the Federal Rules of Evidence may jeopardize the national security interests of the United States.

(c) Clarifications.—

“(1) Protection of rights.—The exclusion of certain provisions of Federal law from the definition of the term ‘civil forfeiture statute’ in section 983(i) of title 18, United States Code, shall not be construed to deny an owner of property the right to contest the confiscation of assets of suspected international terrorists under—

“(A) subsection (a) of this section;
“(B) the Constitution; or
“(C) subchapter II of chapter 5 of title 5, United States Code (commonly known as the ‘Administrative Procedure Act’).

“(2) Savings clause.—Nothing in this section shall limit or otherwise affect any other remedies that may be available to an owner of property under section 983 of title 18, United States Code, or any other provision of law.”.

(2) Subsections (a), (b), and (c) of section 316 of Public Law 107–56 are repealed.

(c) Conforming Amendments Concerning Conspiracies.—

(1) Section 33(a) of title 18, United States Code is amended by inserting “or conspires” before “to do any of the aforesaid acts”.

(2) Section 1366(a) of title 18, United States Code, is amended—

(A) by striking “attempts” each time it appears and inserting “attempts or conspires”; and

(B) by inserting “, or if the object of the conspiracy had been achieved,” after “the attempted offense had been completed”.

SEC. 407. CROSS REFERENCE CORRECTION.

Section 5318(n)(4)(A) of title 31, United States Code, is amended by striking “National Intelligence Reform Act of 2004” and inserting “Intelligence Reform and Terrorism Prevention Act of 2004”.

SEC. 408. AMENDMENT TO AMENDATORY LANGUAGE.

Section 6604 of the Intelligence Reform and Terrorism Prevention Act of 2004 is amended (effective on the date of the enactment of that Act)—
PUBLIC LAW 109–177—MAR. 9, 2006

(1) by striking “Section 2339(c)(2)” and inserting “Section 2339C(c)(2)”;
and
(2) by striking “Section 2339(c)” and inserting “Section 2339C(e)”.

SEC. 409. DESIGNATION OF ADDITIONAL MONEY LAUNDERING PREDICATE.

Section 1956(c)(7)(D) of title 18, United States Code, is amended—
(1) by inserting “, section 2339C (relating to financing of terrorism), or section 2339D (relating to receiving military-type training from a foreign terrorist organization)” after “section 2339A or 2339B (relating to providing material support to terrorists)”;
and
(2) by striking “or” before “section 2339A or 2339B”.

SEC. 410. UNIFORM PROCEDURES FOR CRIMINAL FORFEITURE.

Section 2461(c) of title 28, United States Code, is amended to read as follows:
“(c) If a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized, the Government may include notice of the forfeiture in the indictment or information pursuant to the Federal Rules of Criminal Procedure. If the defendant is convicted of the offense giving rise to the forfeiture, the court shall order the forfeiture of the property as part of the sentence in the criminal case pursuant to the Federal Rules of Criminal Procedure and section 3554 of title 18, United States Code. The procedures in section 413 of the Controlled Substances Act (21 U.S.C. 853) apply to all stages of a criminal forfeiture proceeding, except that subsection (d) of such section applies only in cases in which the defendant is convicted of a violation of such Act.”.

TITLE V—MISCELLANEOUS PROVISIONS

SEC. 501. RESIDENCE OF UNITED STATES ATTORNEYS AND ASSISTANT UNITED STATES ATTORNEYS.

(a) IN GENERAL.—Subsection (a) of section 545 of title 28, United States Code, is amended by adding at the end the following new sentence: “Pursuant to an order from the Attorney General or his designee, a United States attorney or an assistant United States attorney may be assigned dual or additional responsibilities that exempt such officer from the residency requirement in this subsection for a specific period as established by the order and subject to renewal.”.

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall take effect as of February 1, 2005.

SEC. 502. INTERIM APPOINTMENT OF UNITED STATES ATTORNEYS.

Section 546 of title 28, United States Code, is amended by striking subsections (c) and (d) and inserting the following new subsection:
“(c) A person appointed as United States attorney under this section may serve until the qualification of a United States Attorney for such district appointed by the President under section 541 of this title.”.
SEC. 503. SECRETARY OF HOMELAND SECURITY IN PRESIDENTIAL LINE OF SUCCESSION.

Section 19(d)(1) of title 3, United States Code, is amended by inserting “Secretary of Homeland Security” after “Secretary of Veterans Affairs”.

SEC. 504. BUREAU OF ALCOHOL, TOBACCO AND FIREARMS TO THE DEPARTMENT OF JUSTICE.

The second sentence of section 1111(a)(2) of the Homeland Security Act of 2002 (6 U.S.C. 531(a)(2)) is amended by striking “Attorney General” the first place it appears and inserting “President, by and with the advice and consent of the Senate”.

SEC. 505. QUALIFICATIONS OF UNITED STATES MARSHALS.

Section 561 of title 28, United States Code, is amended by adding at the end the following new subsection:

“(i) Each marshal appointed under this section should have—
“(1) a minimum of 4 years of command-level law enforcement management duties, including personnel, budget, and accountable property issues, in a police department, sheriff’s office or Federal law enforcement agency;
“(2) experience in coordinating with other law enforcement agencies, particularly at the State and local level;
“(3) college-level academic experience; and
“(4) experience in or with county, State, and Federal court systems or experience with protection of court personnel, jurors, and witnesses.”

SEC. 506. DEPARTMENT OF JUSTICE INTELLIGENCE MATTERS.

(a) ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY.—

(1) IN GENERAL.—Chapter 31 of title 28, United States Code, is amended by inserting after section 507 the following new section:

“§ 507A. Assistant Attorney General for National Security

“(a) Of the Assistant Attorneys General appointed under section 506, one shall serve, upon the designation of the President, as the Assistant Attorney General for National Security.

“(b) The Assistant Attorney General for National Security shall—

“(1) serve as the head of the National Security Division of the Department of Justice under section 509A of this title;
“(2) serve as primary liaison to the Director of National Intelligence for the Department of Justice; and
“(3) perform such other duties as the Attorney General may prescribe.”.

(2) ADDITIONAL ASSISTANT ATTORNEY GENERAL.—Section 506 of title 28, United States Code, is amended by striking “ten” and inserting “11”.

(3) EXECUTIVE SCHEDULE MATTERS.—Section 5315 of title 5, United States Code, is amended by striking the matter relating to Assistant Attorneys General and inserting the following:

“Assistant Attorneys General (11).”.

(4) CONSULTATION OF DIRECTOR OF NATIONAL INTELLIGENCE IN APPOINTMENT.—Section 106(c)(2) of the National Security Act of 1947 (50 U.S.C. 403–6(c)(2)) is amended by adding at the end the following new subparagraph:
“(C) The Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code."

(5) AUTHORITY TO ACT FOR ATTORNEY GENERAL UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—Section 101(g) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(g)) is amended by striking "or the Deputy Attorney General" and inserting ", the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code".

(6) AUTHORIZATION FOR INTERCEPTION OF COMMUNICATIONS.—Section 2516(1) of title 18, United States Code, is amended by inserting "or National Security Division" after "the Criminal Division".

(7) AUTHORITY TO ACT FOR ATTORNEY GENERAL IN MATTERS INVOLVING WITNESS RELOCATION OR PROTECTION.—Section 3521(d)(3) of title 18, United States Code, is amended by striking "to the Assistant Attorney General in charge of the Criminal Division of the Department of Justice" and inserting "to any Assistant Attorney General in charge of the Criminal Division or National Security Division of the Department of Justice".

(8) PROSECUTION OF CASES INVOLVING CLASSIFIED INFORMATION.—Section 9A(a) of the Classified Information Procedures Act (18 U.S.C. App.) is amended by inserting "or the Assistant Attorney General for National Security, as appropriate," after "Assistant Attorney General for the Criminal Division".

(9) INTELLIGENCE AND NATIONAL SECURITY ASPECTS OF ESPIONAGE PROSECUTION.—Section 341(b) of the Intelligence Authorization Act for Fiscal Year 2004 (28 U.S.C. 519 note) is amended by striking "acting through the Office of Intelligence Policy and Review of the Department of Justice" and inserting "acting through the Assistant Attorney General for National Security".

(10) CERTIFICATIONS FOR CERTAIN UNDERCOVER FOREIGN INTELLIGENCE AND COUNTERINTELLIGENCE INVESTIGATIVE OPERATIONS.—Section 102(b)(1) of Public Law 102–395 (28 U.S.C. 533 note) is amended by striking "Counsel for Intelligence Policy" and inserting "Assistant Attorney General for National Security".

(11) INCLUSION IN FEDERAL LAW ENFORCEMENT COMMUNITY FOR EMERGENCY FEDERAL LAW ENFORCEMENTS ASSISTANCE PURPOSES.—Section 609N(2) of the Justice Assistance Act of 1984 (42 U.S.C. 10502(2)) is amended—

(A) by redesignating subparagraphs (L) and (M) as subparagraphs (M) and (N), respectively; and

(B) by inserting after subparagraph (K) the following new subparagraph (L):

"(L) the National Security Division of the Department of Justice,".

(b) NATIONAL SECURITY DIVISION OF DEPARTMENT OF JUSTICE.—

(1) IN GENERAL.—Chapter 31 of title 28, United States Code, is further amended by inserting after section 509 the following new section:
§ 509A. National Security Division

(a) There is a National Security Division of the Department of Justice.

(b) The National Security Division shall consist of the elements of the Department of Justice (other than the Federal Bureau of Investigation) engaged primarily in support of the intelligence and intelligence-related activities of the United States Government, including the following:

(1) The Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of this title.

(2) The Office of Intelligence Policy and Review (or any successor organization).

(3) The counterterrorism section (or any successor organization).

(4) The counterespionage section (or any successor organization).

(5) Any other element, component, or office designated by the Attorney General.

(2) PROHIBITION ON POLITICAL ACTIVITY.—Section 7323(b)(3) of title 5, United States Code, is amended by inserting “or National Security Division” after “Criminal Division”.

(c) CLERICAL AMENDMENTS.—The table of sections at the beginning of chapter 31 of title 28, United States Code, is amended—

(1) by inserting after the item relating to section 507 the following new item:

507A. Assistant Attorney General for National Security.

and

(2) by inserting after the item relating to section 509 the following new item:

509A. National Security Division.

(d) PROCEDURES FOR CONFIRMATION OF THE ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY.—(1) Section 17 of Senate Resolution 400 (94th Congress) is amended—

(A) in subsection (a), by striking “(a) The” and inserting “(a) Except as otherwise provided in subsection (b), the”; and

(B) in subsection (b), by striking “(2)” and inserting “(2)”;

and

(C) by inserting after subsection (a) the following new subsection:

(b)(1) With respect to the confirmation of the Assistant Attorney General for National Security, or any successor position, the nomination of any individual by the President to serve in such position shall be referred to the Committee on the Judiciary and, if and when reported, to the select Committee for not to exceed 20 calendar days, except that in cases when the 20-day period expires while the Senate is in recess, the select Committee shall have 5 additional calendar days after the Senate reconvenes to report the nomination.

(2) If, upon the expiration of the period described in paragraph (1), the select Committee has not reported the nomination, such nomination shall be automatically discharged from the select Committee and placed on the Executive Calendar.

(2) Paragraph (1) is enacted—
(A) as an exercise of the rulemaking power of the Senate; and

(B) with full recognition of the constitutional right of the Senate to change the rules of the Senate at any time and to the same extent as in the case of any other rule of the Senate.

SEC. 507. REVIEW BY ATTORNEY GENERAL.

(a) APPLICABILITY.—Section 2261 of title 28, United States Code, is amended by striking subsection (b) and inserting the following:

"(b) COUNSEL.—This chapter is applicable if—

"(1) the Attorney General of the United States certifies that a State has established a mechanism for providing counsel in postconviction proceedings as provided in section 2265; and

"(2) counsel was appointed pursuant to that mechanism, petitioner validly waived counsel, petitioner retained counsel, or petitioner was found not to be indigent."

(b) SCOPE OF PRIOR REPRESENTATION.—Section 2261(d) of title 28, United States Code is amended by striking "or on direct appeal".

(c) CERTIFICATION AND JUDICIAL REVIEW.—

(1) IN GENERAL.—Chapter 154 of title 28, United States Code, is amended by striking section 2265 and inserting the following:

"§ 2265. Certification and judicial review

"(a) CERTIFICATION.—

"(1) IN GENERAL.—If requested by an appropriate State official, the Attorney General of the United States shall determine—

"(A) whether the State has established a mechanism for the appointment, compensation, and payment of reasonable litigation expenses of competent counsel in State postconviction proceedings brought by indigent prisoners who have been sentenced to death;

"(B) the date on which the mechanism described in subparagraph (A) was established; and

"(C) whether the State provides standards of competency for the appointment of counsel in proceedings described in subparagraph (A).

"(2) EFFECTIVE DATE.—The date the mechanism described in paragraph (1)(A) was established shall be the effective date of the certification under this subsection.

"(3) ONLY EXPRESS REQUIREMENTS.—There are no requirements for certification or for application of this chapter other than those expressly stated in this chapter.

"(b) REGULATIONS.—The Attorney General shall promulgate regulations to implement the certification procedure under subsection (a).

"(c) REVIEW OF CERTIFICATION.—

"(1) IN GENERAL.—The determination by the Attorney General regarding whether to certify a State under this section is subject to review exclusively as provided under chapter 158 of this title.

"(2) VENUE.—The Court of Appeals for the District of Columbia Circuit shall have exclusive jurisdiction over matters
United States Foreign Intelligence
Surveillance Court of Review

Argued September 9, 2002

Consolidated with
02-002

Decided November 18, 2002

In re Sealed Case No. 02-301

On Motion for Review of Orders of the United States
Foreign Intelligence Surveillance Court
(Ross v. NSA, No. 02-302 and 02-506)

Presiding: Senior Circuit Judge
Panel: Judge STERLING AND LEVY, Senior Circuit Judges

Opinion for the Court filed by
Judge STERLING.

For Plaintiff: This is the first appeal from the Foreign Intelligence Surveillance Court
of Review since the passage of the Foreign Intelligence Surveillance Act (FISA).
50 U.S.C. §§ 1801-1862 (West 1991 and Supp. 2002). This appeal is brought by the
United States from a FISA court surveillance order which imposed certain restrictions on
the government. Since the government is the only party in FISA proceedings, we have accepted
the briefs filed by the American Civil Liberties Union (ACLU) and the National Association
of Criminal Defense Lawyers (NACDL) as amicus curiae.

We therefore stand in accordance with the Constitution and
the restrictions imposed by the Patriot Act. We support the government’s position
and conclude that FISA, as amended by the Patriot Act, is constitutional.

We therefore stand in accordance with the Constitution and
the restrictions imposed by the Patriot Act. We support the government’s position
and conclude that FISA, as amended by the Patriot Act, is constitutional.

1. Joining the ACLU on to brief are the Center for Democracy and Technology, Center
for National Security Studies, Electronic Privacy Information Center, and Electronic Frontier
Foundation.
2. Limiting and Strengthening America by Providing Appropriate Tools Required to
2001).

Therefore, R. Olson, Solicitor General, argued the case for appellant the United States,
Deputy Solicitor General, argued the case for the United States.

Amy Colacone, James Naifeh, Steven R. Shapiro, for amicus curiae American Civil
Liberties Union (ACLU); Jane Alana Frazee, for amicus curiae National Security
Counsel for Electronic Frontier Foundation; and Lee Tressler, for amicus curiae
National Association of Criminal Defense Lawyers.
I.

The court's decision from which the government appeals imposed certain requirements and limitations accompanying an order authorizing electronic surveillance of an "agent of a foreign power" as defined in FISA. There is no disagreement between the government and the FISA court as to the propriety of the electronic surveillance; the court found that the government had shown probable cause to believe that the target is an agent of a foreign power and otherwise met the basic requirements of FISA. The government's application for a surveillance order contains detailed information to support its contention that the target, who is a United States person, is aiding, abetting, or conspiring with others in international terrorism.\[3\] The FISA court authorized the surveillance, but imposed certain restrictions, which the government contends are neither mandated nor authorized by FISA. Particularly, the court ordered that

law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division [of the Department of Justice] shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.

To ensure the Justice Department followed these strictures the court also fashioned what the government refers to as a "chaperone requirement": that a unit of the Justice Department, the Office of Intelligence Policy and Review (OIPR) (composed of 31 lawyers and 25 support staff), "be invited" to all meetings between the FBI and the Criminal Division involving consultations for the purpose of coordinating efforts "to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence

\[3\] The bracketed information is classified and has been redacted from the public version of the opinion.
activities by foreign powers or their agents.” If representatives of OIPR are unable to attend
such meetings, “OIPR shall be apprised of the substance of the meetings forthwith in writing
so that the Court may be notified at the earliest opportunity.”

These restrictions are not original to the order appealed. They are actually set forth
in an opinion written by the former Presiding Judge of the FISA court on May 17 of this year.
But since that opinion did not accompany an order conditioning an approval of an electronic
surveillance application it was not appealed. It is, however, the basic decision before us and
it is its rationale that the government challenges. The opinion was issued after an oral
argument before all of the then-serving FISA district judges and clearly represents the views
of all those judges.5

We think it fair to say, however, that the May 17 opinion of the FISA court does not
clearly set forth the basis for its decision. It appears to proceed from the assumption that FISA
constructed a barrier between counterintelligence/intelligence officials and law enforcement
officers in the Executive Branch—indeed, it uses the word “wall” popularized by certain
commentators (and journalists) to describe that supposed barrier. Yet the opinion does not
support that assumption with any relevant language from the statute.

The “wall” emerges from the court’s implicit interpretation of FISA. The court
apparently believes it can approve applications for electronic surveillance only if the
government’s objective is not primarily directed toward criminal prosecution of the foreign
agents for their foreign intelligence activity. But the court neither refers to any FISA language
supporting that view, nor does it reference the Patriot Act amendments, which the government
contends specifically altered FISA to make clear that an application could be obtained even if
criminal prosecution is the primary counter mechanism.

Instead the court relied for its imposition of the disputed restrictions on its statutory
authority to approve “minimization procedures” designed to prevent the acquisition, retention,
and dissemination within the government of material gathered in an electronic surveillance that
is unnecessary to the government’s need for foreign intelligence information. 50 U.S.C. §
1801(b).

Jurisdiction

This court has authority “to review the denial of any application” under FISA. id. §
1803(b). The FISA court’s order is styled as a grant of the application “as modified.” It seems
obvious, however, that the FISA court’s order actually denied the application to the extent it
rejected a significant portion of the government’s proposed minimization procedures and
imposed restrictions on Department of Justice investigations that the government opposes.
Indeed, the FISA court was clear in rejecting a portion of the application. Under these
circumstances, we have jurisdiction to review the FISA court’s order. to conclude otherwise

---

4 To be precise, there are two surveillance orders on appeal, one reversing the other
with identical conditions.

5 The argument before all of the district judges, some of whose terms have since
expired, was referred to as an “en banc” although the statute does not contemplate such a
proceeding. In fact, it specifically provides that if one judge declines to approve an application
the government may not seek approval from another district judge, but only appeal to the Court
of Review. 50 U.S.C. §§ 1803(a), (b).
would elevate form over substance and deprive the government of judicial review of the minimization procedures imposed by the FISA court. See Mobile Comm. Corp. v. FCC, 77 F.3d 1399, 1403-04 (D.C. Cir.) (grant of station license subject to condition that is unacceptable to applicant is subject to judicial review under statute that permits such review when application for license is denied), cert. denied, 519 U.S. 823 (1996).

II.

The government makes two main arguments. The first, it must be noted, was not presented to the FISA court; indeed, insofar as we can determine it has never previously been advanced either before a court or Congress. That argument is that the supposed pre-Patriot Act limitation in FISA that restricts the government's intention to use foreign intelligence information in criminal prosecutions is an illusion; it finds no support in either the language of FISA or its legislative history. The government does recognize that several courts of appeals, while upholding the use of FISA surveillances, have opined that FISA may be used only if the government's primary purpose in pursuing foreign intelligence information is not criminal prosecution, but the government argues that those decisions, which did not carefully analyze the statute, were incorrect in their statements, if not incorrect in their holdings.

Alternatively, the government contends that even if the primary purpose test was a legitimate construction of FISA prior to the passage of the Patriot Act, that Act's amendments to FISA eliminate that concept. And as a corollary, the government insists the FISA court's construction of the minimization procedures is far off the mark both because it is a misconstruction of those provisions per se, as well as an end run around the specific amendments in the Patriot Act designed to deal with the real issue underlying this case. The government, moreover, contends that the FISA court's restrictions, which the court described as minimization procedures, are so intrusive into the operation of the Department of Justice as to exceed the constitutional authority of Article III judges.

The government's brief, and its supplementary brief requested by this court, also set forth its view that the primary purpose test is not required by the Fourth Amendment. The ACLU and NACDL argue, inter alia, the contrary; that the statutes are unconstitutional unless they are construed as prohibiting the government from obtaining approval of an application under FISA if its "primary purpose" is criminal prosecution.

The 1978 FISA

We turn first to the statute as enacted in 1978.7 It authorizes a judge on the FISA court

---

6 Since proceedings before the FISA court and the Court of Review are ex parte—not adversary—we can entertain an argument supporting the government's position not presented to the lower court.

7 As originally enacted, FISA covered only electronic surveillance. It was amended in 1994 to cover physical searches. Pub. L. No. 103-359, 108 Stat. 3444 (Oct. 14, 1994). Although only electronic surveillance is at issue here, much of our statutory analysis applies to FISA's provisions regarding physical searches, 50 U.S.C. §§ 1821-1829, which mirror to a great extent those regarding electronic surveillance.
to grant an application for an order approving electronic surveillance to “obtain foreign intelligence information” if “there is probable cause to believe that ... the target of the electronic surveillance is a foreign power or an agent of a foreign power,” and that “each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.” 50 U.S.C. § 1805(a)(3). As is apparent, the definitions of agent of a foreign power and foreign intelligence information are crucial to an understanding of the statutory scheme. The latter means

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

Id. § 1801(c)(1).

8 Foreign power is defined broadly to include, inter alia, “a group engaged in international terrorism or activities in preparation therefor” and “a foreign-based political organization, not substantially composed of United States persons.” 50 U.S.C. §§ 1801(a)(4), (5).

9 A second definition of foreign intelligence information includes information necessary to “the national defense or the security of the United States,” or “the conduct of the foreign affairs of the United States.” 50 U.S.C. § 1801(o)(2). This definition generally involves information referred to as “affirmative” or “positive” foreign intelligence information rather than the “protective” or “counterintelligence” information at issue here.

The definition of an agent of a foreign power, if it pertains to a U.S. person (which is the only category relevant to this case), is closely tied to criminal activity. The term includes any person who “knowingly engages in clandestine intelligence gathering activities . . . which activities involve or may involve a violation of the criminal statutes of the United States,” or “knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor.” Id. §§ 1801(b)(2)(A), (C) (emphasis added). International terrorism refers to activities that “involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State.” Id. § 1801(c)(1) (emphasis added). Sabotage means activities that “involve a violation of chapter 105 of [the criminal code], or that would involve such a violation if committed against the United States.” Id. § 1801(d). For purposes of clarity in this opinion we will refer to the crimes referred to in section 1801(a)-(e) as foreign intelligence crimes.

In light of these definitions, it is quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department’s ability to obtain FISA orders if it intended to prosecute the targeted agents—even for foreign intelligence crimes. To be sure, section 1804, which sets forth the elements of an application for an order, required a national security official in the Executive Branch—typically the Director of the

10 Under the current version of FISA, the definition of “agent of a foreign power” also includes U.S. persons who enter the United States under a false or fraudulent identity for or on behalf of a foreign power. Our term “foreign intelligence crimes” includes this fraudulent conduct, which will almost always involve a crime.
FBI to certify that "the purpose" of the surveillance is to obtain foreign intelligence information (amended by the Patriot Act to read "a significant purpose"). But as the government now argues, the definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism. Indeed, it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power if he or she is a U.S. person is grounded on criminal conduct.

It does not seem that FISA, at least as originally enacted, even contemplated that the FISA court would inquire into the government's purpose in seeking foreign intelligence information. Section 1805, governing the standards a FISA court judge is to use in determining whether to grant a surveillance order, requires the judge to find that the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

50 U.S.C. § 1805(a)(5). And section 1804(a)(7)(E) requires that the application include "a statement of the basis of the certification that (i) the information sought is the type of foreign intelligence information designated; and (ii) such information cannot reasonably be obtained by normal investigative techniques." That language certainly suggests that, aside from the probable cause, identification of facilities, and minimization procedures the judge is to determine and approve (also set forth in section 1805), the only other issues are whether electronic surveillance is necessary to obtain the information and whether the information sought is actually foreign intelligence information—not the government's proposed use of that information.12

Nor does the legislative history cast doubt on the obvious reading of the statutory language that foreign intelligence information includes evidence of foreign intelligence crimes. To the contrary, the House Report explained:

[The term "foreign intelligence information," especially as defined in subparagraphs (c)(1)(B) and (c)(1)(C), can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities. With respect to information concerning U.S. persons, foreign intelligence information includes information necessary to protect against clandestine intelligence activities of foreign powers or their agents. Information about a spy's espionage activities obviously is within this definition, and it is most likely at the same time evidence of criminal activities.]


The government argues persuasively that arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully

11 Section 1804(d) simply provides that "[t]he judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title."

12 At oral argument before the FISA judges, the court asked government counsel whether a companion provision of FISA, section 1822(c), that gives the court jurisdiction over physical searches "for the purpose of obtaining foreign intelligence information," obliged the court to consider the government's "primary purpose." We think that language points in the opposite direction since it would be more than a little strange for Congress to require a court to make a searching inquiry into the investigative background of a FISA application before concluding the court had jurisdiction over the application.
continuing their terrorist or espionage activity. The government might wish to surveil the agent for some period of time to discover other participants in a conspiracy or to uncover a foreign power's plans, but typically at some point the government would wish to apprehend the agent and it might be that only a prosecution would provide sufficient incentives for the agent to cooperate with the government. Indeed, the threat of prosecution might be sufficient to "turn the agent." It would seem that the Congress actually anticipated the government's argument and explicitly approved it. The House Report said:

How this information may be used "to protect" against clandestine intelligence activities is not prescribed by the definition of foreign intelligence information, although, of course, how it is used may be affected by minimization procedures . . . . And no information acquired pursuant to this bill could be used for other than lawful purposes . . . . Obviously, use of "foreign intelligence information" as evidence in a criminal trial is one way the Government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism. The bill, therefore, explicitly recognizes that information which is evidence of crimes involving [these activities] can be sought, retained, and used pursuant to this bill.

Id. (emphasis added). The Senate Report is on all fours:

U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnapping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area . . . . [S]urveillance conducted under [FISA] need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate.


Congress was concerned about the government's use of FISA surveillance to obtain information not truly intertwined with the government's efforts to protect against threats from foreign powers. Accordingly, the certification of purpose under section 1804(a)(7)(B) served to prevent the practice of targeting, for example, a foreign power for electronic surveillance when the true purpose of the surveillance is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that the sole purpose of such surveillance is to secure "foreign intelligence information," as defined, and not to obtain some other type of information.

H. REP. at 76; see also S. REP. at 51. But Congress did not impose any restrictions on the government's use of the foreign intelligence information to prosecute agents of foreign powers for foreign intelligence crimes. Admittedly, the House, at least in one statement, noted that FISA surveillances "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns United States persons must be necessary to important national concerns." H. REP. at 36. That, however, was an observation, not a proscription. And the House as well as the Senate made clear that prosecution is one way to combat foreign intelligence crimes. See id.; S. REP. at 10-11.

The origin of what the government refers to as the false dichotomy between foreign intelligence information that is evidence of foreign intelligence crimes and that which is not appears to have been a Fourth Circuit case decided in 1980. United States v. Truong Dinh
Hong. 629 F.2d 908 (4th Cir. 1980). That case, however, involved an electronic surveillance carried out prior to the passage of FISA and predicated on the President’s executive power. In approving the district court’s exclusion of evidence obtained through a warrantless surveillance subsequent to the point in time when the government’s investigation became “primarily” driven by law enforcement objectives, the court held that the Executive Branch should be excused from securing a warrant only when “the object of the search or the surveillance is a foreign power, its agents or collaborators,” and “the surveillance is conducted ‘primarily’ for foreign intelligence reasons.” Id. at 915. Targets must “receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution.” Id. at 916. Although the Truong court acknowledged that “almost all foreign intelligence investigations are in part criminal” ones, it rejected the government’s assertion that “if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment.” Id. at 915.

Several circuits have followed Truong in applying similar versions of the “primary purpose” test, despite the fact that Truong was not a FISA decision. (It was an interpretation of the Constitution, in the context of measuring the boundaries of the President’s inherent executive authority, and we discuss Truong’s constitutional analysis at length in Section III of this opinion.) In one of the first major challenges to a FISA search, United States v. Megahy, 553 F. Supp. 1180 (E.D.N.Y. 1982), aff’d sub nom. United States v. Duggan, 743 F.2d 59 (2d Cir. 1984), the district court acknowledged that while Congress clearly viewed arrest and prosecution as one of the possible outcomes of a FISA investigation, surveillance under FISA would nevertheless be “appropriate only if foreign intelligence surveillance is the Government’s primary purpose.” Id. at 1189-90. Six months earlier, another judge in the same district had held that the Truong analysis did not govern FISA cases, since a FISA order was a warrant that met Fourth Amendment standards. United States v. Falvey, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982). Falvey, however, was apparently not appealed and Megahy was. The Second Circuit, without reference to Falvey, and importantly in the context of affirming the conviction, approved Megahy’s finding that the surveillance was not “directed towards criminal investigation or the institution of a criminal prosecution.” Duggan, 743 F.2d at 78 (quoting Megahy, 553 F. Supp. at 1190). Implicitly then, the Second Circuit endorsed the Megahy dichotomy. Two other circuits, the Fourth and the Eleventh, have similarly approved district court findings that a surveillance was primarily for foreign intelligence purposes without any discussion—or need to discuss—the validity of the dichotomy. See United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987), cert. denied, 486 U.S. 1010 (1988); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987), cert. denied, 485 U.S. 937 (1988).

Then, the First Circuit, seeing Duggan as following Truong, explicitly interpreted FISA’s purpose wording in section 1804(a)(7)(B) to mean that “[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance.” United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991) (citations omitted), cert. denied, 506 U.S. 816 (1992). Notably, however, the Ninth Circuit has refused
Neither Duggan nor Johnson tied the “primary purpose” test to actual statutory language. In Duggan the court stated that “[t]he requirement that foreign intelligence information be the primary objective of the surveillance is plain,” and the district court was correct in “finding that ‘the purpose of the surveillance in this case, both initially and throughout, was to secure foreign intelligence information and was not, as [the] defendants assert, directed towards criminal investigation or the institution of a criminal prosecution.’”

Duggan, 743 F.2d at 77-78 (quoting Megashey, 553 F. Supp. at 1190). Yet the court never explained why it apparently read foreign intelligence information to exclude evidence of crimes endorsing the district court’s implied dichotomy—when the statute’s definitions of foreign intelligence and foreign agent are actually cast in terms of criminal conduct. (It will be recalled that the type of foreign intelligence with which we are concerned is really countereespionage, see supra note 9.) And Johnson did not even focus on the phrase “foreign intelligence information” in its interpretation of the “purpose” language in section 1804(a)(7)(B). Johnson, 952 F.2d at 572.

It is almost as if Duggan, and particularly Johnson, assume that the government seeks foreign intelligence information (countereespionage) for its own sake—expands its pool of knowledge—because there is no discussion of how the government would use that information outside criminal prosecutions. That is not to say that the government could have no other use for that information. The government’s overriding concern is to stop or frustrate the agent’s or the foreign power’s activity by any means, but if one considers the actual ways in which the government would fail espionage or terrorism it becomes apparent that criminal prosecution analytically cannot be placed easily in a separate response category. It may well be that the government itself, in an effort to conform to district court holdings, accepted the dichotomy it now contends is false. Be that as it may, since the cases that “adopt” the dichotomy do affirm district court opinions permitting the introduction of evidence gathered under a FISA order, there was not much need for the courts to focus on the issue with which we are confronted.

In sum, we think that the FISA as passed by Congress in 1978 clearly did not preclude or limit the government’s use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution. In order to understand the FISA court’s decision, however, it is necessary to trace developments and understandings within the Justice Department post-Truong as well as after the passage of the Patriot Act. As we have noted, some time in the 1980s—the exact moment is shrouded in historical mist—the Department applied the Truong analysis to an interpretation of the FISA
statute. What is clear is that in 1995 the Attorney General adopted "Procedures for Contacts
Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign
Counterintelligence Investigations."

Apparently to avoid running afoul of the primary purpose test used by some courts, the
1995 Procedures limited contacts between the FBI and the Criminal Division in cases where
FISA surveillance or searches were being conducted by the FBI for foreign intelligence (FI)
or foreign counterintelligence (FCI) purposes. The procedures state that "the FBI and
Criminal Division should ensure that advice intended to preserve the option of a criminal
prosecution does not inadvertently result in either the fact or the appearance of the Criminal
Division's directing or controlling the FI or FCI investigation toward law enforcement
objectives." 1995 Procedures at 2, ¶ 6 (emphasis added). Although these procedures provided
for significant information sharing and coordination between criminal and FI or FCI
investigations, based at least in part on the "directing or controlling" language, they eventually
came to be narrowly interpreted within the Department of Justice, and most particularly by
OIPR, as requiring OIPR to act as a "wall" to prevent the FBI intelligence officials from
communicating with the Criminal Division regarding ongoing FI or FCI investigations. See
National Laboratory Investigation (AGRT Report), Chapter 20 at 721-34 (May 2000). Thus,
the focus became the nature of the underlying investigation, rather than the general purpose of
the surveillance. Once prosecution of the target was being considered, the procedures, as
interpreted by OIPR in light of the case law, prevented the Criminal Division from providing
any meaningful advice to the FBI. Id.

The Department’s attitude changed somewhat after the May 2000 report by the Attorney
General and a July 2001 Report by the General Accounting Office both concluded that the
Department’s concern over how the FISA court or other federal courts might interpret the
primary purpose test has inhibited necessary coordination between intelligence and law
enforcement officials. See id. at 721-34; General Accounting Office, FBI Intelligence
Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is
Limited (July 2001) (GAO-01-780) (GAO Report) at 3. The AGRT Report also concluded,
based on the text of FISA and its legislative history, that not only should the purpose of the
investigation not be inquired into by the courts, but also that Congress affirmatively anticipated
that the underlying investigation might well have a criminal as well as foreign
counterintelligence objective. AGRT Report at 737. In response to the AGRT Report, the
Attorney General, in January 2000, issued additional, interim procedures designed to address
coordination problems identified in that report. In August 2001, the Deputy Attorney General
issued a memorandum clarifying Department of Justice policy governing intelligence sharing
and establishing additional requirements. (These actions, however, did not replace the 1995

15 According to the Report, within the Department the primary proponent of procedures
that cordoned off criminal investigators and prosecutors from those officers with
counterintelligence responsibilities was the deputy counsel of OIPR. See AGRT Report at 714
& n.949. He was subsequently transferred from that position and made a senior counsel. He
left the Department and became the Legal Advisor to the FISA court.

---

We certainly understand the 1995 Justice Department’s effort to avoid difficulty
with the FISA court, or other courts; and we have no basis to criticize any organization of the
Justice Department that an Attorney General desires.
Procedures.) But it does not appear that the Department thought of these internal procedures as "minimization procedures" required under FISA.\footnote{There are other detailed, classified procedures governing the acquisition, retention, and dissemination of foreign intelligence and non-foreign intelligence information that have been submitted to and approved by the FISA court as "minimization procedures." Those classified minimization procedures are not at issue here.} Nevertheless, the FISA court was aware that the procedures were being followed by the Department and apparently adopted elements of them in certain cases.

The Patriot Act and the FISA Court's Decision

The passage of the Patriot Act altered and to some degree muddied the landscape. In October 2001, Congress amended FISA to change "the purpose" language in 1804(a)(7)(B) to "a significant purpose." It also added a provision allowing "Federal officers who conduct electronic surveillance to acquire foreign intelligence information" to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" attack or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities, by foreign powers or their agents. 50 U.S.C. § 1806(k)(1). And such coordination "shall not preclude" the government's certification that a significant purpose of the surveillance is to obtain foreign intelligence information, or the issuance of an order authorizing the surveillance. Id. § 1806(k)(2). Although the Patriot Act amendments to FISA expressly sanctioned consultation and coordination between intelligence and law enforcement officials, in response to the first applications filed by OIPR under those amendments, in November 2001, the FISA court for the first time adopted the 1995 Procedures, as augmented by the January 2000 and August 2001 Procedures, as "minimization procedures" to apply in all cases before the court.\footnote{In particular, the court adopted Part A of the 1995 Procedures, which covers "Contacts During an F1 or FCI Investigation in which FISA Surveillance or Searches are being Conducted." The remainder of the 1995 Procedures addresses contacts in cases where FISA is not at issue.}

The Attorney General interpreted the Patriot Act quite differently. On March 6, 2002, the Attorney General approved new "Intelligence Sharing Procedures" to implement the Act's amendments to FISA. The 2002 Procedures supersede prior procedures and were designed to permit the complete exchange of information and advice between intelligence and law enforcement officials. They eliminated the "direction and control" test and allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance." On March 7, 2002, the government filed a motion with the FISA court, noting that the Department of Justice had adopted the 2002 Procedures and proposing to follow those procedures in all matters before the court. The government also asked the FISA court to vacate its orders adopting the prior procedures as minimization procedures in all cases and imposing special "wall" procedures in certain cases.

Unpersuaded by the Attorney General's interpretation of the Patriot Act, the court ordered that the 2002 Procedures be adopted, with modifications, as minimization procedures to apply in all cases. The court emphasized that the definition of minimization procedures had
not been amended by the Patriot Act, and reasoned that the 2002 Procedures “cannot be used by the government to amend the Act in ways Congress has not.” The court explained:

Given our experience in FISA surveillances and searches, we find that these provisions in sections II.B and III [of the 2002 Procedures], particularly those which authorize criminal prosecutors to advise FBI intelligence officials on the initiation, operation, continuation or expansion of FISA’s intrusive seizures, are designed to enhance the acquisition, retention and dissemination of evidence for law enforcement purposes, instead of being consistent with the need of the United States to “obtain, produce, and disseminate foreign intelligence information” . . . as mandated in §1801(b) and § 1821(4).

May 17, 2001 Opinion at 22 (emphasis added by the FISA court). The FISA court also adopted a new rule of court procedure, Rule 11, which provides that “[a]ll FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney’s Office.”

Undeterred, the government submitted the application at issue in this appeal on July 19, 2002, and expressly proposed using the 2002 Procedures without modification. In an order issued the same day, the FISA judge hearing the application granted an order for surveillance of the target but modified the 2002 Procedures consistent with the court’s May 17, 2002 en banc order. It is the July 19, 2002 order that the government appeals, along with an October 17, 2002 order granting, with the same modifications as the July 19 order, the government’s application for renewal of the surveillance in this case. Because those orders incorporate the May 17, 2002 order and opinion by reference, however, that order and opinion are before us as well.

* * * *

Essentially, the FISA court took portions of the Attorney General’s augmented 1995 Procedures—adopted to deal with the primary purpose standard—and imposed them generically as minimization procedures. In doing so, the FISA court erred. It did not provide any constitutional basis for its action—we think there is none—and misconstrued the main statutory provision on which it relied. The court mistakenly categorized the augmented 1995 Procedures as FISA minimization procedures and then compelled the government to utilize a modified version of those procedures in a way that is clearly inconsistent with the statutory purpose.

Under section 1805 of FISA, “the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that . . . the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title.” 50 U.S.C. § 1805(a)(4). The statute defines minimization procedures in pertinent part.
as:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance.

Section 1801(h) also contains the following proviso:

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes . . .

Id. § 1801(h).

As is evident from the face of section 1801(h), minimization procedures are designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. If the data is not foreign intelligence information as defined by the statute, the procedures are to ensure that the government does not use the information to identify the target or third party, unless such identification is necessary to properly understand or assess the foreign intelligence information that is collected. Id. § 1801(h)(2). By minimizing acquisition, Congress envisioned that, for example, “where a switchboard line is tapped but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party” to the communication. H. Rep. at 55-56. By minimizing retention, Congress intended that “information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed where feasible.” H. Rep. at 56.

Furthermore, “[e]ven with respect to information needed for an approved purpose, dissemination should be restricted to those officials with a need for such information.” Id. (emphasis added).

The minimization procedures allow, however, the retention and dissemination of nonforeign intelligence information which is evidence of ordinary crimes for preventative or prosecutorial purposes. See 50 U.S.C. § 1801(h)(3). Therefore, if through interceptions or searches, evidence of “a serious crime totally unrelated to intelligence matters” is incidentally acquired, the evidence is “not . . . required to be destroyed.” H. Rep. at 62 (emphasis added).

As we have explained, under the 1978 Act, “evidence of certain crimes like espionage would itself constitute ‘foreign intelligence information,’ as defined, because it is necessary to protect against clandestine intelligence activities by foreign powers or their agents.” H. Rep. at 62; see also id. at 49. In light of these purposes of the minimization procedures, there is simply no basis for the FISA court’s reliance on section 1801(h) to limit criminal prosecutors’ ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such
information includes evidence of a foreign intelligence crime.

The FISA court's decision and order not only misinterpreted and misapplied minimization procedures it was entitled to impose, but as the government argues persuasively, the FISA court may well have exceeded the constitutional bounds that restrict an Article III court. The FISA court asserted authority to govern the internal organization and investigative procedures of the Department of Justice which are the province of the Executive Branch (Article II) and the Congress (Article I). Subject to statutes dealing with the organization of the Justice Department, however, the Attorney General has the responsibility to determine how to deploy personnel resources. As the Supreme Court said in *Morrison v. Olson* in cautioning the Special Division of the D.C. Circuit to avoid unauthorized administrative guidance of Independent Counsel, "[t]he gradual expansion of the authority of the Special Division might in another context be a bureaucratic success story, but it would be one that would have serious constitutional ramifications." 487 U.S. 654, 684 (1988).19

* * * *

We also think the refusal by the FISA court to consider the legal significance of the Patriot Act's crucial amendments was error. The government, in order to avoid the requirement of meeting the "primary purpose" test, specifically sought an amendment to section 1804(a)(7)(B) which had required a certification "that the purpose of the surveillance is to obtain foreign intelligence information" so as to delete the article "the" before "purpose" and replace it with "a." The government made perfectly clear to Congress why it sought the legislative change. Congress, although accepting the government's explanation for the need for the amendment, adopted language which it perceived as not giving the government quite the degree of modification it wanted. Accordingly, section 1804(a)(7)(B)'s wording became "that a significant purpose of the surveillance is to obtain foreign intelligence information" (emphasis added). There is simply no question, however, that Congress was keenly aware that this amendment relaxed a requirement that the government show that its primary purpose was other than criminal prosecution.

No committee reports accompanied the Patriot Act but the floor statements make congressional intent quite apparent. The Senate Judiciary Committee Chairman Senator Leahy acknowledged that "[p]rotection against these foreign-based threats by any lawful means is within the scope of the definition of 'foreign intelligence information,' and the use of FISA to gather evidence for the enforcement of these laws was contemplated in the enactment of FISA." 147 Cong. Rec. S10904 (Oct. 25, 2001). "This bill . . . break[s] down traditional barriers between law enforcement and foreign intelligence. This is not done just to combat international terrorism, but for any criminal investigation that overlaps a broad definition of 'foreign intelligence.'" 147 Cong. Rec. S10992 (Oct. 25, 2001) (statement of Sen. Leahy). And Senator Feinstein, a "strong support[er]," was also explicit. The ultimate objective was

---

19 In light of *Morrison v. Olson* and *Mistretta v. United States*, 488 U.S. 361 (1989), we do not think there is much left to an argument made by an opponent of FISA in 1978 that the statutory responsibilities of the FISA court are inconsistent with Article III case and controversy responsibilities of federal judges because of the secret, non-adversary process. See Foreign Intelligence Electronic Surveillance: Hearings on H.R. 3794, 9745, 7908, and 5632 Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence, 95th Cong., 2d Sess. 221 (1978) (statement of Laurence H. Silberman).
to make it easier to collect foreign intelligence information under the Foreign Intelligence Surveillance Act, FISA. Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence.

But in today's world things are not so simple. In many cases, surveillance will have two key goals—the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. Determining which purpose is the "primary" purpose of the investigation can be difficult, and will only become more so as we coordinate our intelligence and law enforcement efforts in the war against terror.

Rather than foreclose law enforcement to decide which purpose is primary—law enforcement or foreign intelligence gathering, this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA.

The effect of this provision will be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution. Many of the individuals involved in supporting the September 11 attacks may well fall into both of these categories.


To be sure, some Senate Judiciary Committee members including the Chairman were concerned that the amendment might grant too much authority to the Justice Department and the FISA court. Senator Leahy indicated that the change to significant purpose was "very problematic" since it would "make it easier for the FBI to use a FISA wiretap to obtain information where the Government's most important motivation for the wiretap is for use in a criminal prosecution." 147 Cong. Rec. S10593 (Oct. 11, 2001). Therefore he suggested that "it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of 'foreign intelligence information.'" 147 Cong. Rec. S11004 (Oct. 25, 2001) (emphasis added).

But the only dissenting vote against the act was cast by Senator Feingold. For the Record: Senate Votes, 59 CONG. QUARTERLY (Wkly.) 39, Oct. 13, 2001, at 2425. Senator Feingold recognized that the change to "significant purpose" meant that the government could obtain a FISA warrant "even if the primary purpose is a criminal investigation," and was concerned that this development would not respect the protections of the Fourth Amendment. 147 Cong. Rec. S11021 (Oct. 25, 2001).

In sum, there can be no doubt as to Congress’ intent in amending section 1804(a)(7)(B).

Indeed, it went further to emphasize its purpose in breaking down barriers between criminal law enforcement and intelligence (or counterintelligence) gathering by adding section 1806(k):

(k) Consultation with Federal law enforcement officers

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, or

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power, or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1804(a) of this title or the entry of an order under section 1805 of this title.

The FISA court noted this amendment but thought that Congress' approval of consultations was not equivalent to authorizing law enforcement officers to give advice to officers who were conducting electronic surveillance nor did it sanction law enforcement officers “directing or controlling” surveillances. However, dictionary definitions of “consult” include giving advice. See, e.g., OXFORD ENGLISH DICTIONARY ONLINE (2d ed. 1989).

Beyond that, when Congress explicitly authorizes consultation and coordination between different offices in the government, without even suggesting a limitation on who is to direct and control, it necessarily implies that either could be taking the lead.

Neither amicus brief defends the reasoning of the FISA court. NACDL's brief makes no attempt to interpret FISA or the Patriot Act amendments but rather argues the primary purpose test is constitutionally compelled. The ACLU relies on Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522, to interpret FISA, passed 10 years later. That technique, to put it gently, is hardly an orthodox method of statutory interpretation. FISA was passed to deal specifically with the subject of foreign intelligence surveillance. The ACLU does argue that Congress’ intent to preclude law enforcement officials initiating or controlling foreign intelligence investigations is revealed by FISA’s exclusion of the Attorney General—a law enforcement official from the officers who can certify the foreign intelligence purpose of an application under section 1804. The difficulty with that argument is that the Attorney General supervises the Director of the FBI who is both a law enforcement and counterintelligence officer. The Attorney General or the Deputy Attorney General, moreover, must approve all applications no matter who certifies that the information sought is foreign intelligence information. 50 U.S.C. § 1804(a).

The ACLU insists that the significant purpose amendment only “clarified” the law permitting FISA surveillance orders “even if foreign intelligence is not its exclusive purpose” (emphasis added). In support of this rather strained interpretation, which ignores the legislative history of the Patriot Act, the ACLU relies on a September 10, 2002 hearing of the Judiciary Committee (the day after the government's oral presentation to this court) at which certain senators made statements—somewhat at odds with their floor statements prior to the passage of the Patriot Act—on to what they had intended the year before. The D.C. Circuit has described such post-enactment legislative statements as “legislative fiction” rather than legislative history, not entitled to authoritative weight. See General Instrument Corp. v. FCC, 213 F.3d 724, 733 (D.C. Cir. 2000).

Accordingly, the Patriot Act amendments clearly disapprove the primary purpose test. And as a matter of straightforward logic, if a FISA application can be granted even if “foreign intelligence” is only a significant—not a primary—purpose, another purpose can be primary.

Furthermore, the Attorney General of Deputy Attorney General must approve the use in a criminal proceeding of information acquired pursuant to FISA. 50 U.S.C. § 1806(b).
One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime. We therefore believe the Patriot Act amply supports the government's alternative argument but, paradoxically, the Patriot Act would seem to conflict with the government's first argument because by using the term "significant purpose," the Act now implies that another purpose is to be distinguished from a foreign intelligence purpose.

The government heroically tries to give the amended section 1804(a)(7)(B) a wholly benign interpretation. It concedes that "the 'significant purpose' amendment recognizes the existence of the dichotomy between foreign intelligence and law enforcement," but it contends that "it cannot be said to recognize (or approve) its legitimacy." Supp. Br. of U.S. at 25 (emphasis in original). We are not persuaded. The very letter the Justice Department sent to the Judiciary Committee in 2001 defending the constitutionality of the significant purpose language implicitly accepted as legitimate the dichotomy in FISA that the government now claims (and we agree) was false. It said, "it is also clear that while FISA states that 'the' purpose of a search is for foreign surveillance, that need not be the only purpose. Rather, law enforcement considerations can be taken into account, so long as the surveillance also has a legitimate foreign intelligence purpose." The senatorial statements explaining the significant purpose amendments which we described above are all based on the same understanding of FISA which the Justice Department accepted at least until this appeal. In short, even though we agree that the original FISA did not contemplate the "false dichotomy," the Patriot Act actually did—which makes it no longer false. The addition of the word "significant" to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes. Although section 1805(a)(3), as we discussed above, may well have been intended to authorize the FISA court to review only the question whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804 it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information.

That leaves us with something of an analytic conundrum. On the one hand, Congress did not amend the definition of foreign intelligence information which, we have explained, includes evidence of foreign intelligence crimes. On the other hand, Congress accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test. Nevertheless, it is our task to do our best to read the statute to honor congressional intent. The better reading, it seems to us, excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution. We therefore reject the government's argument to the contrary. Yet this may not make much practical difference. Because, as the government points out, when it commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent (whatever may be the subjective intent of the investigators or lawyers who initiate an investigation). So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.

The important point is—and here we agree with the government—the Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to
balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the application's purpose articulates a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.

The government claims that even prosecutions of non-foreign intelligence crimes are consistent with a purpose of gaining foreign intelligence information so long as the government's objective is to stop espionage or terrorism by putting an agent of a foreign power in prison. That interpretation transgresses the original FISA. It will be recalled that Congress intended section 1804(a)(7)(B) to prevent the government from targeting a foreign agent when its "true purpose" was to gain non-foreign intelligence information—such as evidence of ordinary crimes or scandals. See supra at p.14. (If the government inadvertently came upon evidence of ordinary crimes, FISA provided for the transmission of that evidence to the proper authority. 50 U.S.C. § 1801(b)(3).) It can be argued, however, that by providing that an application is to be granted if the government has only a "significant purpose" of gaining foreign intelligence information, the Patriot Act allows the government to have a primary objective of prosecuting an agent for a non-foreign intelligence crime. Yet we think that would be an anomalous reading of the amendment. For we see not the slightest indication that Congress meant to give that power to the Executive Branch. Accordingly, the manifestation of such a purpose, it seems to us, would continue to disqualify an application. That is not to deny that ordinary crimes might be inextricably intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself. But the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.

One final point; we think the government's purpose as set forth in a section 1804(a)(7)(B) certification is to be judged by the national security official's articulation and not by a FISA court inquiry into the origins of an investigation or an examination of the personnel involved. It is up to the Director of the FBI, who typically certifies, to determine the government's national security purpose, as approved by the Attorney General or Deputy Attorney General. This is not a standard whose application the FISA court legitimately reviews by seeking to inquire into which Justice Department officials were instigators of an investigation. All Justice Department officials—including those in the FBI—are under the control of the Attorney General. If he wishes a particular investigation to be run by an officer of any division, that is his prerogative. There is nothing in FISA or the Patriot Act that suggests otherwise. That means, perforce, if the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose—or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval. The important point is that the relevant
purpose is that of those senior officials in the Executive Branch who have the responsibility
of appraising the government's national security needs.

III.

Having determined that FISA, as amended, does not oblige the government to demon-
strate to the FISA court that its primary purpose in conducting electronic surveillance is not
criminal prosecution, we are obliged to consider whether the statute as amended is consistent
with the Fourth Amendment. The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,
shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly
describing the place to be searched, and the persons or things to be seized.

Although the FISA court did not explicitly rely on the Fourth Amendment, it at least suggested
that this provision was the animating principle driving its statutory analysis. The FISA court
indicated that its disapproval of the Attorney General's 2002 Procedures was based on the need
to safeguard the "privacy of Americans in these highly intrusive surveillances and searches,"
which implies the invocation of the Fourth Amendment. The government, recognizing the
Fourth Amendment's shadow effect on the FISA court's opinion, has affirmatively argued that
FISA is constitutional. And some of the very senators who fashioned the Patriot Act
amendments expected that the federal courts, including presumably the FISA court, would
carefully consider that question. Senator Leahy believed that "[n]o matter what statutory
change is made . . . the court may impose a constitutional requirement of 'primary purpose'
based on the appellate court decisions upholding FISA against constitutional challenges over
the past 20 years." 147 Cong. Rec. S11003 (Oct. 25, 2001). Senator Edwards stated that "the
FISA court will still need to be careful to enter FISA orders only when the requirements of the
Constitution as well as the statute are satisfied." 147 Cong. Rec. S10589 (Oct. 11, 2001).

We are, therefore, grateful to the ACLU and NACDL for their briefs that vigorously
contest the government's argument. Both NACDL (which, as we have noted above, presents
only the argument that the statute as amended is unconstitutional) and the ACLU rely on two
propositions. The first is not actually argued; it is really an assumption—that a FISA order does
not qualify as a warrant within the meaning of the Fourth Amendment. The second is that any
government surveillance whose primary purpose is criminal prosecution of whatever kind
is per se unreasonable if not based on a warrant.

The FISA court expressed concern that unless FISA were "construed" in the fashion that
it did, the government could use a FISA order as an improper substitute for an ordinary
criminal warrant under Title III. That concern seems to suggest that the FISA court thought
Title III procedures are constitutionally mandated if the government has a prosecutorial
objective regarding an agent of a foreign power. But in United States v. United States District
Court (Keith), 407 U.S. 297, 322 (1972) in which the Supreme Court explicitly declined to
consider foreign intelligence surveillance—the Court indicated that, even with respect to
domestic national security intelligence gathering for prosecutorial purposes where a warrant
was mandated, Title III procedures were not constitutionally required: "[W]e do not hold that
the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime.” Nevertheless, in asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts. Obviously, the closer those FISA procedures are to Title III procedures, the lesser are our constitutional concerns.

Comparison of FISA Procedures with Title III

It is important to note that while many of FISA’s requirements for a surveillance order differ from those in Title III, few of those differences have any constitutional relevance. In the context of ordinary crime, beyond requiring searches and seizures to be reasonable, the Supreme Court has interpreted the warrant clause of the Fourth Amendment to require three elements:

First, warrants must be issued by neutral, disinterested magistrates. Second, those seeking the warrant must demonstrate to the magistrate their probable cause to believe that “the evidence sought will aid in a particular apprehension or conviction” for a particular offense. Finally, “warrants must particularly describe the ‘things to be seized,’” as well as the place to be searched.


With limited exceptions not at issue here, both Title III and FISA require prior judicial scrutiny of an application for an order authorizing electronic surveillance. 50 U.S.C. § 1805;

18 U.S.C. § 2518. And there is no dispute that a FISA judge satisfies the Fourth Amendment’s requirement of a “neutral and detached magistrate.” See *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (FISA court is a “detached and neutral body”); see also *Keith*, 407 U.S. at 323 (in domestic national security context, suggesting that a request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court).

The statutes differ to some extent in their probable cause showings. Title III allows a court to enter an *ex parte* order authorizing electronic surveillance if it determines on the basis of the facts submitted in the government’s application that “there is probable cause for belief that an individual is committing, has committed, or is about to commit” a specified predicate offense. 18 U.S.C. § 2518(3)(a). FISA by contrast requires a showing of probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1803(a)(3).

We have noted, however, that where a U.S. person is involved, an “agent of a foreign power” is defined in terms of criminal activity.21 Admittedly, the definition of one category of U.S.-person agents of foreign powers—that is, persons engaged in espionage and clandestine intelligence activities for a foreign power—does not necessarily require a showing of an imminent violation of criminal law. See 50 U.S.C. § 1801(b)(2)(A) (defining such activities as those which “involve” or “may involve” a violation of criminal statutes of the United States).

---

21 The term “foreign power,” which is not directly at issue in this case, is not defined solely in terms of criminal activity. For example, although the term includes a group engaged in international terrorism, which would involve criminal activity, it also includes any foreign government. 50 U.S.C. § 1801(a)(1).
Congress clearly intended a lesser showing of probable cause for these activities than that applicable to ordinary criminal cases. See H. REP. at 39-40, 79. And with good reason—these activities present the type of threats contemplated by the Supreme Court in Keith when it recognized that the focus of security surveillance "may be less precise than that directed against more conventional types of crime" even in the area of domestic threats to national security. Keith, 407 U.S. at 322. Congress was aware of Keith's reasoning, and recognized that it applies a fortiori to foreign threats. See S. REP. at 15. As the House Report notes with respect to clandestine intelligence activities:

The term "may involve" not only requires less information regarding the crime involved, but also permits electronic surveillance at some point prior to the time when a crime sought to be prevented, as for example, the transfer of classified documents, actually occurs.

H. REP. at 40. Congress allowed this lesser showing for clandestine intelligence activities—but not, notably, for other activities, including terrorism—because it was fully aware that such foreign intelligence crimes may be particularly difficult to detect.22 At the same time, however, it provided another safeguard not present in Title III—that is, the requirement that there be probable cause to believe the target is acting "for or on behalf of a foreign power."

Under the definition of "agent of a foreign power" FISA surveillance could not be authorized against an American reporter merely because he gathers information for publication in a newspaper, even if the information was classified by the Government. Nor would it be authorized against a Government employee or former employee who reveals secrets to a reporter or in a book for the purpose of informing the American people. This definition would not authorize surveillance of ethnic Americans who lawfully gather political information and perhaps even lawfully share it with the foreign government of their national origin. It obviously would not apply to lawful activities to lobby, influence, or inform Members of Congress or the administration to take certain positions with respect to foreign or domestic concerns. Nor would it apply to lawful gathering of information preparatory to such lawful activities.

H. REP. at 40. Similarly, FISA surveillance would not be authorized against a target engaged in purely domestic terrorism because the government would not be able to show that the target is acting for or on behalf of a foreign power. As should be clear from the foregoing, FISA applies only to certain carefully delineated, and particularly serious, foreign threats to national security.

Turning then to the first of the particularity requirements, while Title III requires probable cause to believe that particular communications concerning the specified crime will be obtained through the interception, 18 U.S.C. § 2518(3)(b), FISA instead requires an official to designate the type of foreign intelligence information being sought, and to certify that the information sought is foreign intelligence information. When the target is a U.S. person, the FISA judge reviews the certification for clear error, but this "standard of review is not, of course, comparable to a probable cause finding by the judge." H. REP. at 80. Nevertheless, FISA provides additional protections to ensure that only pertinent information is sought. The certification must be made by a national security officer—typically the FBI Director—and must...
be approved by the Attorney General or the Attorney General’s Deputy. Congress recognized
that this certification would “assure[] written accountability within the Executive Branch” and
provide “an internal check on Executive Branch arbitrariness.” H. REP. at 80. In addition, the
court may require the government to submit any further information it deems necessary to
determine whether or not the certification is clearly erroneous. See 50 U.S.C. § 1804(d).

With respect to the second element of particularity, although Title III generally
requires probable cause to believe that the facilities subject to surveillance are being used or
are about to be used in connection with commission of a crime or are leased to, listed in the
name of, or used by the individual committing the crime, 18 U.S.C. § 2518(3)(d), FISA
requires probable cause to believe that each of the facilities or places at which the surveillance
is directed is being used, or is about to be used, by a foreign power or agent. 50 U.S.C. §
1805(a)(3)(B). In cases where the targeted facilities are not leased to, listed in the name of,
or used by the individual committing the crime, Title III requires the government to show a
nexus between the facilities and communications regarding the criminal offense. The
government does not have to show, however, anything about the target of the surveillance; it
is enough that “un individual”—not necessarily the target—is committing a crime. 18 U.S.C.
§§ 2518(3)(a), (d); see United States v. Kahn, 415 U.S. 143, 157 (1974) (“when there is
probable cause to believe that a particular telephone is being used to commit an offense but
no particular person is identifiable, a wire interception order may, nevertheless, properly issue
under [Title III]”). On the other hand, FISA requires probable cause to believe the target is an
agent of a foreign power (that is, the individual committing a foreign intelligence crime who
uses or is about to use the targeted facility. Simply put, FISA requires less of a nexus between
the facility and the pertinent communications than Title III, but more of a nexus between the
target and the pertinent communications. See H. REP. at 73 (“the target of a surveillance is
the individual or entity or about whom or from whom information is sought”).

There are other elements of Title III that at least some circuits have determined are
constitutionally significant—that is, necessity, duration of surveillance, and minimization. See,
e.g., United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994). Both statutes have a “necessity”
provision, which requires the court to find that the information sought is not available through
1805(a)(5). Although the court’s clearly erroneous review under FISA is more limited than
under Title III, this greater deference must be viewed in light of FISA’s additional requirement
that the certification of necessity come from an upper level Executive Branch official. The
statutes also have duration provisions; Title III orders may last up to 30 days, 18 U.S.C. §
2518(5), while FISA orders may last up to 90 days for U.S. persons. 50 U.S.C. § 1805(c)(1).
This difference is based on the nature of national security surveillance, which is “often long
range and involves the interrelation of various sources and types of information.” Keith, 407
U.S. at 322; see also S. REP. at 16, 56. Moreover, the longer surveillance period is balanced
by continuing FISA court oversight of minimization procedures during that period. 50 U.S.C.
§ 1805(c)(3); see also S. REP. at 56. And where Title III requires minimization of what is
acquired, as we have discussed, for U.S. persons, FISA requires minimization of what is acquired, retained, and disseminated. The FISA court notes, however, that in practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications. The reasonableness of this approach depends on the facts and circumstances of each case. *Scott v. United States*, 436 U.S. 128, 140-43 (1978) (acquisition of virtually all conversations was reasonable under the circumstances). Less minimization in the acquisition stage may well be justified to the extent the intercepted communications are “ambiguous in nature or apparently involve[] guarded or coded language,” or “the investigation is focusing on what is thought to be a widespread conspiracy [where] more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise.” *Id.* at 140. Given the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots. 

Amici particularly focus on the differences between the two statutes concerning Title III requires agents to conduct surveillance “in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter.” 18 U.S.C. § 2518(5).

\[24\] Amici also emphasize that Title III generally entitles a defendant to obtain the surveillance application and order to challenge to the legality of the surveillance, 18 U.S.C. § 2518(9), while FISA does not normally allow a defendant to obtain the same if the Attorney General states that disclosure or an adversary hearing would harm national security, 50 U.S.C. § 1806(f). Under such circumstances, the judge conducts an *in camera* and *ex parte* review to determine whether the electronic surveillance was lawful, whether disclosure or discovery is necessary, and whether to grant a motion to suppress. *Id.* §§ 1806(f), (g). Clearly, the decision whether to allow a defendant to obtain FISA materials is made by a district judge on a case by case basis, and the issue whether such a decision protects a defendant’s constitutional rights in any given case is not before us.

\[25\] In addition to the protections already discussed, FISA has more extensive reporting requirements than Title III, *compare* 18 U.S.C. § 2519(2) with 50 U.S.C. § 1808(a)(1), and is subject to close and continuing oversight by Congress as a check against Executive Branch abuses. S. REP. at 11-12. Also, the Patriot Act contains sunset provisions, see Section 224(a)
diverge in constitutionally relevant areas—in particular, in their probable cause and particularity showings—a FISA order may not be a "warrant" contemplated by the Fourth Amendment. The government itself does not actually claim that it is, instead noting only that there is authority for the proposition that a FISA order is a warrant in the constitutional sense. See Cavanagh, 807 F.2d at 790 (concluding that FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause); see also Pelton, 835 F.2d at 1075 (joining Cavanagh in holding that FISA procedures meet constitutional requirements); Ful bey, 540 F. Supp. at 1314 (holding that unlike in Truong, a congressionally crafted warrant that met Fourth Amendment standards was obtained authorizing the surveillance). We do not decide the issue but note that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment.

Did Truong Articulate the Appropriate Constitutional Standard?

Ultimately, the question becomes whether FISA, as amended by the Patriot Act, is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens. Cf. Keith, 407 U.S. at 322-23 (in domestic security context, holding that standards different from those in Title III "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the government for intelligence information and the protected rights of our citizens"). To answer that question—whether the Patriot Act's disavowal of the primary purpose test is constitutional—besides comparing the FISA procedures with Title III, it is necessary to consider carefully the underlying rationale of the primary purpose test.

It will be recalled that the case that set forth the primary purpose test as constitutionally required was Truong. The Fourth Circuit thought that Keith's balancing standard implied the adoption of the primary purpose test. We reiterate that Truong dealt with a pre-FISA surveillance based on the President's constitutional responsibility to conduct the foreign affairs of the United States. 629 F.2d at 914. Although Truong suggested the line it drew was a constitutional minimum that would apply to a FISA surveillance, see id. at 914 n.4, it had no occasion to consider the application of the statute carefully. The Truong court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.26 It was incumbent upon the court, therefore, to determine the boundaries of that constitutional authority in the case before it. We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power. The question before us is the reverse, does FISA amplify the President's power by providing a

26 Although the plurality opinion in Zwenon v. Mitchell, 516 F.2d 594, 633-35 (D.C. Cir. 1975) (en banc), cert. denied, 425 U.S. 944 (1976), suggested the contrary in dicta, it did not decide the issue.
mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable.

The district court in the *Truong* case had excluded evidence obtained from electronic surveillance after the government’s investigation—the court found—had converted from one conducted for foreign intelligence reasons to one conducted primarily as a criminal investigation. (The defendants were convicted based in part on surveillance evidence gathered before that point.) The district judge had focused on the date that the Criminal Division had taken a central role in the investigation. The court of appeals endorsed that approach stating:

> We think that the district court adopted the proper test, because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis of a criminal prosecution.

*Id.* at 915 (emphasis added).

That analysis, in our view, rested on a false premise and the line the court sought to draw was inherently unstable, unrealistic, and confusing. The false premise was the assertion that once the government moves to criminal prosecution, its “foreign policy concerns” recede. As we have discussed in the first part of the opinion, that is simply not true as it relates to counterintelligence. In that field the government's primary purpose is to halt the espionage or terrorism efforts, and criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power’s efforts. Indeed, the Fourth Circuit itself, rejecting defendant's arguments that it should adopt a “solely foreign intelligence purpose test,” acknowledged that “almost all foreign intelligence investigations are in part criminal investigations.” *Id.* (It would have been more accurate to refer to counterintelligence investigations.)

The method the court endorsed for determining when an investigation became primarily criminal was based on the organizational structure of the Justice Department. The court determined an investigation became primarily criminal when the Criminal Division played a lead role. This approach has led, over time, to the quite intrusive organizational and personnel tasking the FISA court adopted. Putting aside the impropriety of an Article III court imposing such organizational strictures (which we have already discussed), the line the *Truong* court adopted—subsequently referred to as a “wall”—was unstable because it generates dangerous confusion and creates perverse organizational incentives. See, e.g., AGRIT Report at 723-26.\(^\text{27}\)

That is so because counterintelligence brings to bear both classic criminal investigation techniques as well as less focused intelligence gathering. Indeed, effective counterintelligence, we have learned, requires the wholehearted cooperation of all the government's personnel who can be brought to the task. A standard which punishes such cooperation could well be thought dangerous to national security.\(^\text{28}\) Moreover, by focusing on

---

\(^{27}\) We are told that the FBI has even thought it necessary because of FISA court rulings to pass off a criminal investigation to another government department when the FBI was conducting a companion counterintelligence inquiry.

\(^{28}\) The AGRIT Report bears this out: "Unfortunately, the practice of excluding the Criminal Division from FCI investigations was not an isolated event confined to the Wen Ho Lee matter. It has been a way of doing business for OSIPR, acquiesced in by the FBI, and inexplicably indulged by the Department of Justice. One FBI supervisor has said that it has
the subjective motivation of those who initiate investigations, the Truong standard, as
administered by the FISA court, could be thought to discourage desirable initiatives. (It is also
at odds with the Supreme Court’s Fourth Amendment jurisprudence which regards the
subjective motivation of an officer conducting a search or seizure as irrelevant. See, e.g.,
Wisconsin v. United States, 517 U.S. 806 (1996).)

Recent testimony before the Joint Intelligence Committee amply demonstrates that the
Truong line is a very difficult one to administer. Indeed, it was suggested that the FISA court
requirements based on Truong may well have contributed, whether correctly understood or
not, to the FBI missing opportunities to anticipate the September 11, 2001 attacks.29 That is
not to say that we should be prepared to jettison Fourth Amendment requirements in the
interest of national security. Rather, assuming arguendo that FISA orders are not Fourth
Amendment warrants, the question becomes, are the searches constitutionally reasonable. And

only been ‘lucky’ that a case has not yet been hampered by the rigid interpretation of the rules
governing contacts with the Criminal Division. It may be said that in the Wen Ho Lee
investigation, luck ran out.” Id. at 708 (citation omitted).

29 An FBI agent recently testified that efforts to conduct a criminal investigation of two
of the alleged hijackers were blocked by senior FBI officials—understandably concerned about
prior FISA court criticism—who interpreted that court’s decisions as precluding a criminal
investigator’s role. One agent, frustrated at encountering the “wall,” wrote to headquarters:
“[S]omeday someone will die and wall or not-the public will not understand why we were not
more effective and throwing everyone resource we had at certain ‘problems.’ Let’s hope the
National Security Law Unit will stand behind their decisions then, especially since the biggest
threat to us now, [Usama Bin Laden], is getting the most ‘protection.'” The agent was told in
response that headquarters was frustrated with the issue, but that those were the rules, and the
National Security Law Unit does not make them up. The Malaysia Hijacking and September
11th: Joint Hearing Before the Senate and House Select Intelligence Committees (Sept. 20,

in judging reasonableness, the instability of the Truong line is a relevant consideration.

The Fourth Circuit recognized that the Supreme Court had never considered the constitu-
tionality of warrantless government searches for foreign intelligence reasons, but concluded
the analytic framework the Supreme Court adopted in Keith-in the case of domestic
intelligence surveillance-pointed the way to the line the Fourth Circuit drew. The Court in
Keith had, indeed, balanced the government’s interest against individual privacy interests,
which is undoubtedly the key to this issue as well, but we think the Truong court misconceived
the government’s interest and, moreover, did not draw a more appropriate distinction that Keith
at least suggested. That is the line drawn in the original FISA statute itself between ordinary
crimes and foreign intelligence crimes.

It will be recalled that Keith carefully avoided the issue of a warrantless foreign
intelligence search: “We have not addressed, and express no opinion as to, the issues which
may be involved with respect to activities of foreign powers or their agents.” 407 U.S. at 321-
22. But in indicating that a somewhat more relaxed warrant could suffice in the domestic
intelligence situation, the court drew a distinction between the crime involved in that case,
which posed a threat to national security, and “ordinary crime.” Id. at 322. It pointed out that
“the focus of domestic surveillance may be less precise than that directed against more
conventional types of crimes.” Id.

The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to

30 The Court in a footnote though, cited authority for the view that warrantless
surveillance may be constitutional where foreign powers are involved. Keith, 407 U.S. at 322
n.20.
deter other persons in society from embarking on the same course. The government’s concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity. As we discussed in the first section of this opinion, the criminal process is often used as part of an integrated effort to counter the malign efforts of a foreign power. Punishment of the terrorist or espionage agent is really a secondary objective. Indeed, punishment of a terrorist is often a moot point.

Supreme Court’s Special Needs Cases

The distinction between ordinary criminal prosecutions and extraordinary situations underlies the Supreme Court’s approval of entirely warrantless and even suspicionless searches that are designed to serve the government’s “special needs, beyond the normal need for law enforcement.” Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (internal quotation marks omitted)) (random drug-testing of student athletes).32 Apprehending drunk drivers and securing the border constitute such unique interests beyond ordinary, general law enforcement. Id. at 654 (citing Michigan Dep’t of State Police v. Sitz, 496 U.S. 444 (1990), and United States v. Martinez-Fuerte, 428 U.S. 543 (1976)).

A recent case, City of Indianapolis v. Edmond, 531 U.S. 32 (2000), is relied on by both the government and amici. In that case, the Court held that a highway check point designed to catch drug dealers did not fit within its special needs exception because the government’s “primary purpose” was merely “to uncover evidence of ordinary criminal wrongdoing.” Id. at 41-42. The Court rejected the government’s argument that the “severe and intractable nature of the drug problem” was sufficient justification for such a dragnet seizure lacking any individualized suspicion. Id. at 42. Amici particularly rely on the Court’s statement that “the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose.” Id.

But by “purpose” the Court makes clear it was referring not to a subjective intent, which is not relevant in ordinary Fourth Amendment probable cause analysis, but rather to a programmatic purpose. The Court distinguished the prior check point cases Martinez-Fuerte (involving checkpoints less than 100 miles from the Mexican border) and Sitz (checkpoints to detect intoxicated motorists) on the ground that the former involved the government’s “longstanding concern for the protection of the integrity of the border,” id. at 38 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985)), and the latter was “aimed at reducing the immediate hazard posed by the presence of drunk drivers on the highways.” Id. at 39. The Court emphasized that it was decidedly not drawing a distinction between suspicionless seizures with a “non-law-enforcement primary purpose” and those designed for law enforcement. Id. at 44 n.1. Rather, the Court distinguished general crime control

31 To be sure, punishment of a U.S. person’s espionage for a foreign power does not have a deterrent effect on others similarly situated.

programs and those that have another particular purpose, such as protection of citizens against special hazards or protection of our borders. The Court specifically acknowledged that an appropriately tailored roadblock could be used "to thwart an imminent terrorist attack." *Id.* at 44. The nature of the "emergency," which is simply another word for threat, takes the matter out of the realm of ordinary crime control.35

Conclusion

FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from "ordinary crime control." After the events of September 11, 2001, though, it is hard to imagine greater emergencies facing Americans than those experienced on that date.

We acknowledge, however, that the constitutional question presented by this case—whether Congress's disapproval of the primary purpose test is consistent with the Fourth Amendment—has no definitive jurisprudential answer. The Supreme Court's special needs cases involve random stops (seizures) not electronic searches. In one sense, they can be thought of as a greater encroachment into personal privacy because they are not based on any particular suspicion. On the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning.

Although the Court in City of Indianapolis cautioned that the threat to society is not dispositive in determining whether a search or seizure is reasonable, it certainly remains a crucial factor. Our case may well involve the most serious threat our country faces. Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from *Keith*, that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

Accordingly, we reverse the FISA court's orders in this case to the extent they imposed conditions on the grant of the government's applications, vacate the FISA court's Rule 11, and remand with instructions to grant the applications as submitted and proceed henceforth in accordance with this opinion.

35 *Amici* rely on *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), in arguing that the "special needs" cases acknowledge that the Fourth Amendment is particularly concerned with intrusions whose primary purpose is to gather evidence of crime. In that case, the Court struck down a non-consensual policy of testing obstetrics patients for drug use. The Court stated that "[w]hile the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs, the immediate objective of the searches was to generate evidence for law enforcement purposes in order to reach that goal." *Id.* at 82-83 (emphasis in original, footnotes omitted). In distinguishing the "special needs" cases, the Court noted that "[i]t is especially difficult to argue that the program here was designed simply to save lives," in light of evidence that the sort of program at issue actually discouraged women from seeking prenatal care. *Id.* at 844 n.23. Thus, *Ferguson* does not involve a situation in which law enforcement is directly connected to the prevention of a special harm.
PUBLIC LAW 110–53—AUG. 3, 2007

IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007
An Act

To provide for the implementation of the recommendations of the National Commission on Terrorist Attacks Upon the United States.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Implementing Recommendations of the 9/11 Commission Act of 2007”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—HOMELAND SECURITY GRANTS

Sec. 101. Homeland Security Grant Program.
Sec. 102. Other amendments to the Homeland Security Act of 2002.
Sec. 104. Technical and conforming amendments.

TITLE II—EMERGENCY MANAGEMENT PERFORMANCE GRANTS

Sec. 201. Emergency management performance grant program.

TITLE III—ENSURING COMMUNICATIONS INTEROPERABILITY FOR FIRST RESPONDERS

Sec. 301. Interoperable emergency communications grant program.
Sec. 302. Border interoperability demonstration project.

TITLE IV—STRENGTHENING USE OF THE INCIDENT COMMAND SYSTEM

Sec. 401. Definitions.
Sec. 402. National exercise program design.
Sec. 403. National exercise program model exercises.
Sec. 404. Preidentifying and evaluating multijurisdictional facilities to strengthen incident command; private sector preparedness.
Sec. 405. Federal response capability inventory.
Sec. 406. Reporting requirements.
Sec. 407. Federal preparedness.
Sec. 408. Credentialing and typing.
Sec. 409. Model standards and guidelines for critical infrastructure workers.
Sec. 410. Authorization of appropriations.

TITLE V—IMPROVING INTELLIGENCE AND INFORMATION SHARING WITHIN THE FEDERAL GOVERNMENT AND WITH STATE, LOCAL, AND TRIBAL GOVERNMENTS

Subtitle A—Homeland Security Information Sharing Enhancement

Sec. 501. Homeland Security Advisory System and information sharing.
Sec. 502. Intelligence Component Defined.
Sec. 503. Role of intelligence components, training, and information sharing.
Sec. 504. Information sharing.
PUBLIC LAW 110–53—AUG. 3, 2007

“(I) The Under Secretary of Homeland Security for Intelligence and Analysis.”
(c) TREATMENT OF INCUMBENT.—The individual administratively performing the duties of the Under Secretary for Intelligence and Analysis as of the date of the enactment of this Act may continue to perform such duties after the date on which the President nominates an individual to serve as the Under Secretary pursuant to section 201 of the Homeland Security Act of 2002, as amended by this section, and until the individual so appointed assumes the duties of the position.

Subtitle E—Authorization of Appropriations

SEC. 541. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for each of fiscal years 2008 through 2012 such sums as may be necessary to carry out this title and the amendments made by this title.

TITLE VI—CONGRESSIONAL OVERSIGHT OF INTELLIGENCE

SEC. 601. AVAILABILITY TO PUBLIC OF CERTAIN INTELLIGENCE FUNDING INFORMATION.

(a) AMOUNTS APPROPRIATED EACH FISCAL YEAR.—Not later than 30 days after the end of each fiscal year beginning with fiscal year 2007, the Director of National Intelligence shall disclose to the public the aggregate amount of funds appropriated by Congress for the National Intelligence Program for such fiscal year.
(b) WAIVER.—Beginning with fiscal year 2009, the President may waive or postpone the disclosure required by subsection (a) for any fiscal year by, not later than 30 days after the end of such fiscal year, submitting to the Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives—

(1) a statement, in unclassified form, that the disclosure required in subsection (a) for that fiscal year would damage national security; and
(2) a statement detailing the reasons for the waiver or postponement, which may be submitted in classified form.
(c) DEFINITION.—As used in this section, the term “National Intelligence Program” has the meaning given the term in section 3(6) of the National Security Act of 1947 (50 U.S.C. 401a(6)).

SEC. 602. PUBLIC INTEREST DECLASSIFICATION BOARD.

The Public Interest Declassification Act of 2000 (50 U.S.C. 435 note) is amended—
(1) by striking “Director of Central Intelligence” each place that term appears and inserting “Director of National Intelligence”;
(2) in section 704(e)—
(A) by striking “If requested” and inserting the following:
“(1) IN GENERAL.—If requested”;
and

219
U.S. Intelligence Community Budget

The U.S. intelligence budget has two major components: the National Intelligence Program and the Military Intelligence Program. The National Intelligence Program includes all programs, projects, and activities of the intelligence community as well as any other intelligence community programs designated jointly by the DNI and the head of department or agency, or the DNI and the President.

The MIP is devoted to intelligence activity conducted by the military departments and agencies in the Department of Defense that support tactical U.S. military operations. In addition, other departments and agencies may engage in certain activities related to intelligence for their own mission needs that are not captured here.

### U.S. INTELLIGENCE COMMUNITY BUDGET

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>NIP Budget Requested</th>
<th>NIP Budget Appropriated</th>
<th>MIP Budget Requested</th>
<th>MIP Budget Appropriated</th>
<th>Total Appropriated</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>$53.9 Billion</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>$50.4 Billion</td>
<td>$16.6 Billion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>$52.2 Billion</td>
<td>$50.5 Billion</td>
<td>$14.6 Billion</td>
<td>$17.4 Billion</td>
<td>67.9 Billion</td>
</tr>
<tr>
<td>2013</td>
<td>$52.6 Billion</td>
<td>$49.0 Billion</td>
<td>$19.2 Billion</td>
<td>$18.6 Billion</td>
<td>67.6 Billion</td>
</tr>
<tr>
<td>2012</td>
<td>$55.0 Billion</td>
<td>$53.9 Billion</td>
<td></td>
<td>$21.5 Billion</td>
<td>75.4 Billion</td>
</tr>
<tr>
<td>2011</td>
<td>---</td>
<td>$54.6 Billion</td>
<td></td>
<td>$24.0 Billion</td>
<td>78.6 Billion</td>
</tr>
<tr>
<td>2010</td>
<td>---</td>
<td>$53.1 Billion</td>
<td></td>
<td>$27.0 Billion</td>
<td>80.1 Billion</td>
</tr>
<tr>
<td>2009</td>
<td>---</td>
<td>$49.6 Billion</td>
<td></td>
<td>$26.4 Billion</td>
<td>76.2 Billion</td>
</tr>
<tr>
<td>2008</td>
<td>---</td>
<td>$47.5 Billion</td>
<td></td>
<td>$22.9 Billion</td>
<td>70.4 Billion</td>
</tr>
<tr>
<td>2007</td>
<td>---</td>
<td>$43.5 Billion</td>
<td></td>
<td>$20.0 Billion</td>
<td>63.5 Billion</td>
</tr>
<tr>
<td>2006</td>
<td>---</td>
<td>$40.9 Billion</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FOOTNOTES**

1. The aggregate amount appropriated to the NIP for Fiscal Year 2013 was $52.7 billion, which was reduced by sequester to $49.0 billion.
2. The aggregate amount appropriated to the MIP for Fiscal Year 2013 was $19.2 billion, which was reduced by sequester to $16.6 billion.
3. Prior to 2007 there was no statutory requirement to publish the NIP appropriated topline figure.

**Disclosure of Appropriated Funds**

One of the recommendations of the 9/11 Commission was for the Intelligence Community to declassify its budget. This recommendation was enacted in 2007 by section 601 of the Implementing Recommendations of the 9/11 Commission Act (Public Law 110-53). This law established the requirement for the Director of National Intelligence to disclose the "aggregate amount of funds appropriated by Congress" for the NIP within 30 days of the end of the fiscal year.
Disclosure of Requested Funds

The National Intelligence Program budget request was first publicly disclosed in February 2011, pursuant to a requirement enacted by Congress in Section 364 of the Intelligence Authorization Act for Fiscal Year 2010. The Military Intelligence Program budget request was first released in February 2012.
Contents
Executive Summary ............................................................................................................. 2
Methodology ..................................................................................................................... 3
Security Clearance Volume for the Entire Federal Government ........................................ 4
  The FY 2010 IAA requires the number of individuals who held, and who were approved to
  hold, a security clearance as of October 1, 2014, to be calculated and categorized by
  personnel type – government employees, contractors, or other – and by security
  clearance level................................................................................................................ 4
Security Clearance Performance for Each Element of the IC ........................................... 7
  i. The time in days to process the shortest and longest security clearance determination
     made among 80% of security clearance determinations, and the time in days for the
     shortest and longest security clearance determination made among 90% of
     determinations ........................................................................................................ 8
  ii. The number of pending security clearance investigations for such level as of October
    1, 2014 that have remained pending for: 4 months or less; between 4 months and 8
    months; between 8 months and one year; and for more than one year ...................... 8
  iii. The percentage of reviews during the preceding fiscal year that resulted in a denial or
    revocation of a security clearance ............................................................................ 9
  iv. The percentage of investigations during the preceding fiscal year that resulted in
    incomplete information ............................................................................................ 9
  v. The percentage of investigations during the preceding fiscal year that did not result in
    enough information to make a decision on potentially adverse information ............... 9
  vi. The number of completed or pending security clearance determinations for
    government employees and contractors during the preceding fiscal year that have
    taken longer than one year to complete; the agencies that investigated and
    adjudicated such determinations; and the cause of significant delays in such
    determinations .......................................................................................................... 10
Conclusion ...................................................................................................................... 11
EXECUTIVE SUMMARY

The Intelligence Authorization Act (IAA) for Fiscal Year (FY) 2010\(^1\) requires the President to submit an annual *Report on Security Clearance Determinations* to Congress. The IAA directs this report to include the number of United States Government (USG) employees who held a security clearance at each level as of October 1 of the preceding year and the number of USG employees who were approved for a security clearance at each level during the preceding fiscal year. Similar data pertaining to USG contractors is also required. Also, for each element of the Intelligence Community (IC), in-depth security clearance timeliness determination metrics are required. In response to these IAA requirements, the Office of the Director of National Intelligence (ODNI) has prepared this *2014 Report on Security Clearance Determinations* consistent with the security clearance data requirements as outlined by the categories listed below.

<table>
<thead>
<tr>
<th>Security Clearance Volume Levels for USG Employees and USG Contractors</th>
<th>Security Clearance Determination Processing Metrics for the Seven IC Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of individuals, categorized by government employees and contractors who held and who were approved for a security clearance as of 1 October 2014; sorted by security clearance level.</td>
<td>i. The time in days to process the shortest and longest security clearance determination made among 80% of security clearance determinations, and the time in days for the shortest and longest security clearance determination made among 90% of determinations.</td>
</tr>
<tr>
<td></td>
<td>ii. The number of security clearance investigations as of October 1 of the preceding fiscal year open for:</td>
</tr>
<tr>
<td></td>
<td>o 4 months or less;</td>
</tr>
<tr>
<td></td>
<td>o 4 – 8 months;</td>
</tr>
<tr>
<td></td>
<td>o 8 – 12 months; and</td>
</tr>
<tr>
<td></td>
<td>o more than 1 year.</td>
</tr>
<tr>
<td></td>
<td>iii. Percentage of reviews during the preceding fiscal year that resulted in a denial or revocation of a security clearance.</td>
</tr>
<tr>
<td></td>
<td>iv. Percentage of investigations during the preceding fiscal year that resulted in incomplete information.</td>
</tr>
<tr>
<td></td>
<td>v. Percentage of investigations during the preceding fiscal year that did not result in enough information to make a decision on potentially adverse information.</td>
</tr>
<tr>
<td></td>
<td>vi. The number of completed or pending security clearance determinations for government employees and contractors during the preceding fiscal year that have taken longer than one year to complete; the agencies that investigated and adjudicated such determinations, and the cause of significant delays in such determinations.</td>
</tr>
</tbody>
</table>

---

\(^1\) Intelligence Authorization Act for Fiscal Year 2010, Sec. 367 Security Clearances: Reports; Reciprocity (PL 111-259).
This 2014 annual security clearance determinations report provides the current state of government security clearances. The total volume of individuals eligible for access to classified information is reported and is further broken down by the number of individuals who have been briefed and are currently “in access” as well as those eligible but currently “not in access.” In FY 2014, there were across-the-board decreases in all categories. There was also a reduction in new clearances approved. These decreases were the result of efforts across the USG to review and validate whether an employee or contractor still requires access to classified information and several additional Department of Defense (DoD) initiatives to review its cleared population.

**METHODOLOGY**

In order to report security clearance volume levels, the National Counterintelligence and Security Center’s (NCSC) Special Security Directorate (SSD) compiled and processed data from the three primary security clearance record repositories: ODNI’s Scattered Castles (SC); DoD’s Joint Personnel Adjudication System (JPAS); and the Office of Personnel Management’s (OPM) Central Verification System (CVS). To fulfill specific reporting requirements of the FY 2010 IAA, the SSD issued a special data call to the seven IC agencies with delegated authority to conduct investigations or adjudications.

SSD worked with the three clearance repository owners to minimize double-counting of duplicate records in those repositories. This was necessary because adjudicative facilities are increasingly recording their determinations in multiple repositories for reciprocity purposes. Therefore, duplicate entries may be created when different agencies grant eligibility for access to the same individual. Queries between SC and JPAS, which account for approximately 93 percent of all clearance entries, were structured to eliminate duplication where possible.

During FY 2014, SSD and OPM collaborated to set the stage for the upload of active, completed clearance records from CVS to SC. This, in addition to the current upload of records from JPAS, will enable SC to contain active security clearance records from all federal agencies in FY 2015, making metrics for reporting purposes more exact, and enabling SC users to view CVS data on the classified system. OPM continues to partner with the IC to explore cross-domain interface technology and various alternative solutions for enhanced CVS/SC information sharing for agencies that use unclassified systems.
SECURITY CLEARANCE VOLUME FOR THE ENTIRE FEDERAL GOVERNMENT

The FY 2010 IAA requires the number of individuals who held, and who were approved to hold, a security clearance as of October 1, 2014, to be calculated and categorized by personnel type – government employees, contractors, or other2 – and by security clearance level.

Table 1 provides the number of individuals in these categories for both FY 2013 and FY 2014. As in last year’s report, we show the total number of individuals “in access” (Table 1.1), those eligible, but currently “not in access” (Table 1.2), and the total number of individuals eligible to hold a security clearance (Table 1.3).

Table 1.1, Eligible (In access), refers to individuals who were investigated and adjudicated favorably and also were briefed into access to classified information. As of October 1, 2014, there were 164,501 fewer individuals “in access” than on October 1, 2013 (a 5.3 percent decrease).

Table 1.2, Eligible (Not in access), reflects that there were 471,302 fewer individuals in this category as compared to October 1, 2013 (a 22.9 percent decrease). Individuals, such as those supporting the military, may be determined eligible due to the sensitivity of their positions and the potential need for immediate access to classified information, but may not have actual access to classified information until the need arises.

Table 1.3, Total Eligibility, shows a decrease of 635,803 individuals (12.3 percent) found eligible to hold a clearance, to include those “in access,” since October 2013. Total Eligibility refers to individuals who were investigated and adjudicated favorably and had access to classified information as well as those who were favorably adjudicated but did not have access to classified information.

2 The “government” category includes all government employees and military personnel. Contractors include all industry employees, independent contractors and consultants. The “other” category includes the number of cleared government and contractor personnel reported in CVS, which does not have an employee type field, and the number of individuals in JPAS and Scattered Castles for which the employee type category field was not complete.
**Table 1**
Number of Security Clearances

### Table 1.1
Eligible (In access)

<table>
<thead>
<tr>
<th>Employee Type</th>
<th>As of 10/1/13:</th>
<th>As of 10/1/14:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Conf/Secret</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Government</td>
<td>1,204,416</td>
<td>646,527</td>
</tr>
<tr>
<td>Contractor</td>
<td>467,909</td>
<td>452,102</td>
</tr>
<tr>
<td>Other</td>
<td>144,512</td>
<td>176,511</td>
</tr>
<tr>
<td>Sub-Total</td>
<td>1,816,837</td>
<td>1,275,140</td>
</tr>
<tr>
<td>Total</td>
<td>3,091,977</td>
<td></td>
</tr>
</tbody>
</table>

### Table 1.2
Eligible (Not in access)

<table>
<thead>
<tr>
<th>Employee Type</th>
<th>As of 10/1/13:</th>
<th>As of 10/1/14:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Conf/Secret</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Government</td>
<td>1,681,690</td>
<td>205,393</td>
</tr>
<tr>
<td>Contractor</td>
<td>90,717</td>
<td>45,581</td>
</tr>
<tr>
<td>Other</td>
<td>31,347</td>
<td>3,674</td>
</tr>
<tr>
<td>Sub-Total</td>
<td>1,803,754</td>
<td>254,648</td>
</tr>
<tr>
<td>Total</td>
<td>2,058,402</td>
<td></td>
</tr>
</tbody>
</table>

### Table 1.3
Total Eligibility

<table>
<thead>
<tr>
<th>Employee Type</th>
<th>As of 10/1/13:</th>
<th>As of 10/1/14:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Conf/Secret</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Government</td>
<td>2,886,106</td>
<td>851,920</td>
</tr>
<tr>
<td>Contractor</td>
<td>558,626</td>
<td>497,683</td>
</tr>
<tr>
<td>Other</td>
<td>175,859</td>
<td>180,185</td>
</tr>
<tr>
<td>Sub-Total</td>
<td>3,620,591</td>
<td>1,529,788</td>
</tr>
<tr>
<td>Total</td>
<td>5,150,379</td>
<td></td>
</tr>
</tbody>
</table>
The USG made a concerted effort in FY 2014 to determine whether individuals eligible for access to classified information still required such access. On October 31, 2013, the Director of National Intelligence, in his role as Security Executive Agent, issued executive correspondence, "Validation of Personnel with Eligibility for Access to Classified Information." The memorandum called for department and agency heads to review and validate the need of their personnel for continued eligibility for access to classified information, consistent with Executive Order 12968, as amended. This effort resulted in a 3.1 percent reduction in the number of individuals eligible for access to classified information and accelerated several initiatives already underway to validate information in the clearance repositories.

Since the beginning of FY 2014, with the concurrence of the Under Secretary of Defense for Intelligence, the Defense Manpower Data Center has implemented several data quality initiatives (DQI) which resulted in reductions to the eligible population across the DoD; particularly in the “not in access” category. DQIs were developed to improve the data quality within JPAS and ensure that personnel security policies are consistently enforced in JPAS through the implementation of scripts and data analysis. Most significant were DQIs 597, 689, and 690.

- DQI 597 administratively debriefs access in JPAS for subjects whose eligibility does not support the current access. This includes subjects who have separated from the military or who are deceased, and/or records for which there is no owning or servicing security management office (SMO). This DQI occurs on a monthly basis and mainly impacted the reduction of the eligible “in access” population.

- DQI 689 administratively modified military or civilian categories where the subjects did not have any owning or servicing SMO and where there had been no activity on the person, or the person had not been briefed into access within the past 24 months. Military or civilian subjects who had no other active categories were administratively withdrawn which resulted in an approximate 440,000 reduction.

- DQI 690 downgraded military members in the Individual Ready Reserve (IRR)/Standby Reserve (SR) category to be downgraded to “Favorable” if there were no other active person categories (e.g. industry), no owning or servicing SMO, and no other activity on record for the past 24 months. “Favorable” status allows the quick recall of that population should the mission warrant it. This resulted in an approximate 25,000 reduction. This initiative additionally benefitted the services by assigning an owning SMO to approximately 67,000 other IRR/SR records.
Table 2, *Number of Security Clearance Approvals*, presents the number of individuals approved for a security clearance by clearance level. Variations in data collection fields in the repositories limit the ability to collect precise data. For instance, a query of the security clearance determination *approvals* recorded in some repositories cannot distinguish between initial clearance and periodic reinvestigation approvals. Therefore, the number of approvals does not represent the number of new clearances granted, but rather a combination of approvals for initial clearances and for reinvestigations of existing clearances. Within this category, however, there has been a 14.4 percent reduction in the number of security clearances approved as compared to FY 2013.

<table>
<thead>
<tr>
<th>Employee Type</th>
<th>In FY 2013:</th>
<th>In FY 2014:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Conf/Secret</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Government</td>
<td>369,245</td>
<td>152,490</td>
</tr>
<tr>
<td>Contractor</td>
<td>82,875</td>
<td>131,209</td>
</tr>
<tr>
<td>Other</td>
<td>28,564</td>
<td>12,785</td>
</tr>
<tr>
<td>Sub-Total</td>
<td>480,684</td>
<td>296,484</td>
</tr>
<tr>
<td>Total</td>
<td>777,168</td>
<td></td>
</tr>
</tbody>
</table>

**Security Clearances Performance for Each Element of the IC**

To collect information responsive to FY 2010 IAA requirements set forth in items “i” through “vi” below, the ODNI issued a special data call to seven IC agencies with delegated authority to conduct investigations or adjudications: Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Federal Bureau of Investigation (FBI), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and the Department of State (State). The results follow.\(^4\)

---

3 CIA also processes security clearances for ODNI employees and contractors.
4 FBI and Department of State provided data for their entire cleared population which has been included. Data from other agencies that have IC elements (DHS, DoE, DEA, and Departments of the Treasury, Army, Navy, Marine Corps, Coast Guard, and Air Force) was not requested and is not included since these agencies are unable to extract data on clearance actions for individuals assigned to IC positions without a manual review of files.
i. The time in days to process the shortest and longest security clearance determination made among 80% of security clearance determinations, and the time in days for the shortest and longest security clearance determination made among 90% of determinations

Table 3, *Processing Timeliness*, provides the total number of days required to process the shortest and longest security clearance cases—from initiation to adjudicative decision—for the fastest 80 percent of cases and for the fastest 90 percent of cases.

<table>
<thead>
<tr>
<th>Agency</th>
<th>80th Percentile</th>
<th></th>
<th></th>
<th>90th Percentile</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TS</td>
<td>Secret/Confidential</td>
<td></td>
<td>TS</td>
<td>Secret/Confidential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Longest</td>
<td>Shortest</td>
<td>Longest</td>
<td>Shortest</td>
<td>Longest</td>
<td>Shortest</td>
</tr>
<tr>
<td>CIA</td>
<td>265</td>
<td>1</td>
<td>151</td>
<td>1</td>
<td>414</td>
<td>1</td>
</tr>
<tr>
<td>DIA</td>
<td>334</td>
<td>28</td>
<td>DNP</td>
<td>DNP</td>
<td>387</td>
<td>28</td>
</tr>
<tr>
<td>FBI</td>
<td>125</td>
<td>1</td>
<td>180</td>
<td>7</td>
<td>164</td>
<td>1</td>
</tr>
<tr>
<td>NGA</td>
<td>198</td>
<td>39</td>
<td>DNP</td>
<td>DNP</td>
<td>313</td>
<td>39</td>
</tr>
<tr>
<td>NRO</td>
<td>262</td>
<td>13</td>
<td>254</td>
<td>94</td>
<td>316</td>
<td>13</td>
</tr>
<tr>
<td>NSA</td>
<td>214</td>
<td>13</td>
<td>DNP</td>
<td>DNP</td>
<td>316</td>
<td>13</td>
</tr>
<tr>
<td>State</td>
<td>169</td>
<td>2</td>
<td>121</td>
<td>8</td>
<td>238</td>
<td>2</td>
</tr>
</tbody>
</table>

DNP = Does Not Perform

ii. The number of pending security clearance investigations for such level as of October 1, 2014 that have remained pending for: 4 months or less; between 4 months and 8 months; between 8 months and one year; and for more than one year

Table 4, *Age Pending*, provides the number of pending security clearance investigations by length of time and by agency.

<table>
<thead>
<tr>
<th>Agency</th>
<th>Top Secret Initial Security Clearance Investigations</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 to 4 Months</td>
<td>4 to 8 Months</td>
<td>8 to 12 Months</td>
</tr>
<tr>
<td>CIA</td>
<td>408</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>DIA</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FBI</td>
<td>1,362</td>
<td>332</td>
<td>14</td>
</tr>
<tr>
<td>NGA</td>
<td>18</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>NRO</td>
<td>185</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NSA</td>
<td>430</td>
<td>312</td>
<td>187</td>
</tr>
<tr>
<td>State</td>
<td>479</td>
<td>157</td>
<td>18</td>
</tr>
</tbody>
</table>

The IC reported that the focus on periodic reinvestigations and potential insider threat cases during FY 2014 caused resources to be reprioritized. Going forward, this may cause an increase in the number of initial cases pending for more than 4 months.
iii. The percentage of reviews during the preceding fiscal year that resulted in a denial or revocation of a security clearance

Table 5, *Denials and Revocations*, reflects the percentage of denials (resulting from adjudications of initial cases) and revocations (resulting from adjudications of periodic reinvestigations) in FY 2014. Revocations based solely on adverse reporting not requiring an investigation are not included. This situation might arise where information comes to light that is so damaging, timely revocation of a security clearance is prudent and necessary.

<table>
<thead>
<tr>
<th>Agency</th>
<th>FY 2014 Denials</th>
<th>FY 2014 Revocations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIA</td>
<td>6.5%</td>
<td>0.6%</td>
</tr>
<tr>
<td>DIA</td>
<td>0.5%</td>
<td>0.1%</td>
</tr>
<tr>
<td>FBI</td>
<td>0.1%</td>
<td>0.3%</td>
</tr>
<tr>
<td>NGA</td>
<td>3.9%</td>
<td>2.2%</td>
</tr>
<tr>
<td>NRO</td>
<td>7.4%</td>
<td>1.6%</td>
</tr>
<tr>
<td>NSA</td>
<td>9.2%</td>
<td>0.1%</td>
</tr>
<tr>
<td>State</td>
<td>0.3%</td>
<td>0.2%</td>
</tr>
</tbody>
</table>

The difference in the percentage of denials and revocations among agencies can be attributed to different processes employed by those agencies. For example, FBI and State may discontinue security processing due to automatic disqualifiers found during a suitability review before the case reaches the security clearance adjudication phase. These cases are cancelled by Human Resources before security clearance determinations are rendered and are not, therefore, categorized as security clearance denials. Other IC elements consider all relevant information in their security clearance adjudicative process. They render security clearance denials based upon the totality of the information contained in the case files, which results in a higher percentage of denials.

iv. The percentage of investigations during the preceding fiscal year that resulted in incomplete information

Agencies confirmed that their final reports of investigation contained all required/relevant information prior to adjudication.

v. The percentage of investigations during the preceding fiscal year that did not result in enough information to make a decision on potentially adverse information

The seven IC agencies listed on Table 5 reported that they had no cases to report against this category. Agencies worked to ensure that sufficient information was available to make a decision on any potentially adverse information.
vi. The number of completed or pending security clearance determinations for government employees and contractors during the preceding fiscal year that have taken longer than one year to complete; the agencies that investigated and adjudicated such determinations; and the cause of significant delays in such determinations

Table 6, *Delays More Than 1 Year*, shows the number of security clearance determinations for **USG employees** that required more than a year to complete.

Table 7, *Delays More Than 1 Year*, shows the number of security clearance determinations for **contractors** that required more than a year to complete.

<table>
<thead>
<tr>
<th>Agency</th>
<th>Government Cases Over 1 Year</th>
<th>Contractor Cases Over 1 Year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Pending</td>
<td>Completed</td>
</tr>
<tr>
<td>CIA</td>
<td>106</td>
<td>139</td>
</tr>
<tr>
<td>DIA</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>FBI</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>NGA</td>
<td>34</td>
<td>45</td>
</tr>
<tr>
<td>NRO</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>NSA</td>
<td>102</td>
<td>10</td>
</tr>
<tr>
<td>State</td>
<td>39</td>
<td>44</td>
</tr>
</tbody>
</table>

Some DoD IC agencies only have delegated investigative authority over their civilian employee population and therefore, can only report the overall timeliness for that population. These agencies only conduct adjudications of contractors who already have a Top Secret clearance for access to sensitive compartmented information.

Table 8, *Causes of Significant Delays*, contains detailed information for cases pending more than one year. Some agencies cannot report detailed information, either for their entire population—due to the technical limitations of their current database of record—or for their contractor population for the reasons cited in the previous section.
Table 8
Causes of Significant Delays

<table>
<thead>
<tr>
<th>Agency</th>
<th>Volume</th>
<th>Delays:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Government</td>
<td>Contractor</td>
</tr>
<tr>
<td>ASP &amp; ISP</td>
<td>245</td>
<td>961</td>
</tr>
<tr>
<td>CIA</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>DIA</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>NGA</td>
<td>79</td>
<td>0</td>
</tr>
<tr>
<td>NRO</td>
<td>1</td>
<td>170</td>
</tr>
<tr>
<td>NSA</td>
<td>112</td>
<td>512</td>
</tr>
<tr>
<td>State</td>
<td>83</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Significant Adjudicative Events</th>
<th>Unable to provide at this time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreign Influence</td>
<td>5</td>
</tr>
<tr>
<td>Foreign Preference</td>
<td>24</td>
</tr>
<tr>
<td>Foreign Access</td>
<td>60</td>
</tr>
<tr>
<td>Financial Considerations</td>
<td>80</td>
</tr>
<tr>
<td>Alcohol Consumption</td>
<td>326</td>
</tr>
<tr>
<td>Drug Use/Abuse</td>
<td>57</td>
</tr>
</tbody>
</table>

* Other: Includes delays involving high risk cases, derogatory information, protected information, and polygraph or medical issues.

For agencies that can report detailed information, “multiple issues” was cited as the cause for significant delay in 552 or 55 percent of cases. Among those multiple issues cited, “foreign influence” was reported as the most common single reason for delay and “financial considerations” was the second most common reason for delay overall.

**CONCLUSION**

In FY 2014, the number of individuals eligible for a security clearance declined across both the “in access” and “not in access” populations. The majority of the decreases resulted from DoD’s successful implementation of DQIs that have positively impacted areas of data quality, data integrity, and overall system security and availability. The benefits include improved data synchronization and consistency with the Defense Enrollment Eligibility Reporting System, DoD Personnel Center databases, and CVS. In addition, the IC reported a 1.3 percent reduction and the rest of the USG reported a 1.5 percent reduction in their eligible populations. This suggests the validation effort subsequent to the DNI’s issuance of executive correspondence “Validation of Personnel with Eligibility for Access to Classified Information,” October 31, 2013, was effective. Overall, the USG reported a 3.1% reduction in the total eligible population attributed to this effort.

The IC continues to face timeliness challenges in clearing individuals with unique or critical skills—such as highly desirable language abilities—who often have significant foreign associations that may take additional time to investigate and adjudicate. The ODNI, in partnership with OMB, OPM, and DoD, continues to drive improvements in the timeliness, accuracy and consistency of investigative and adjudicative clearance processes government-wide.
Office of the Director of National Intelligence

Statistical Transparency Report Regarding use of National Security Authorities

Annual Statistics for Calendar Year 2013
Statistical Transparency Report Regarding use of National Security Authorities

June 26, 2014

Introduction.

In June 2013, President Obama directed the Intelligence Community to declassify and make public as much information as possible about certain sensitive U.S. Government surveillance programs while protecting sensitive classified intelligence and national security information. Over the past year, the Director of National Intelligence (DNI) has declassified and authorized the public release of thousands of pages of documents relating to the use of critical national security authorities. Today, and consistent with the DNI's directive on August 29, 2013, we are releasing information related to the use of these important tools, and will do so in the future on an annual basis. Accordingly, the DNI has declassified and directed the release of the following information for calendar year 2013.

Annual Statistics for Calendar Year 2013 Regarding Use of Certain National Security Legal Authorities.

Titles I, III, IV, and VII of FISA.

<table>
<thead>
<tr>
<th>Legal Authority</th>
<th>Annual Number of Orders</th>
<th>Estimated Number of Targets Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISA Orders based on probable cause (Title I and III of FISA, Sections 703 and 704 of FISA)</td>
<td>1,767 orders</td>
<td>1,144</td>
</tr>
<tr>
<td>Section 702 of FISA</td>
<td>1 order</td>
<td>89,138</td>
</tr>
<tr>
<td>FISA Pen Register/Trap and Trace (Title IV of FISA)</td>
<td>131 orders</td>
<td>319</td>
</tr>
</tbody>
</table>

It is important to provide some additional context to the above statistics.

- **Targets.** Within the Intelligence Community, the term “target” has multiple meanings. For example, “target” could be an individual person, a group, or an organization composed of multiple individuals or a foreign power that possesses or is likely to communicate foreign intelligence information that the U.S. government is authorized to acquire by the above-referenced laws. Some laws require that the government obtain a Court order specifying the communications facilities used by a “target” to be subject to intelligence collection. Although the government may have legal authority to conduct intelligence collection against multiple communications facilities used by the target, the user of the facilities - the “target” - is only counted once in the above figures.
• **702 Targets.** In addition to the explanation of target above, in the context of Section 702 the term “target” is generally used to refer to the act of intentionally directing intelligence collection at a particular person, a group, or organization. For example, the statutory provisions of Section 702 state that the Government “may not intentionally target any person known at the time of the acquisition to be located in the United States” (emphasis added), among other express limitations. Under Section 702, the Foreign Intelligence Surveillance Court (FISC) approves Certifications as opposed to individualized orders. Thus, the number of 702 “targets” reflects an estimate of the number of known users of particular facilities (sometimes referred to as selectors) subject to intelligence collection under those Certifications. This estimate is based on the information readily available to the Intelligence Community to identify unique targets – users, whose identity may be unknown, but who are reasonably believed to use the particular facility from outside the United States and who are reasonably believed to be non-United States persons. For example, foreign intelligence targets often communicate using several different email accounts. Unless the Intelligence Community has information that multiple email accounts are used by the same target, each of those accounts would be counted separately in these figures. On the other hand, if the Intelligence Community is aware that the accounts are all used by the same target, as defined above, they would be counted as one target.

• **Relationship of Orders to Targets.** In some cases, one order can by its terms affect multiple targets (as with Section 702). Alternatively, a target may be the subject of multiple orders, as noted below.

• **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. To avoid redundant counting, these statistics do not count such amendments separately. Moreover, some orders may be renewed multiple times during the calendar year (for example, the FISA statute provides that a Section 704 FISA Order against a U.S. person target may last no longer than 90 days but permits the order to be renewed). The statistics count each such renewal as a separate order.

**Title V of FISA (Business Records).**

We are reporting information about the Government’s use of the FISA Business Records provision (Title V) separately because this authority has been used in two distinct ways – collection of business records to obtain information about a specific subject and collection of business records in bulk. Accordingly, in the interest of transparency, we have decided to clarify the extent to which individuals are affected by each use. In addition, instead of reporting on the number of Business Record orders, the government is reporting on the number of applications submitted to the Foreign Intelligence Surveillance Court because the FISC may issue several orders to different recipients based upon a particular application.
<table>
<thead>
<tr>
<th>Legal Authority</th>
<th>Annual Number of Applications</th>
<th>Estimated Number Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISA Business Records (Title V of FISA)</td>
<td>178</td>
<td>172: The number of individuals, entities, or foreign powers subject to a business records application to obtain information about a specific subject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>423: The number of selectors approved to be queried under the NSA telephony metadata program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>248: The number of known or presumed U.S. persons who were the subject of queries of information collected in bulk or who were subject to a business records application.</td>
</tr>
</tbody>
</table>

**National Security Letters.**

Finally, we are reporting information on the Government’s use of National Security Letters (NSLs). On April 30, 2014, the Department of Justice released its Annual Foreign Intelligence Surveillance Act Report to Congress. That report, which is available here reports on the number of requests made for certain information concerning different United States persons pursuant to NSL authorities during calendar year 2013. In addition to those figures, today we are reporting (1) the total number of NSLs issued for all persons, and (2) the total number of requests for information contained within those NSLs. For example, one NSL seeking subscriber information from one provider may identify three e-mail addresses, all of which are relevant to the same pending investigation and each is considered a “request.”

We are reporting the annual number of requests rather than “targets” for multiple reasons. First, the FBI’s systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases this occurs because individual
subscribers may identify themselves differently for each account, e.g., inclusion of middle name, middle initial, etc., when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities, e.g., multiple e-mail accounts, landline telephone numbers, cellular phone numbers, etc. The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

<table>
<thead>
<tr>
<th>Legal Authority</th>
<th>Annual Number of NSLs Issued</th>
<th>Annual Number of Requests for Information</th>
</tr>
</thead>
</table>

This information will be available at the website of the Office of the Director of National Intelligence (ODNI); and ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the Government, IContheRecord.tumblr.com.
Office of the Director of National Intelligence

LEADERSHIP

Director (DNI)
Principal Deputy Director (PDDNI)
Chief Management Officer (CMO)

CORE MISSION

Deputy DNI for Intelligence Integration (DDNI/II)

Mission Integration Division (MID)
National Counterproliferation Center (NCPC)
National Intelligence Council (NIC)
National Counterterrorism Center (NCTC)
National Intelligence Management Council (NIMC)
National Counterintelligence & Security Center (NCSC)

ENABLERS

Acquisition, Technology, & Facilities (AT&F)
Partner Engagement (PE)
Chief Financial Officer (CFO)
Policy & Strategy (P&S)
Chief Human Capital Officer (CHCO)
Systems & Resource Analyses (SRA)
IC Chief Information Officer (IC CIO)
Information Sharing Environment (ISE)

OVERSIGHT

Civil Liberties and Privacy Office (CLPO)
Office of the General Counsel (OGC)
IC Equal Employment Opportunity & Diversity (EEOD)
Office of Legislative Affairs (OLA)
IC Inspector General (IC IG)
Public Affairs Office (PAO)
The Financial Times published the following op-ed by ODNI General Counsel Robert Litt today in its online edition.

Financial Times - The ECJ has its facts wrong about Prism

October 5, 2015

Robert Litt

Last month an advocate-general of the European Court of Justice issued an opinion in a case of exceptional significance for commercial relations between the US and the EU. Washington, which is not a party to the proceedings, has no opportunity to make a direct submission to the court. We respect the EU’s legal process. However, the advocate-general’s judgment contains a number of inaccuracies — and before the court makes a final decision we want to set the record straight.

The case concerns the “safe harbour” rules that allow companies with operations in Europe to transfer personal data to servers in the US. This framework, in operation since 2000, is based on a finding by the European Commission that it provides adequate privacy protection under EU law. More than 4,400 companies rely on it to transfer data necessary to support transatlantic trade, the digital economy and jobs in both the EU and the US. The lawsuit was brought in Ireland. It is based on press reports concerning a US foreign intelligence programme called Prism, which, the complaint says, allows “unrestricted access to mass data stored on servers in the United States”.

The Irish High Court adopted this characterisation, as did the advocate-general, who said: “The evidence now available would admit of no other realistic conclusion.”

Actually, the available evidence demonstrates the contrary.

Since press reports about this programme began surfacing in 2013, President Barack Obama has ordered extensive public disclosures about it. Court documents have been released and two independent bodies have released reports examining US surveillance practices. These sources, which are publicly available, accurately describe the Prism programme, which is another name for foreign intelligence collection subject to judicial supervision under section 702 of the Foreign Intelligence Surveillance Act.

Prism “is not based on the indiscriminate collection of information in bulk”, as a report from the US Privacy and Civil Liberties Oversight Board makes clear. This body, an independent, bipartisan agency within the executive branch, has stated that the programme “consists entirely of targeting specific persons about whom an individualised determination has been made”. It can be used only to collect communications for an approved foreign intelligence purpose, such as combating terrorism or weapons proliferation, and the court must approve procedures that ensure that targets are appropriately chosen.

The programme does not give the US “unrestricted access” to data. Rather, the US may obtain communications only relating to specific identifiers, such as an email address or telephone number; only if the US believes those identifiers are being used to communicate foreign intelligence information; and only with the legally compelled assistance of communications service providers under the supervision of an independent court.
Even when the US does intercept communications of ordinary people — because, for example, those people are communicating with valid foreign intelligence targets — strict procedures limit how long they can be retained and how they can be disseminated.

Last year there were 90,000 targets of surveillance under Section 702. That may sound a lot, but it is a tiny proportion of the 3.2bn people who use the internet worldwide.

This programme helps protect Americans as well as our partners and allies. But it can be used only when authorised by law, in a manner that protects the privacy of all persons, and with extensive oversight from all three branches of our government.

The US legal framework for intelligence collection includes robust protection for privacy under multiple layers of oversight and a remarkable degree of transparency.

The decisions of judicial bodies should be informed by accurate information. Prism is focused and reasonable. It does not involve "mass" and "unrestricted" collection of data, as the advocate-general says.

* #ODNI
  * #NSA
  * #RobertLitt
  * #Prism
  * #PCLOB
  * #privacy
  * 4 days ago
  * 5
  * Permalink

Share

Short URL

http://tmb.fr/ZZQysq1t

Twitter
Facebook
Pinterest
Google+

DECLASSIFIED

View Separately

Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Documents Related to Section 702 of the Foreign Intelligence Surveillance Act

September 29, 2015

The Executive Branch has publicly released various documents related to Section 702 of the Foreign Intelligence Surveillance Act, with appropriate redactions to protect national security information. These documents are available at the website of the Office of the Director of National Intelligence and ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the U.S. Government. IC on the Record.

Section 702

Section 702 was enacted as part of the FISA Amendments Act of 2008. Section 702 authorizes the targeting of non-U.S. persons reasonably believed to be outside the United States to acquire foreign intelligence information. This collection authority is one of the most significant tools in the Intelligence Community’s arsenal for the detection, identification, and disruption of terrorist threats to the United States and around the world.

Section 702 incorporates substantial protections to ensure that the surveillance activities conducted pursuant to it are properly targeted and that the retention and use of the collected information is appropriately limited. And, as noted in the Intelligence Community’s January 2015 Signals Intelligence Reform Report, the Intelligence Community is taking steps to further strengthen these protections.

Section 702 Certifications

http://iconghererecord.tumblr.com/
Included in this release is a redacted copy of a complete Section 702 certification filing from 2014. Certifications like this one are the key documents governing the Intelligence Community’s surveillance activities under Section 702.

Section 702 permits the Attorney General and the Director of National Intelligence (DNI) to approve annual certifications authorizing the Intelligence Community to target non-U.S. persons reasonable believed to be located outside of the United States to acquire certain categories of foreign intelligence information. Each certification is supported, as appropriate, by affidavits of appropriate national security officials attesting to how the Intelligence Community will conduct the proposed surveillance.

Under Section 702, instead of identifying in the certification the specific individuals or communication facilities (e.g., telephone numbers) to be targeted, the Attorney General and the DNI adopt targeting procedures that explain in significant detail how the Intelligence Community will ensure that the proposed surveillance will be limited to targeting non-U.S. persons reasonable believed to be located outside the United States for the purpose of acquiring foreign intelligence information discussed in the certification and accompanying affidavits. Because these targeting procedures explain in depth how the Intelligence Community decides whether to target a person, the specifics of these targeting procedures are classified.

The certification package also contains minimization procedures, which explain in similar detail how the Intelligence Community limits its acquisition, retention, and dissemination of the information collected under Section 702. The Executive Branch has declassified significant portions of these minimizations procedures and they are available below.

---

DNI-AG 702(g) Certification

Government’s Ex Parte Submission of Reauthorization Certifications

Affidavit of Acting Director NSA

Affidavit of Director FBI

Affidavit of Director CIA

Certification Exhibit F *

FBI Section 702 Targeting Procedures *

NSA Section 702 Targeting Procedures *

Letter to Judge Walton 18 March 2014

Letter to Judge Hogan 29 May 2014

Letter to Judge Hogan 25 July 2014

Letter to Judge Hogan 30 July 2014

2014 NSA Section 702 Minimization Procedures

2014 FBI Section 702 Minimization Procedures

2014 CIA Section 702 Minimization Procedures

2014 NCTC Section 702 Minimization Procedures

* Because these targeting procedures, as well as an associated list of foreign powers subject to targeting under this certification (Exhibit F), explain in depth how the Intelligence Community decides whether to target a person, the content of these documents remains classified except for the document titles.

---

Section 702 Certification FISC Opinion

Under Section 702, the Attorney General and the DNI must submit each Section 702 certification for a thorough review and approval by the Foreign Intelligence Surveillance Court (FISC). In deciding whether to approve a certification, the FISC must assess whether the Intelligence Community’s targeting procedures “are reasonably designed” to “ensure” that an authorized acquisition is “limited to targeting persons reasonably believed to be located outside the United States,” and to prevent the intentional acquisition of wholly domestic communications.

The FISC must also determine that the Intelligence Community’s minimization procedures are “specific” and that they are “reasonably designed” to appropriately limit the acquisition, retention, and dissemination of any non-publicly available
U.S. person information that may be collected consistent with the needs of the United States to obtain, produce, and disseminate foreign intelligence information. Additionally, each time the Government submits a Section 702 certification, the FISC must determine that the proposed surveillance complies with the Fourth Amendment.

Section 702 requires that the FISC issue a written opinion explaining its approval or disapproval of a certification. The Executive Branch is releasing a redacted copy of the FISC opinion associated with the 2014 certification package described above. In its opinion, the FISC reviewed the certification being released today, as well as the Government's implementation of Section 702 over the prior year. The FISC held that the proposed certification complied with all statutory requirements and was consistent with the Fourth Amendment. The FISC also imposed several additional reporting requirements to facilitate its ongoing oversight of the Government's implementation of Section 702.

FISC Memorandum Opinion and Order 26 August 2014

* 1 week ago
* 3
  * Permalink

Share

Short URL
http://tmblr.co/2ZQjsq1Vc

Twitter Facebook Pinterest Google+

DECLASSIFIED

View Separately

Newly Declassified Documents

September 29, 2015

Today we've added a newly declassified document to a prior post:

Release of Documents Concerning Activities under the Foreign Intelligence Surveillance Act - Published March 3, 2015

From time to time we are able to update older posts on IC on the Record with newly declassified information. When we do so, we always note the addition in the original post (in this case, marked as "added September 29, 2015") as well as create a new blog entry to direct you to the freshly released information.

* #declassified
  * #NGC
  * #minimization_procedures
* 1 week ago
* 1
  * Permalink

Share

Short URL
http://tmblr.co/2ZQjsq1Vc

Twitter Facebook Pinterest Google+

DECLASSIFIED

View Separately

The Department of Justice Releases Additional Information from Inspectors General Reports Concerning Collection Activities Authorized by President George W. Bush After the Attacks of September 11, 2001

September 21, 2015
The Department of Justice has released additional information contained within Inspectors General reports on the President's Surveillance Program (PSP). The additional information concerns the presidential documents that authorized the inception and implementation of the program.

The release today supplements the IC on the Record posting of April 25, 2015, wherein the ODNI posted statutorily mandated, detailed reviews of the PSP by the Inspectors General of five different agencies—DoJ, DoD, NSA, the Central Intelligence Agency, and ODNI—as well as a joint report signed by the IGs of each of those agencies.

Today's posting was made in response to requests made by the Department of Justice Inspector General to the Department of Justice and the Office of the Director of National Intelligence, and in response to requests made under the Freedom of Information Act.

Volume I

PSP Vol IA | PSP Vol IB | PSP Vol IC

Volume II

PSP Vol IIA | PSP Vol IIB | PSP Vol IIC | PSP Vol IID | PSP Vol IIE |

PSP Vol IIF | PSP Vol IIG

Volume III

PSP Vol IIIA | PSP Vol IIIB | PSP Vol IIIC | PSP Vol IIID | PSP Vol IIIE |


- 2 weeks ago
- 3
- PermLink

Share

Short URL
http://tmbrr.co/ZZQjoq1us

TwitterFacebookPinterestGoogle+

View Separately

Joint Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of the Renewal of Collection Under Section 215 of the USA PATRIOT Act (50 U.S.C. Sec. 1861), as amended by the USA FREEDOM Act

August 28, 2015

On August 27, 2015, the Foreign Intelligence Surveillance Court issued a Primary Order approving the government’s application to renew the Section 215 bulk telephony program. The USA FREEDOM Act of 2015 banned bulk collection under Section 215 of the USA PATRIOT Act, but provided a new mechanism to allow the government to obtain data held by the providers. To ensure an orderly transition to this new mechanism, the USA FREEDOM Act provided for a 180-day transition period during which the existing NSA bulk telephony metadata program may continue.

After considering an application filed shortly after the passage of the USA FREEDOM Act, on June 29, 2015, the Court held that the continuation of the NSA’s bulk telephony metadata program during the transition period remains consistent with both the statute and the Fourth Amendment. The authority under the Court’s June 29 order was set to expire today, August 28, 2015.

The Government recently filed an application to renew the authority to collect bulk telephony metadata. On August 27, 2015, the Court authorized the continued collection of telephony metadata through November 28, 2015, the end of the 180-day transition period contemplated by the USA FREEDOM Act. As of November 29, 2015, both the 180-day transition...
period and the Court’s authorization will have expired and the bulk collection of telephony metadata pursuant to Section 215 will cease.

As previously stated in a July 27, 2013 Joint Statement, NSA has determined that analytic access to the historical metadata collected under Section 215 (any data collected before November 29, 2015) will also cease on November 29, 2015. However, solely for data integrity purposes to verify the records produced under the now targeted production mechanism authorized by the USA FREEDOM Act, NSA, subject to court approval, plans to allow technical personnel to continue to have access to the historical metadata for an additional three months.

Separately, NSA remains under a continuing legal obligation to preserve its bulk 215 telephony metadata collection until civil litigation regarding the program is resolved, or the relevant courts relieve NSA of such obligations. The telephony metadata preserved solely because of preservation obligations in pending civil litigation will not be used or accessed for any other purpose, and, as soon as possible, NSA will destroy the Section 215 bulk telephony metadata upon expiration of its litigation preservation obligations.

As background, early last year in a speech at the Department of Justice, President Obama announced that the Intelligence Community would end the Section 215 bulk telephony metadata program as it previously existed. The President directed the Intelligence Community and the Attorney General to develop options for a new approach to match the capabilities and fill gaps that the Section 215 program was designed to address without the government holding this metadata.

After carefully considering the available options, the President announced in March 2014 that the government should not hold this data in bulk, and that the data should remain at the telephone companies with a legal mechanism in place that would allow the government to obtain data pursuant to individual orders from the FISC approving the use of specific numbers for such queries.

The President also noted, however, that legislation would be required to implement this new approach and the administration worked closely with Congress to enact the President’s proposal. On June 2, 2015, Congress passed and the President signed the USA FREEDOM Act of 2015, which reauthorized several important national security authorities; banned bulk collection under Section 215 of the USA PATRIOT Act; under the pen register and trap and trace provisions found in Title IV of FISA, and pursuant to National Security Letters; and adopted the new legal mechanism proposed by the President.

As in past primary orders in effect since February 2014, and consistent with the President’s direction, the Court’s new Primary Order requires that during the transition period, absent a true emergency, telephony metadata can only be queried after a judicial finding that there is a reasonable, articulable suspicion that the selection term is associated with an approved international terrorist organization. In addition, the query results must be limited to metadata within two hops of the selection term instead of three.

The new Primary Order is available here.
Statement by the ODNI on Retention of Data Collected Under Section 215 of the USA PATRIOT Act

July 27, 2015

On June 29, 2015, the Foreign Intelligence Surveillance Court approved the Government’s application to resume the Section 215 bulk telephony metadata program pursuant to the USA FREEDOM Act’s 180-day transition provision. As part of our effort to transition to the new authority, we have evaluated whether NSA should maintain access to the historical metadata after the conclusion of that 180-day period.

NSA has determined that analytic access to that historical metadata collected under Section 215 (any data collected before November 29, 2015) will cease on November 29, 2015. However, solely for data integrity purposes to verify the records produced under the new targeted production authorized by the USA FREEDOM Act, NSA will allow technical personnel to continue to have access to the historical metadata for an additional three months.

Separately, NSA remains under a continuing legal obligation to preserve its bulk 215 telephony metadata collection until civil litigation regarding the program is resolved, or the relevant courts relieve NSA of such obligations. The telephony metadata preserved solely because of preservation obligations in pending civil litigation will not be used or accessed for any other purpose, and, as soon as possible, NSA will destroy the Section 215 bulk telephony metadata upon expiration of its litigation preservation obligations.

The Office of the Director of National Intelligence is one of seven federal agencies participating in a pilot program to make records requested via the Freedom of Information Act more readily available to the public:

"...the Department of Justice is pleased to announce the launch of a new pilot program at seven agencies designed to test the feasibility of posting online FOIA responses so that they are available not just to the individual requester, but to the general public as well."

During the pilot, we seek to answer many important questions, including: costs associated with such a policy, effect on staff time required to process requests, effect on interactions with government...
stakeholders, and the justification for exceptions to such a policy, such as for personal privacy. For privacy reasons, participating agencies will not post online responses to requests in which individuals seek access to information about themselves.

The agencies participating in the pilot are the Office of the Director of National Intelligence, the Millennium Challenge Corporation, the Environmental Protection Agency, and components or offices of the Departments of Defense, Homeland Security and Justice, and the National Archives and Records Administration, with OIP leading the effort.

The results of this six-month pilot program will be made available to the public, and we intend to be transparent about the pilots and their implementation by participating agencies. We also invite the public’s feedback as we explore this proposed policy shift, and welcome innovative ideas and suggestions for overcoming the implementation challenges.

Read the full “Proactive Disclosure” press release at DOJ.gov.

* #FOIA
* #Transparency
* #OpenGov
* #Open Government
* 2.months age > odnigov
* 27
* Permalink

Short URL
http://tmb.ly/0ZOlq1of

Twitter Facebook Pinterest Google+

View Separately

Joint Statement by the DOJ and the ODNI on the Declassification of the Resumption of Collection Under Section 215 of the USA Patriot Act

June 30, 2015

Yesterday, the Foreign Intelligence Surveillance Court [FISC] issued an opinion and primary order approving the government’s application to renew the Section 215 bulk telephony program. The USA FREEDOM Act of 2015 banned bulk collection under Section 215 of the USA PATRIOT Act, but provided a new mechanism to allow the government to obtain data held by the providers.

To ensure an orderly transition to this new mechanism, the USA FREEDOM Act provides for a 180-day transition period during which the existing National Security Agency (NSA) bulk telephony metadata program may continue. After considering the views of amici, the court held that the continuation of the NSA’s bulk telephony metadata program during the transition period remains consistent with both the statute and the Fourth Amendment.

As background, early last year in a speech at the Department of Justice, President Obama announced a transition that would end the Section 215 bulk telephony metadata program as it previously existed. The president directed the intelligence community and the Attorney General to develop options for a new approach to match the capabilities and fill gaps that the Section 215 program was designed to address without the government holding this metadata.

After carefully considering the available options, the president announced in March 2014 that the best path forward is that the government should not hold this data in bulk, and that the data should remain at the telephone companies with a legal mechanism in place that would allow the government to obtain data pursuant to individual orders from the FISC approving the use of specific numbers for such queries.

President Obama also noted that legislation would be required to implement this option and he called on Congress to enact this important change. The administration subsequently worked closely with members of Congress to enact the president’s proposal. On June 2, 2015, Congress passed and President Obama signed the USA FREEDOM Act of 2015, which reauthorized several important national security authorities; banned bulk collection under Section 215 of the USA PATRIOT Act; under the pen register and trap and trace provisions found in Title IV of FISA, and pursuant to National Security Letters; and adopted the new legal mechanism proposed by the president.
As in past primary orders in effect since February 2014, and consistent with the president's direction, the court's new primary order requires that during the transition period, absent true emergency, telephony metadata can only be queried after a judicial finding that there is a reasonable, articulable suspicion that the selection term is associated with an approved international terrorist organization. In addition, the query results must be limited to metadata within two hops of the selection term instead of three.

In addition to the release of the court's opinion, the administration is undertaking a declassification review of this most recent primary order, and when complete, the Office of the Director of National Intelligence will post the document to its website and icontherecord.tumblr.com.

- #NSA
- #ODNI
- #FISA
- #USA FREEDOM ACT
- #Declassified
- 3 months ago
- S
- Permalink

Share

Short URL  
http://tumblr.co/ZZ0j0x10v

Twitter|Facebook|Pinterest|Google+

DECLASSIFIED

View Separately

CIA Releases Declassified Documents Related to 9/11 Attacks

June 12, 2015


The first of these documents is a redacted version of the 2005 CIA Office of Inspector General (OIG) Report on Central Intelligence Agency Accountability Regarding Findings and Conclusions of the Report of the Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001. In 2005, then-CIA Director Porter Goss issued a public statement on the OIG report. In 2007, CIA publicly released a redacted executive summary of the report along with a statement from then-Director Michael Hayden. In response to FOIA requests for the full 2005 OIG report, CIA and other agencies conducted an extensive review of the nearly 500-page document in order to release information that no longer needed to be protected in the interests of national security.

To further contribute to the public record on these events, CIA has also released today redacted versions of four other documents that relate to the 2005 OIG report and provide alternate views on the Agency's performance prior to 9/11. These documents underwent the same review process as the 2005 OIG report. These additional documents include two internal statements by former CIA Director George Tenet in February 2005 and June 2005 that respond to drafts of the 2005 OIG report. They also include two other documents that were previously released, but now contain fewer redactions in light of the recent declassification of information on CIA’s counterterrorism operations. These documents are an August 2001 OIG Inspection Report of the DCI Counterterrorism Center (CTC), released in 2010, and a July 2005 memorandum from 17 CTC officers responding to the 2005 OIG report, released in 2005.

The events of 9/11 will be forever seared into the memories of all Americans who bore witness to the single greatest tragedy to befall our homeland in recent history. The documents released today reflect differing views formed roughly a decade ago within CIA about the Agency’s performance prior to 9/11.

Via CIA.gov

- #CIA
Newly Declassified Documents

June 1, 2015

Today we’ve added newly declassified documents to two prior posts:

- The Department of Justice Releases Additional Documents Concerning Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 - Published December 12, 2014
- Release of Documents Concerning Activities under the Foreign Intelligence Surveillance Act - Published March 3, 2015

From time to time we are able to update older posts on IC on the Record with newly declassified information. When we do so, we always note the addition in the original post (in this case, marked as “added June 1, 2015”) as well as create a new blog entry to direct you to the freshly released information.

IC ON THE RECORD:

Direct access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community.

Created at the direction of the President of the United States and maintained by the Office of the Director of National Intelligence.

Follow @IContherecord

CONTENT:

- Official Statements
- Declassified Documents
- Testimony
- Speeches & Interviews
- Fact Sheets
- Oversight & Compliance

http://icontherecord.tumblr.com/
HOT TOPICS:

- Civil Liberties
- FISA
- FISC
- Section 215
- Section 702

THEIR OWN WORDS:

- James Clapper, DNI
- Mike Rogers, Dir. NSA
- Rick Ledgett, Dep. Dir., NSA
- Robert Litt, GC, ODNI
- Alex Joel, CIPO, ODNI
- Becky Richards, CIPO, NSA
- John Delong, CD, NSA

(Former IC Officials)

- Keith Alexander, Dir. NSA
- John Inglis, Dep. Dir. NSA
- Edward DeCh., GC, NSA

Search this site

This website is maintained by the Office of the Director of National Intelligence.
PUBLIC LAW 111–259—OCT. 7, 2010

INTELLIGENCE AUTHORIZATION ACT
FOR FISCAL YEAR 2010
(b) MODIFICATIONS TO ANNUAL REPORT ON PROTECTION OF INTELLIGENCE IDENTITIES.—The first sentence of section 603(a) of the National Security Act of 1947 (50 U.S.C. 423(a)) is amended by inserting “including an assessment of the need, if any, for modification of this title for the purpose of improving legal protections for covert agents,” after “measures to protect the identities of covert agents.”

SEC. 384. NATIONAL INTELLIGENCE PROGRAM BUDGET.

Section 601 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 415c) is amended to read as follows:

50 USC 415c.

“SEC. 601. AVAILABILITY TO PUBLIC OF CERTAIN INTELLIGENCE FUNDING INFORMATION.

“(a) BUDGET REQUEST.—At the time that the President submits to Congress the budget for a fiscal year pursuant to section 1105 of title 31, United States Code, the President shall disclose to the public the aggregate amount of appropriations requested for that fiscal year for the National Intelligence Program.

“(b) AMOUNTS APPROPRIATED EACH FISCAL YEAR.—Not later than 30 days after the end of each fiscal year, the Director of National Intelligence shall disclose to the public the aggregate amount of funds appropriated by Congress for the National Intelligence Program for such fiscal year.

“(c) WAIVER.—

“(1) IN GENERAL.—The President may waive or postpone the disclosure required by subsection (a) or (b) for a fiscal year by submitting to the Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives—

“A statement, in unclassified form, that the disclosure required in subsection (a) or (b) for that fiscal year would damage national security; and

“(B) a statement detailing the reasons for the waiver or postponement, which may be submitted in classified form.

“(2) SUBMISSION DATES.—The President shall submit the statements required under paragraph (1)—

“A (A) in the case of a waiver or postponement of a disclosure required under subsection (a), at the time of the submission of the budget for the fiscal year for which such disclosure is waived or postponed, and

“(B) in the case of a waiver or postponement of a disclosure required under subsection (b), not later than 30 days after the date of the end of the fiscal year for which such disclosure is waived or postponed.

“(d) DEFINITION.—As used in this section, the term ‘National Intelligence Program’ has the meaning given the term in section 3(6) of the National Security Act of 1947 (50 U.S.C. 401a(6)).”.

SEC. 385. IMPROVING THE REVIEW AUTHORITY OF THE PUBLIC INTEREST DECLASSIFICATION BOARD.

Paragraph (5) of section 703(b) of the Public Interest Declassification Act of 2000 (50 U.S.C. 435 note) is amended—

(1) by striking “jurisdiction,” and inserting “jurisdiction or by a member of the committee of jurisdiction,”; and
Introduction

In accord with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), in February 2005 President George W. Bush nominated John D. Negroponte to serve as the first Director of National Intelligence (DNI). Shortly thereafter, the Presidentially mandated Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the “WMD Commission”), co-chaired by former Senator Charles S. Robb and Judge Laurence H. Silberman, issued its report. Ultimately, the President endorsed 70 of the Commission’s 74 recommendations, approved detailed implementation plans, and assigned implementation of the vast majority of recommendations to the DNI.

Since its establishment in spring 2005, the Office of the DNI (ODNI) has closely monitored and tracked implementation of the Commission’s recommendations—ensuring that each met the Commission’s original intent as well as the more specific implementation plans endorsed by the White House. This has been in addition to reform efforts in compliance with, for instance, the IRTPA. In looking at the Intelligence Community (IC) a year later, a good deal has already changed. A review of the WMD Commission recommendations, though by no means exhaustive, provides a good basis for assessing the breadth of those changes and for prioritizing the ODNI’s goals for continuing IC reform in the coming year.

I. An End-to-End Enterprise: Realizing the Vision for Mission Management

Recognizing the value the ODNI could add by integrating all aspects of intelligence, particularly on high-priority intelligence targets, the WMD Commission recommended that the DNI create “Mission Managers” to bring the full array of the DNI’s authorities and tools to bear upon specific targets. The Commission also recommended that the DNI create a comprehensive, or “end-to-end,” collection enterprise that would improve target development and collection management against all topics. In the past year significant progress has been made toward realizing this vision—both for specific mission managers and for a broader mission management process with enhanced collection management.

- To direct and organize strategic efforts across collection, analysis, and all intelligence disciplines, the DNI promulgated the first National Intelligence Strategy in October 2005. (Recommendation 7.01)

- In November 2005 the DNI directed the establishment of Mission Managers for counterterrorism, counterproliferation, Iran, and North Korea. In Intelligence Community Directive 1 the DNI also designated the National Counterintelligence Executive (NCIX) as Mission Manager for counterintelligence. While the National Counterterrorism Center (NCTC) and the NCIX existed in some form prior to the ODNI’s establishment, the National Counterproliferation Center (NCPC) and the Mission Managers for Iran and North Korea have built their offices from scratch, erecting entirely new structures for organizing the IC on these key topics. The ODNI has had considerable success in establishing its Mission Managers as the principal designees for ensuring that the Community addresses key intelligence needs on high-priority topics and aggressively seeks to close critical intelligence gaps. (Recommendations 6.01, 8.01, and 11.01)
The ODNI’s offices for analytic mission management and the Hard Target Boards have initiated a new targeting process in which analysts formulate detailed targeting lists to penetrate hard targets for use by the ODNI’s office for collection. (Recommendation 6.02)

In response to the Commission’s critique of the National Intelligence Collection Board (NICB) process, the ODNI has overhauled the NICB, establishing a new framework that involves closer collaboration with analysts and employs a more systematic approach to identifying and addressing collection gaps. (Recommendation 7.01)

The ODNI is currently in the midst of developing an Integrated Collection Architecture, a mapping of the IC’s collection resources and capabilities across all disciplines that will provide a baseline for future planning decisions. The technical portion of the architecture is slated for completion by fall 2006. (Recommendation 7.01)

To direct and organize strategic efforts across collection, analysis, and all other intelligence disciplines, the DNI promulgated the first National Intelligence Strategy in October 2005. (Recommendation 7.01)

To direct the IC’s Science and Technology (S&T) efforts strategically and ensure that the United States is prepared to face growing technological intelligence challenges, the Associate DNI for S&T is preparing an S&T Investment Plan for the IC. The first of its kind, the plan identifies gaps in the IC’s S&T efforts and sets aside resources to close them. The Associate DNI for S&T has also implemented new human resources programs to reward, recruit, and retain top S&T talent with prestigious awards and career-enhancing rotational assignments. (Recommendation 6.05)

II. Structural Change: Creating New Organizations and Rationalizing Old Ones

Among the major structural changes over the past year, the most immediately relevant is the standup of the ODNI itself. Yet many of the Community’s new structures lie outside the ODNI, consistent with the Commission’s vision of a top-level management structure with decentralized execution. Over the past year the IC has established several important new organizations: the National Clandestine Service (NCS), to reshape HUMINT collection by serving as the national authority on HUMINT across the IC; the National Security Branch (NSB), to invigorate and institutionalize intelligence reforms at the FBI; and the Open Source Center (OSC), to raise the stature and availability of open source material. The DNI has also strengthened the NCTC, which is currently establishing counterterrorism analysis “lanes in the road” and augmenting its analytic cadre.

On December 21, 2005 the DNI announced the formal establishment of the NCPC. Consistent with the WMD Commission Recommendation, the NCPC is small (with fewer than 75 officers) and, rather than conduct analysis, will provide strategic direction for the entire counterproliferation (CP) community. Also in accord with the Commission’s recommendations, the NCPC has a designated Bio Threats Advisor and is establishing an Advisory Board specifically for biological threats. Among other initiatives, the NCPC has undertaken an “Over the Horizon” Program to look at emerging or potential WMD
programs or problems; begun to develop integrated analytic and collection strategies against key proliferation targets; launched an Innovation Fund to support proposals for improving CP intelligence; and designed a Human Capital Initiative to develop a CP training curriculum. Finally, the NCPC is evaluating CP funding throughout the IC to inform the DNI's budgetary decisions on where and how money can be best spent. (Recommendations 6.06, 13.01, 13.02, 13.03)

The WMD Commission's Iraq case study, among others, demonstrated the need for increased interagency HUMINT coordination, better and more uniform tradecraft standards, and increased joint training for operators. In response, on October 13, 2005, consistent with the Commission's recommendation and working in close coordination with the ODNI, the CIA received the President's approval to establish the NCS. The Director of the NCS has new Community responsibilities related to clandestine HUMINT operations, in addition to managing the CIA's Clandestine Service (the former Directorate of Operations). The Director of the NCS serves as the national authority for the integration, coordination, deconfliction, and evaluation of HUMINT operations across the IC. Included as part of the NCS's mission, as envisioned by the Commission, is implementation of common standards for training, tradecraft, asset validation, reports standardization, HUMINT-related research and development, and other areas affecting HUMINT operations. The NCS is currently staffing its new Community components and is beginning to formulate these Community standards. (Recommendations 7.03 and 7.04)

On September 12, 2005 the FBI established the NSB to bring together under a single umbrella its counterterrorism, counterintelligence, and intelligence programs. The NSB is led by an Executive Assistant Director (EAD) for National Security with direct line authority over the FBI's CT and CI Divisions as well as its Directorate of Intelligence. Creation of the NSB has changed the way the FBI interacts as a member of the IC. The EAD now attends weekly meetings of the "Big Six" IC agency leaders with the Principal Deputy DNI, a shift from the previous "Big Five" model that excluded the FBI. In January 2006 the NSB initiated a pilot program in five field offices (San Francisco, Pittsburgh, Charlotte, Miami, and Little Rock) to test the NSB concept in the field. The FBI launched a second phase, to include five more field offices, in May 2006. The FBI is also engaged in developing an advanced training program for agents and is improving its intelligence training for analysts by requiring that new analysts enter a five-week analytic training program upon their arrival. Further, the FBI's intelligence budget has been rationalized, a cornerstone of the Commission's recommendations, with an initial realignment of this funding enacted in FY 2006. (Recommendations 10.01 and 11.05)

Recognizing the growing importance of open source intelligence, the WMD Commission recommended creation of an Open Source Directorate at the CIA to improve exploitation and availability of open source capabilities and information. On November 1, 2005 the DNI established the OSC, with the CIA as its executive agent. The OSC has already seen returns on its efforts; open source analytic pieces have received greater senior policymaker attention than in previous years and the Center's internet resources have registered a surge in interest from the IC. The Assistant DNI for Open Source has promulgated a strategy for a decentralized but centrally managed National Open Source
Enterprise and is working to professionalize the Community’s open source cadre. Toward this end, the OSC has opened its training academy to others from around the Community and is developing a core guild of analysts to conduct open source outreach across the IC, an effort it will continue into 2007.

The ODNI has also helped bring centralized management and oversight to Measurement and Signals Intelligence (MASINT). Consistent with the applicable WMD Commission recommendation, in July 2005 the DNI appointed a MASINT Community Executive and realigned critical MASINT responsibilities to help clarify IC roles and make MASINT resources more transparent and easier to manage. The Executive will review the MASINT portion of each IC program budget prior to DNI approval and provide input as necessary. (Recommendation 7.08)

III. Collection and Analysis: Improving Community Tradecraft

Below the level of organizational change are several changes the Commission recommended to remedy specific tradecraft or methodological problems. The Commission perceived an IC that had not institutionalized alternative analysis and thus fell prey to its own ingrained assumptions (as in the case of pre-war intelligence on Iraq), that often tied itself in knots trying to unravel or rationalize rules on protecting the privacy of U.S. persons, and that was unable to differentiate between sources from different agencies or validate them using consistently rigorous methods. The IC has made a number of improvements to its tradecraft practices in response to the WMD Commission recommendations.

In response to the Commission’s observations that the President’s Daily Briefing (PDB) tended to have a myopic focus on the issues of the day, that it should incorporate competing conclusions and the reasons for disagreement into articles, and that redundant reporting streams to the President should be consolidated, the ODNI opened the PDB to IC contributions beyond the CIA and eliminated a separate stream of counterterrorism reporting to the President by incorporating it into the PDB. Today, all agencies can contribute to the PDB and many, including DIA, INR, OSC, NCTC, the National Intelligence Council (NIC), NSA, FBI, and the military services, have done so. In July 2005 the PDB staff established a strategic planning team to ensure that strategic and long-term issues are addressed. These innovations have been accompanied by changes in analytic tradecraft. PDB and NIC products now incorporate alternative views to illuminate where and why differences in judgment exist, encouraging IC analysts to adhere to the PDB’s rigorous tradecraft standards in all their analytic work. (Recommendation 8.14)

Another institutional change that is gradually reshaping analysis is the creation of a Long Range Analysis Unit under NIC auspices. The aim of the Unit, as envisioned by the Commission, is to create a haven where analysts can concentrate on long-term projects, free from the demands of producing current intelligence. The Unit has already completed a National Intelligence Assessment on “Global Democratization and Promotion Strategies, 2006-10” and has several other projects underway. (Recommendation 8.05)
In a related recommendation, the Commission proposed the creation of a not-for-profit sponsored research institute to expand contacts with those outside the IC. The Administration chose instead to rely on existing IC outreach mechanisms and other means to address this need. The ODNI appointed a Coordinator for Analytic Outreach to lead the ODNI’s outreach initiative and chair a coordinating body composed of members from all 16 IC elements. One new ODNI-sponsored external outreach event is the Summer Hard Problem Initiative, a series of intensive summer studies that will bring together outside experts to address challenging analytic problems. (Recommendation 8.04)

Among its recommendations for improved analytic tradecraft, the Commission proposed that the DNI foster diverse and independent analysis throughout the IC by encouraging alternative hypothesis generation. Various agencies have acted on this recommendation, incorporating alternative analysis into their research plans and analytic units. The CIA, for instance, has developed alternative analysis cells in every office in the Directorate of Intelligence. DIA has encouraged debate through its “Devil’s Advocate Program.” DHS has established an Alternative Analysis Division and an analytic Red Cell unit. Meanwhile, the ODNI is working with IC partners to promulgate Community standards for diverse and independent analysis and has expanded the NIC associates program to include experts in analytic methodology. (Recommendation 8.07)

Another key to improving analysis called for by the Commission was greater collaboration among IC analysts. The ODNI’s Analytic Resources Catalog is both a database and tool that meets these requirements. The Catalog contains information on 17,000 IC analysts throughout the IC, including current assignment, professional experience, academic background, language ability, and other biographical information. (Recommendation 8.01)

Sourcing for NIC products, including National Intelligence Estimates, and the PDB has improved a great deal over the last year. NIC products now include sections on the reliability and nature of, and gaps in, the intelligence upon which they are based. Marked improvements in these two Community products will encourage similar changes to analytic sourcing across the Community. The ODNI is also working on sourcing standards for the entire IC. (Recommendation 8.10)

In response to the Commission’s recommendation, the ODNI is currently surveying the analytic community to identify S&T and weapons analysis capabilities and shortfalls as a prelude to devising and implementing strategies for improving the Community’s analytic capabilities in key areas. The ODNI is also engaged in a project to increase the number of S&T developers supporting S&T analysts. This effort and others like it have been aided by the Analytic Resources Catalog. (Recommendation 8.12)

Working side-by-side with IC HUMINT collectors, the NCS has compiled a set of Community standards for asset validation of clandestine sources. The FBI has incorporated these standards into a new field source manual. As early as August 2005, Defense HUMINT responded to this WMD Commission recommendation by designing new reporting guidelines for HUMINT sources, drafting internal policies on overt source management and asset validation, and realigning reporting within the asset validation.
program. (Recommendation 7.05)

The ODNI has established a new Lessons Learned Center to coordinate lessons learned and promulgate IC standards for lessons learned studies. The Center is currently working with the NCTC on a specific lessons learned project that will support future counterterrorism planning. This summer the Center is launching a series of symposia around the Community on lessons learned and will soon follow with new web services. The Assistant Deputy DNI for Analytic Integrity and Standards, working collaboratively with the Community's analytic elements, is developing tradecraft standards for the IC. She has also launched an evaluation of finished intelligence on several topics and will use the findings to focus analytic training. (Recommendations 6.09 and 8.16)

Working with the Department of Justice (DOJ) and attorneys from throughout the Community, the ODNI has completed a review of U.S. persons rules and procedures and prepared initial recommendations for changes to achieve consistency wherever possible. Unlike prior reviews, the final product will contain specific recommendations and implementation plans. The DNI has also appointed a Civil Liberties Protection Officer responsible for ensuring the due protection of civil liberties in the IC. (Recommendation 9.04)

IV. Human Capital: Laying the Foundations

Human capital is one of the areas where the ODNI has made the most progress in its first year—laying the foundations for an integrated Intelligence Community.

The ODNI established a centralized human resources authority for the IC in the person of its Chief Human Capital Officer. By working closely with agencies and departments across the Community, the Chief Human Capital Officer has initiated far-reaching human capital reforms that will affect the entire IC workforce. The ODNI has completed the first Strategic Human Capital Plan for the IC: developed competencies for analysts and managers across the Community to set baselines for IC-wide standards for promotion, qualification, training, and education; mandated individual Personal Performance Agreements for agency heads and senior IC executives to make them accountable for implementing agreed-upon innovations; completed policies that will make joint duty a prerequisite for promotion to senior levels of the IC; and initiated development of a modern, performance-based compensation system for civilian employees that will be completed over the next two years. (Recommendation 6.04)

To complement the implementation of a performance-based compensation system, the ODNI is developing a comprehensive non-monetary awards program. Initial efforts have built on previous IC and agency-specific awards for analytic excellence. Although implementation of this recommendation has not yet addressed incentives beyond prizes and such "awards" as increased travel, training, rotations, and sabbaticals, the second phase of implementation will involve less tangible incentives. (Recommendation 8.15)

The Commission's recommendations in the human capital arena also focus on the need for more centralized training and greater education oversight. To date, the National
Intelligence University (NIU) system has focused on developing competency models that will shape training standards for analysts, managers, and all other IC members. The Office of the Deputy Director for Analysis is working with the NIU to develop a new introductory training course for IC analysts. The NIU has also begun to offer training services on matters of common concern to agencies. For example, it will soon open 25 percent of the enrollment in core leadership/management training courses to participants from outside the hosting agency, thereby increasing the Community nature of such courses and promoting cross-fertilization. (Recommendations 8.08 and 8.09)

V. Information Access: Beyond Sharing

Information sharing has been one of the imperatives driving intelligence reform since September 11, 2001, yet the challenge posed extends far beyond the IC to encompass the federal, state, local, and tribal levels and the private sector. The IRTPA required the President to establish an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information among federal, state, local, and tribal agencies and, as appropriate, with private-sector entities in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties. The IRTPA also called for the designation of a Program Manager to oversee ISE implementation and management. The WMD Commission subsequently recommended that the Program Manager be incorporated into the ODNI, a change the President made in June 2005.

The recommendations regarding information sharing present formidable challenges for the U.S. Government and the IC in particular. In many cases, improved information sharing requires the reexamination of such foundational policies as classification and U.S. Persons rules. The issue of information access is broader than information sharing and will require changes to how the IC categorizes, processes, and handles information of all kinds, an effort that will extend over the next several years.

In addition to the Program Manager, the creation of the ODNI put in place a second institutional feature that will help drive information sharing: the ISE Program Manager mentioned above, and the DNI Chief Information Officer (CIO), a Senate-confirmed member of the DNI’s senior leadership team. The CIO has substantially greater authority over IC information technology than was previously vested in a single individual. In addition, the Deputy Director of National Intelligence for Customer Outcomes is helping advance changes in information sharing by consulting with key customers—such as military and law enforcement officials—regarding their needs. (Recommendations 9.01 and 9.02)

The CIO, appointed in December 2005, has pursued implementation of a classified information sharing initiative designed to enhance and expand information sharing with key U.S. allies. Bold measures were needed to push this initiative through the interagency process, illustrating the value of an independent arbiter to manage risk corporately. While the success of this program is only one step toward overhauling the IC’s information management system, as called for in the Commission report, it represented a paradigm shift in the IC’s information sharing policies. The CIO has also
overcome barriers to information sharing and implementation of information sharing standards. For instance, by dismantling prohibitive firewalls, leveraging commercial technologies, and inter-connecting DoD and IC transport systems, the CIO has allowed for broader federal access to INTELINK’s Sensitive But Unclassified domain. This initiative increased the potential customer base approximately four-fold to four million users across the Federal government, providing unencumbered access to this rapidly growing environment. Government officials and subject matter experts outside the IC, including those at the Departments of Health and Human Services and Justice, can now actively share information and collaborate over this IC network. (Recommendation 6.03)

The WMD Commission recognized the importance of building on existing enterprise architectures (information networks and structures) to create the information sharing environment. Faced with a plethora of existing systems, not to mention myriad studies and surveys on the Federal government’s terrorism information sharing capabilities, the Program Manager dedicated most of the first year to establishing a baseline for these capabilities to ensure that the Program Manager’s final analysis was grounded in solid assumptions. Working closely with the CIO, the Program Manager will soon issue an Implementation Plan Report that will include, along with a recommended design and implementation plan for the ISE, recommendations on whether to expand the ISE to encompass all intelligence information. These reports follow a preliminary report to the President and Congress on June 15, 2005 and an interim report on the creation of the ISE in January 2006. The Program Manager has rolled out “blue pages” as part of its electronic directory services (as called for in recommendation 9.06) that will provide agency contact information for all agencies with counterterrorism responsibilities in the Federal government. These blue pages will be followed by yellow and white pages that will include more specific information. (Recommendations 9.01 and 9.06)

One of the recommendations on information sharing calls for the DNI to simplify and modernize the information classification system. Several new ODNI classification policies are currently in the final stages of review, but more significant shifts may be required. If so, the DNI’s classification and declassification authorities may require strengthening. The ODNI is currently engaged with the NSC in examining the possibility of broader change. (Recommendation 9.07)

A related information access problem pertains to disclosures of intelligence information—authorized and unauthorized. With respect to authorized disclosures, the IC’s challenge is to improve security awareness and exercise appropriate caution when releasing information. The ODNI is investigating different disclosure policies IC agencies have in place before disseminating an IC-wide policy. With regard to unauthorized disclosures (or “leaks”), the IC has done a great deal to improve training and awareness, implement audit technologies, and ensure follow-through on investigations. The DOJ and ODNI are also working closely on leaks issues. In March 2006 the ODNI issued policies to consolidate IC reporting of leaks and is now preparing to issue a Community-wide directive on disclosures. (Recommendations 7.10 and 7.01)

The final recommendations on information access—8.05, 8.11, and 8.13—pertain to analytic tools and making analysis available to customers and intelligence officials in
innovative ways; combined, they have significant implications for the IC. The ODNI is currently engaged in several projects to foster the use of more multi-INT analytic tools to improve the IC’s collection against difficult targets, and in the fall will roll out an Executive Intelligence Summary that will provide intelligence users a daily web-based compendium of IC reporting. (Recommendations 8.05, 8.11, and 8.13)

Conclusion

In its first year, the ODNI and the IC have issued a National Intelligence Strategy, restructured the IC’s processes for collection management, established the National Security Branch and National Clandestine Service, made the PDB more of a Community product, and instituted changes in information sharing. The ODNI has made greatest use of its authorities in the personnel arena, though its strategic plans and integrated architectures foretell (and will enable) serious budgetary tradeoffs for the future. The ODNI actions outlined above will generate marked added value in the future.

Through these various reform efforts, the IC has made critical improvements to the security of the United States of America. The IC has met considerable success, has clear plans for moving forward, and remains committed to surpassing the Commission’s recommendations.
ODNI FACT SHEET
Forging an Intelligence Community that delivers the most insightful intelligence possible

HISTORY AND BACKGROUND
Post 9/11 investigations proposed sweeping change in the Intelligence Community, resulting in Congressional passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The IRTPA created the Office of the Director of National Intelligence (ODNI) to oversee a 17-organization Intelligence Community (IC) and improve information sharing, promote a strategic, unified direction, and ensure integration across the nation’s IC.

- The Office of the Director of National Intelligence stood up on April 21, 2005. The ODNI is led by a Director of National Intelligence (DNI), who is currently James R. Clapper.

- Under DNI Clapper’s leadership, the ODNI has refocused its Core Mission to “Lead Intelligence Integration” with a Vision of a Nation made more secure because of a fully integrated Intelligence Community.

- The DNI, in compliance with the law:
  - Serves as the President’s principal intelligence advisor;
  - Oversees the National Intelligence Program budget ($54.6 billion in FY2011);
  - Establishes Intelligence Community priorities with clear and measurable goals and objectives;
  - Sets direction through policies and budgets;
  - Ensures integration of IC personnel, expertise, and capabilities;
  - Provides leadership on IC cross-cutting issues; and
  - Monitors IC agency and leadership performance.

- The DNI works closely with the Principal Deputy DNI to effectively integrate foreign, military and domestic intelligence in defense of the homeland and in support of United States national security interests at home and abroad.

- The organizational structure of the ODNI also includes the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), the National Counterintelligence Executive (NCIX), and the Intelligence Advanced Research Projects Activity (IARPA).

PROGRESS TO DATE
The task of improving and integrating our intelligence structure, and the capabilities and information technologies of 17 diverse intelligence elements is a massive one, and remains a work in progress. However, since its creation, the ODNI has made considerable progress toward breaking down the information-sharing, technical, and cultural barriers across the IC that were identified in the wake of the 9/11 attacks. We continue to build upon IC successes in preventing and minimizing threats, increasing information sharing and integration across the Community, and improving intelligence capabilities to prepare for tomorrow’s challenges while performing today’s mission. The following list of selected achievements illustrates that progress.
**Threat Prevention**

Led the IC’s integrated effort in taking down Osama bin Laden, an event that showed the rest of the world the unyielding determination and resilience of the United States. While the most successful intelligence operation ever was a victory for our Nation, it was an accomplishment made possible by the men and women of the ODNI and the entire IC. It was also an example of how we have worked together to make significant progress toward the critical goal of integrating our intelligence efforts.

**Fused domestic and foreign intelligence to quickly understand and disrupt homeland threats posed by alleged extremists**, including Najibullah Zazi, David Headley, and Abdulhakim Mujahid Muhammad. The IC rapidly produced and pushed relevant counterterrorism information to state, local, tribal, and private partners through the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS).

**Strengthened watchlisting criteria** in response to the attempted bombing of Northwest Flight 253 in December 2009. ODNI dedicated additional resources to enhance terrorist identities records maintained at the NCTC, and established an analytic “Pursuit Group” to focus exclusively on information that could lead to the discovery of threats aimed against the United States or interests abroad. NCTC Pursuit Groups examine emerging terrorist threat threads and other non-obvious connections, and provide intelligence leads to partner agencies and law enforcement organizations for their action as appropriate.

**Developed an infrastructure to integrate threat information.** In conjunction with other intelligence agencies, NCTC developed an infrastructure to meet the demands of the evolving threat. This includes the enhancements of search capabilities across databases, and the development of a “CT Data Layer” to discover non-obvious terrorist relationships. This enables analysts to examine potential threats more efficiently. All of these efforts are being pursued with careful consideration of legal, policy, and technical issues to protect privacy and civil liberties.

**Surged intelligence support to Mexico** to help combat drug cartels and their impact on Mexican governance and U.S. border security.

**Employed IC resources and capabilities to address emerging transnational public health emergencies.** The IC quickly provided policymakers with assessments and projections on the spread and impact of the H1N1 virus, on foreign government responses to the pandemic, and on the political and economic impacts that the virus and mitigation efforts may have. To improve analysis of and integrate collection on future public health emergencies, the DNI created a Senior Advisor for Global Health Security and a Program Director for Global Health to lead the IC’s response to naturally occurring or accidental biological events.

**Funded more than 80 new technologies for interagency intelligence operations through ODNI’s Rapid Technology Transition Initiative (RTTI).** One of the technologies, FBI’s Biometric QuickCapture Platform program, combines electronic fingerprint collection, satellite communication, and database interoperability technologies to help law enforcement agents immediately identify a suspect as a known terrorist or international criminal. The use of this platform resulted in the identification and capture of hundreds of valuable intelligence targets in high-priority countries.
Strengthened insider threat protection. In the wake of the WikiLeaks compromise, ODNI developed a blueprint and guidelines for insider threat detection. This will assist U.S. government organizations in establishing and operating insider threat programs, thereby reducing the risk that compromises will occur in the future.

*Increased Information Sharing and Integration*

Stood up and operationalized a new Deputy Directorate for Intelligence Integration (DDNI/II) to lead ODNI’s core mission by serving as a single stop for collection and analysis requirements across the IC. DDNI/II accomplishes this by uniting the functions of the former Analysis and Collection directorates, the National Intelligence Council (NIC), and other ODNI elements in support of developing Unifying Intelligence Strategies (UIS) for geographic and topic areas. National Intelligence Managers (NIMs) support and execute the UIS, and are the Community’s touchpoints of responsibility for intelligence integration.

Created the Intelligence Community Executive Committee (EXCOM) to ensure full coverage of key intelligence priorities and eliminate duplication of effort. This senior advisory group, led by the DNI and made up of the directors of the other 16 IC elements, advises and supports the DNI, conducts in-depth discussions on critical issues such as intelligence support to Afghanistan and Pakistan and terrorist finance, and enables proper resource allocation. No such IC-wide senior leadership gathering existed prior to the inception of the ODNI.

Strengthened and expanded the duties of the cross-community Analytic Production Board, resulting in faster and more pointed policy advice, improved liaison among IC elements, and improved integration through greater transparency. The Board is led by a senior ODNI officer, ensuring close liaison and clarity of message between ODNI and all IC analysis production elements.

*Promoted integration through the IC Joint Duty program.* Joint Duty builds a new generation of intelligence leaders who have a better understanding of the scope and complexity of the IC and are able to integrate and engage the IC’s vast resources in support of our national security mission. Joint Duty, a winner of Harvard University’s 2008 Innovations in American Government Awards, is now a prerequisite for promotion to senior leadership levels. More than 12,000 intelligence officers have earned or are currently earning Joint Duty credit to gain critical cross-agency perspectives. The NCTC, in particular, has benefited from the Joint Duty Program, with nearly 50 percent of its personnel detailed from other IC agencies.

*Transformed analysis through the creation of online collaborative tools.* Intellipedia and A-Space provide IC analysts a common platform to post information, conduct research and analysis, and easily collaborate with colleagues working similar issues. The value of both Intellipedia and A-Space (praised by *Time Magazine* as one of the best inventions of 2008) became apparent in the wake of the 2008 Mumbai terror attacks, when an ad hoc group of IC analysts convened on the classified sites to post video, photos, and satellite imagery, and discuss the events as they were unfolding in real-time. Analysts used intelligence that had been posted and discussed on A-Space in the previous months to identify an al-Qaida-affiliated extremist group as the perpetrator of the attacks.
Strengthened information sharing and integration under Intelligence Community Directive 501, which requires each IC element responsible for making information collected and analyzed discoverable electronically. In support of this effort, the DNI directed enhancements to the Library of National Intelligence (LNI), a virtual card catalogue, that now offers access to at least 10 million analytic products to more than 100,000 IC employees. LNI is transforming IC employees’ ability to discover information they or their home agencies may not have had access to in the past.

Created an IC Information Sharing Executive. Published in August 2011, the Strategic Intent for Information Sharing clarifies the role of the IC Information Sharing Executive in leading a Community-wide effort to improve information sharing capabilities. The role also provides governance, removes or reduces policy and legal impediments, protects privacy and civil liberties, and promotes a culture embracing information sharing as a core and fundamental responsibility of every IC officer.

Improved information sharing to state and urban fusion centers by granting personnel with federal security clearances access to select Secret Internet Protocol Router Network (SIPRNet) websites with classified homeland security-related information. Partners access these sites via DHS’ Data Network, which is currently being deployed to the 72 recognized state and local fusion centers across the country. This agreement, carried out between the Departments of Homeland Security and Defense and brokered by the ODNI, reflects the IC’s commitment to improving two-way information sharing and enhanced situational awareness among state, local, and tribal partners who are on the front lines of our homeland security enterprise. Within NCTC, the Interagency Threat Assessment and Coordination Group assists state, local and tribal first responders in accessing and understanding federal intelligence reporting and to encourage the sharing of information.

Integrated IC-wide analysis and collection for high-priority intelligence targets by establishing country-and issue-specific National Intelligence Managers (NIM). The NIM concept allows the IC to consolidate Community-wide expertise on specific countries and issues, respond quickly to policymakers’ intelligence needs, and identify knowledge gaps across the Community. For example, ODNI’s designation of a NIM South Asia/Afghanistan-Pakistan enables the IC to bring wide-ranging resources and capabilities to bear against one of the Administration’s most urgent national security challenges. Additionally, ODNI’s NIM Iran increased the speed by which high-impact collection and analysis on Iran reaches policymakers, and created an IC-wide program to develop Iran expertise.

Led effort to improve counterintelligence protection for select government organizations outside the national security community. These organizations possess and develop a range of valuable information and technology that foreign intelligence services seek to steal. ODNI assessed challenges to counterintelligence (CI) program development and then assisted federal partners in strengthening their CI capabilities.

Improved supply chain threat information sharing across the United States Government (USG) and with the private sector through a series of technical and analytic initiatives. The Office of the National Counterintelligence Executive has increased USG and private sector understanding of the risks associated with their dependence on a globalized supply chain. These initiatives include the deploying of an acquisition risk assessment system to more uniformly inform agencies’ procurement decisions, leading the Threat Information Sharing Working Group to share threat information across the
Intelligence Community, and providing threat briefings to IC and non-IC government organizations, policymakers, and the private sector.

**Advanced the security clearance reform effort** by collaborating with the Department of Defense, the Office of Personnel Management, and the Office of Management and Budget. ODNI completed 25 of 51 key policy and technology projects in the Clearance Reform Strategic Plan, resulting in improved clearance timeliness, quality and reciprocity. The DNI’s government-wide personnel security duties and responsibilities as Security Executive Agent (SecEA) are performed under Executive Order 13467. To date, the SecEA staff completed more than 50 policy requests and oversight actions from across the U.S. government in the first half of CY2011. Additionally, ODNI worked with federal partners to modify a long-standing policy, making it easier for first-generation Americans to attain the highest security clearance and improve the IC’s ability to recruit and retain officers with critical native language capabilities and cultural expertise.

**Executed the Intelligence Community Badge Interoperability Program**, which gives IC employees easier access to facilities outside their parent organizations. For example, the recent addition of the Departments of State, Homeland Security, and the Treasury has improved collaboration with these offices.

**Created Intelligence Today**, which enables those senior policymakers who do not receive the President’s Daily Brief (PDB) access to a wider variety of the IC’s most timely analytic insights on key national security decisions. Intelligence Today represents the first time that intelligence products from each IC organization are consolidated in one web-based platform and disseminated to senior customers and their staffs, similar to how information is distributed via online news publications. Additionally, the website’s online feedback mechanism allows policymakers to submit comments, ask questions, and solicit additional information on a specific intelligence product.

**Fielded new technical advances that drive information sharing throughout the Community and with key international allies across multiple security domains.** New capabilities include: an enhanced IC-Email service that features encryption, improved directory services, and standardized user naming conventions; and IC-Login, a system that allows IC users with the appropriate clearances to access information at other IC organizations.

**Improved Intelligence Community financial management**, strengthening financial controls and reporting, and setting IC elements on a path to achieve an unqualified audit of their financial statements by 2016. In support of this effort, the ODNI directed the use of best practices transforming financial management processes and systems across the Community. For example, ODNI released the first IC financial management guidelines and reporting standards for the Community in compliance with federal financial management laws and regulations; standardized financial reporting, corrective action plans, and quarterly reporting to Congress; and published a workforce planning guide and appendix to ICD 610, which established financial and performance management competencies.

**Enhanced sustainable two-way information sharing through the Federal Partners Intelligence Forum.** Since 2006, the ODNI has led a monthly forum with the intelligence points of contacts from across the USG. The goal of the forum is to address complex national security issues through a whole of
government approach. The ODNI focuses on education and enhancement of relationships leading to greater collaboration between federal departments and agencies and the IC.

**Strengthened intelligence relationships with foreign partners.** Significantly increased synchronization and alignment of interactions between the IC senior leadership and our foreign partners. Improved collaboration and coordination among the IC organizations has resulted in IC senior leadership delivering a more unified and harmonized message on any given issue, thereby advancing U.S. intelligence relationships with foreign partners.

**Improved Intelligence Capabilities**

**Revamped the President’s Daily Briefing (PDB) to incorporate timely analyses from across the IC,** thus ensuring that reports to senior policymakers provide diverse perspectives and encompass the breadth and depth of IC expertise. Additionally, ODNI created a strategic planning unit to provide overall guidance to the PDB process and ensure strategic and long-term issues are addressed. These innovations were accompanied by changes in analytic tradecraft, encouraging IC analysts to adhere to the PDB’s rigorous standards in their analytic work.

**Led modernization of the Foreign Intelligence Surveillance Act (FISA) to dramatically improve foreign intelligence collection while protecting the privacy and civil liberties of U.S. citizens and legal residents.** ODNI continues to ensure that the IC’s legal authorities are subject to proper oversight and comply with U.S. laws and the Constitution.

**Established a Civil Liberties and Privacy Office (CLPO) to ensure privacy and civil liberties are an integral part of the intelligence mission.** Since ODNI’s inception, CLPO’s guidance has enabled intelligence officers to perform their duties with confidence that individuals’ rights are properly protected, and it assures congressional oversight entities that Intelligence Community elements are complying with legal requirements. CLPO has provided advice and oversight for critical initiatives, such as watchlisting, intelligence collection, information sharing programs, cybersecurity, and the Foreign Intelligence Surveillance Act. CLPO also examines emerging issues and technologies to clarify how protections apply to new situations.

**Developed the first performance-based budget with the FY2010 National Intelligence Program,** strengthening the linkage between strategic outcomes and budget, and addressing the Administration’s highest intelligence priorities. Through the National Intelligence Priorities Framework (NIPF), ODNI aligned collection and analytic resources across the IC to ensure that adequate resources are reaching the most complex national security challenges and emerging threats.

**Focused research on innovative tools and capabilities that help the IC respond to emerging threats.** Through the creation of IARPA, ODNI is funding high-risk, high-payoff research and development projects in many areas, including quantum computing, biometrics, multimedia analytics, and computational linguistics that will address cross-Community challenges in the future. Modeled after the research and development office for the Department of Defense, IARPA aims to dramatically improve the value of collected data, maximize insight from those collections, and strengthen the IC’s ability to operate in a highly networked world. IARPA’s Coherent Superconducting Qubits program
contributed to *Science* magazine's 2010 "Breakthrough of the Year" with measurements of the world's first quantum mechanical vibrating device.

**Applied standards to analytic tradecraft Community-wide.** These standards are used across the IC to promote more rigorous analytic thinking against our hardest targets. ODNI established an entity to evaluate the quality of IC analytic products against these standards, and developed an “Analysis 101” course open to all new IC analysts for instruction in critical-thinking in a joint training environment.

**Strengthened the National Intelligence Estimates (NIEs) process** by instituting a formal review of the strengths, credibility, and reliability of all intelligence sources used in developing the critical judgments; ensuring subject matter experts from outside the Intelligence Community review every NIE to challenge IC analysts’ assumptions; and including analysis to point out possible opportunities for policymakers. In addition, NIEs are shorter, with discussion and analysis presented to substantiate key judgments. NIEs represent a coordinated and integrated analytic effort among the intelligence enterprise, and are the IC’s most authoritative written judgments concerning national security issues and estimates about the course of future events.

**Augmented language capability and cultural expertise across the IC** through three initiatives: the Heritage Community Liaison Council, the Boren Program and STARTALK. The IC Heritage Community Liaison Council is composed of first and second generation citizens representing mission critical heritage communities. ODNI works with council leaders to improve outreach and recruitment in their respective communities. The Boren Program, which has enabled 180 undergraduate or graduate students a year to study abroad, has created a pipeline of candidates with very high language proficiency, many of whom are now employed by intelligence organizations, the Departments of Defense and State, and supporting contractors. STARTALK, a summer language study program that began in 2007, has taught more than 5,000 middle and high school students mission-critical languages, such as Chinese, Arabic, Hindi, Farsi, and Turkish, and will soon be expanded to reach students in all 50 states.

**Enabled the IC to attract, recruit, and retain individuals with the right language skills and cultural expertise** via partnerships with government agencies, the private sector, and academia. Through ODNI’s IC Centers of Academic Excellence (CAE), the IC has increased access to first and second generation Americans who possess regional, cultural, and critical foreign language expertise. Roughly 60 percent of scholars accepted into the program have traveled overseas and about 70 percent have traveled to countries where a critical language is spoken. Additionally, the CAE program worked with its academic partners to develop national security studies baccalaureate programs to produce future national security professionals.

**Sponsored IC-wide Virtual Career Fairs**, using cutting-edge technologies to find the best and brightest recruits in the United States. The virtual career fairs enabled the IC to reach a greater number of people in a cost effective manner while attendees learned about the IC and applied for positions from the comfort of their homes. More than 5,000 of those who registered for the first fair held in March 2010 reported proficiency in languages critical to national security, and participating IC organizations continue to follow up on applications and interview attendees. The ODNI plans to continue with this new recruiting trend to attract a tech-savvy workforce with the skills necessary to combat the threats of the 21st century.
Panel VI:

Domestic Drones

Moderator:
Laura K. Donohue
Sixty-fourth Legislative Assembly of North Dakota
In Regular Session Commencing Tuesday, January 6, 2015

HOUSE BILL NO. 1328
(Representatives Rick C. Becker, Beadle, Boehning, Kasper, Klemin, Ruby, Thoreson, Toman)
(Senators Anderson, Hogue, Larsen, Unruh)

AN ACT to provide for limitations on the use of an unmanned aerial vehicle for surveillance.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1.

Definitions.

As used in this Act:

1. "Flight data" means imaging or other observation recording.

2. "Flight information" means flight duration, flight path, and mission objective.

3. "Law enforcement agency or agents" has the meaning provided for law enforcement officer in section 12.1-01-04.

4. "Unmanned aerial vehicle" means any aerial vehicle that is operated without the possibility of direct human intervention within or on the aerial vehicle. The term does not include satellites.

5. "Unmanned aerial vehicle system" means an unmanned aerial vehicle and associated elements, including communication links and the components that control the unmanned aerial vehicle, which are required for the pilot in command to operate safely and efficiently in state airspace.

SECTION 2.

Limitations on use of unmanned aerial vehicle system.

1. Information obtained from an unmanned aerial vehicle is not admissible in a prosecution or proceeding within the state unless the information was obtained:
   a. Pursuant to the authority of a search warrant; or
   b. In accordance with exceptions to the warrant requirement.

2. Information obtained from the operation of an unmanned aerial vehicle may not be used in an affidavit of probable cause in an effort to obtain a search warrant, unless the information was obtained under the circumstances described in subdivision a or b of subsection 1 or was obtained through the monitoring of public lands or international borders.

SECTION 3.

Warrant requirements.

A warrant for the use of an unmanned aerial vehicle must satisfy the requirements of the Constitution of North Dakota. In addition, the warrant must contain a data collection statement that includes:

1. The persons that will have the power to authorize the use of the unmanned aerial vehicle;

2. The locations in which the unmanned aerial vehicle system will operate;
3. The maximum period for which the unmanned aerial vehicle system will operate in each flight; and

4. Whether the unmanned aerial vehicle system will collect information or data about individuals or groups of individuals, and if so:
   a. The circumstances under which the unmanned aerial vehicle system will be used; and
   b. The specific kinds of information or data the unmanned aerial vehicle system will collect about individuals and how that information or data, as well as conclusions drawn from that information or data, will be used, disclosed, and otherwise handled, including:
      (1) The period for which the information or data will be retained; and
      (2) Whether the information or data will be destroyed, and if so, when and how the information or data will be destroyed.

SECTION 4.

Exceptions.

This Act does not prohibit any use of an unmanned aerial vehicle for surveillance during the course of:

1. Patrol of national borders. The use of an unmanned aerial vehicle to patrol within twenty-five miles [40.23 kilometers] of a national border, for purposes of policing that border to prevent or deter the illegal entry of any individual, illegal substance, or contraband.

2. Exigent circumstances. The use of an unmanned aerial vehicle by a law enforcement agency is permitted when exigent circumstances exist. For the purposes of this subsection, exigent circumstances exist when a law enforcement agency possesses reasonable suspicion that absent swift preventative action, there is an imminent danger to life or bodily harm.

3. An environmental or weather-related catastrophe. The use of an unmanned aerial vehicle by state or local authorities to preserve public safety, protect property, survey environmental damage to determine if a state of emergency should be declared, or conduct surveillance for the assessment and evaluation of environmental or weather-related damage, erosion, flood, or contamination.

4. Research, education, training, testing, or development efforts undertaken by or in conjunction with a school or institution of higher education within the state and its political subdivisions, nor to public and private collaborators engaged in mutually supported efforts involving research, education, training, testing, or development related to unmanned aerial vehicle systems or unmanned aerial vehicle system technologies and potential applications.

SECTION 5.

Prohibited use.

1. A law enforcement agency may not authorize the use of, including granting a permit to use, an unmanned aerial vehicle armed with any lethal weapons.

2. This Act prohibits any use of an unmanned aerial vehicle for:
   a. Domestic use in private surveillance. A law enforcement agency may not authorize the use of, including granting a permit to use, an unmanned aerial vehicle to permit any private person to conduct surveillance on any other private person without the express, informed consent of that other person or the owner of any real property on which that other private person is present.
b. Surveillance of the lawful exercise of constitutional rights, unless the surveillance is otherwise allowed under this chapter.

SECTION 6.

Documentation of unmanned aerial vehicle use.

1. The person authorized to conduct the surveillance under this Act shall document all use of an unmanned aerial vehicle for surveillance. The person shall document all surveillance flights as to duration, flight path, and mission objectives.

2. The flight information must be verified as accurate and complete by the supervising person authorized by a court to conduct the surveillance.

3. The flight information required under this section must be retained for five years.

4. Any imaging or any other forms of data lawfully obtained under this Act which are not accompanied by a reasonable and articulable suspicion that the images or data contain evidence of a crime, or are relevant to an ongoing investigation or trial, may not be retained for more than ninety days.

5. Except for the operational capabilities of the unmanned aerial vehicle system and other operational information strictly related to the technical conduct and physical security of the surveillance operation, a person accused of a crime that includes evidence gathered through the use of an unmanned aerial vehicle system surveillance may obtain all information relating to the person acquired in the course of the surveillance through subpoena and discovery proceedings available in criminal proceedings.

6. Any other person that has an interest in obtaining the documentation required by this section may obtain that documentation pursuant to chapter 44-04.
This certifies that the within bill originated in the House of Representatives of the Sixty-fourth Legislative Assembly of North Dakota and is known on the records of that body as House Bill No. 1328.

House Vote:  
Yea: 78  
Nay: 14  
Absent: 2

Senate Vote:  
Yea: 29  
Nay: 17  
Absent: 1

Received by the Governor at _______ M. on __________________________, 2015.

Approved at _______ M. on __________________________, 2015.

Filed in this office this _______ day of __________________________, 2015,
at _______ o'clock _______ M.
Domestic Drones and Privacy: A Primer

Richard M. Thompson II
Legislative Attorney

March 30, 2015
Summary

It has been three years since Congress enacted the FAA Modernization and Reform Act of 2012 (FMRA), calling for the integration of unmanned aircraft systems (UAS), or “drones,” into the national airspace by September 2015. During that time, the substantive legal privacy framework relating to UAS on the federal level has remained relatively static: Congress has enacted no law explicitly regulating the potential privacy impacts of drone flights, the courts have had no occasion to rule on the constitutionality of drone surveillance, and the Federal Aviation Administration (FAA) did not include privacy provisions in its proposed rule on small UAS. This issue, however, has not left the national radar. Congress has held hearings and introduced legislation concerning the potential privacy implications of domestic drone use; President Obama recently issued a directive to all federal agencies to assess the privacy impact of their drone operations; and almost half the states have enacted some form of drone legislation.

There are two overarching privacy issues implicated by domestic drone use. The first is defining what “privacy” means in the context of aerial surveillance. Privacy is an ambiguous term that can mean different things in different contexts. This becomes readily apparent when attempting to apply traditional privacy concepts such as personal control and secrecy to drone surveillance. Other, more nuanced privacy theories such as personal autonomy and anonymity must be explored to get a fuller understanding of the privacy risks posed by drone surveillance. Moreover, with ever-increasing advances in data storage and manipulation, the subsequent aggregation, use, and retention of drone-obtained data may warrant an additional privacy impact analysis.

The second predominant issue is which entity should be responsible for regulating drones and privacy. As the final arbiter of the Constitution, the courts are naturally looked upon to provide at least the floor of privacy protection from UAS surveillance, but as will be discussed in this report, under current law, this protection may be minimal. In addition to the courts, the executive branch likely has a role to play in regulating privacy and drones. While the FAA has taken on a relatively passive role in such regulation, the President’s new privacy directive for government drone use and multi-stakeholder process for private use could create an initial framework for privacy regulations. With its power over interstate commerce, Congress has the broadest authority to set national standards for UAS privacy regulation. Several measures were introduced in the 113th Congress that would have restricted both public- and private-actor domestic UAS operations, and reintroduction of these bills is likely in the 114th Congress. Lastly, some have argued that under our system of federalism, the states should be left to experiment with various privacy schemes. It is reported that by the end of 2014, 20 states have enacted some form of drone regulation.

This report will provide a primer on privacy issues related to various UAS operations, both public and private, including an overview of current UAS uses, the privacy interests implicated by these operations, and various potential approaches to UAS privacy regulation.
# Contents

Introduction.................................................................................................................. 1

Background.................................................................................................................... 2
  Authorization and Uses ................................................................................................. 3
  Public Operators ........................................................................................................ 3
  Private Operators ....................................................................................................... 5

Privacy Interests Implicated by UAS Operations ......................................................... 6
  Surveillance .................................................................................................................. 6
  Personal Control ......................................................................................................... 6
  Secrecy ....................................................................................................................... 7
  Autonomy .................................................................................................................. 7
  Anonymity .................................................................................................................. 8

Post-Collection Activities ............................................................................................ 8
  Aggregation .................................................................................................................. 9
  Use .............................................................................................................................. 10
  Retention ................................................................................................................... 10

Various Approaches to UAS Privacy Regulation ......................................................... 11
  Courts ......................................................................................................................... 11
  Fourth Amendment ................................................................................................... 11
  Privacy Torts ............................................................................................................. 14

Executive Branch ......................................................................................................... 17
  FAA—Privacy Rules at the Test Sites and Beyond ...................................................... 17
  President’s Memorandum on UAS and Privacy ......................................................... 19
  Privacy Impact Assessments and Privacy Working Groups ...................................... 21
  DOJ Inspector General UAS Report .......................................................................... 22

Congress ....................................................................................................................... 23
  Legislation ................................................................................................................... 23
  Oversight .................................................................................................................... 25
  States .......................................................................................................................... 26

# Contacts

Author Contact Information.......................................................................................... 27
Introduction

It has been three years since Congress enacted the FAA Modernization and Reform Act of 2012 (FMRA), calling for the integration of unmanned aircraft systems (UAS), or “drones,” into the national airspace by September 2015.1 During that time, the substantive legal privacy framework relating to UAS on the federal level has remained relatively static: Congress has enacted no law explicitly regulating the potential privacy impacts of drone flights; the courts have had no occasion to rule on the constitutionality of drone surveillance; and the Federal Aviation Administration (FAA) did not include privacy provisions in its proposed rule on small UAS.2 However, this issue has not left the national radar. Congress held several hearings in the 113th Congress on the potential privacy impacts of domestic drone use on American citizens;3 Members have introduced legislation to regulate both public- and private-actor use of drones;4 the executive branch has taken various measures to assess the privacy impact of its drone operations;5 and almost half the states have enacted UAS legislation.6

As this report will discuss, there are two overarching privacy issues implicated by domestic drone flights. The first issue is defining and understanding what the chameleon phrase “privacy” means in the context of aerial surveillance. Traditional privacy concepts such as the right to control information about oneself or secrecy do not adequately capture potential privacy concerns raised by visual surveillance; instead, privacy concepts such as personal autonomy and anonymity must be explored to get a fuller understanding about the scope of privacy interests implicated by UAS operations. Additionally, a separate set of privacy interests might be implicated by the subsequent aggregation, use, and retention of drone-obtained information. For instance, the Supreme Court’s aerial surveillance cases generally hold that it is not a Fourth Amendment search to conduct surveillance of private property while flying in navigable airspace.7 However, one could argue that beyond the initial collection of data, a unique privacy interest is at risk by aggregating multiple flights over one’s home, using drone-obtained data in ways never envisioned by the initial collection, or retaining that data indefinitely.

The second predominant issue is which entity should be responsible for regulating UAS privacy issues. The courts can be expected to apply traditional privacy rules encompassed in the Fourth Amendment’s prohibition against unreasonable searches and privacy torts found largely in state statutory and common law. Since drone use has been relatively limited to date, the courts have yet to address how these laws apply to UAS flights. Privacy safeguards might also come from

---

5 See “Executive Branch,” infra p. 17.
executive branch policies. On February 15, 2015, President Obama issued a memorandum charging all federal agencies that use drones in their operations to evaluate the privacy impact of such use and develop policies to mitigate any privacy concerns. The need for this new initiative may have been prompted, in part, by the FAA’s relatively passive role in setting privacy rules for drone operations. The FAA’s recently proposed rule for small UAS operations and certifications did not include any privacy provisions, and it is likely the FAA will remain in an advisory, rather than regulatory, role with respect to this issue. With its power over interstate commerce, Congress has the broadest authority to set national standards for UAS privacy regulation. For instance, Congress could create a broad legislative scheme regulating all UAS uses; it could pass more narrow proposals such as a warrant requirement for law enforcement use; or it could create a scheme regulating the subsequent use, retention, and dissemination of drone-obtained data. Federal legislation introduced in the 113th Congress, and likely to be introduced in the 114th Congress, utilized, to some extent, these various approaches. Lastly, some have argued that under our system of federalism, the states should be left to experiment with various privacy schemes. Indeed, the states have taken up this call with 20 states reportedly enacting laws addressing UAS issues by the end of 2014.

In reviewing these various forms of regulation, it is clear that understanding privacy rights vis-à-vis drones is not as simple as applying Supreme Court case law or federal and state statutes. Rather, regulations may come from myriad sources, some statutory, some regulatory, and some practical. With this in mind, this report will provide a primer on privacy issues relating to various UAS operations, both public and private, including an overview of current UAS uses, the privacy interests implicated by these operations, and various potential approaches to UAS privacy regulation.

Background

The FMRA defined an “unmanned aircraft” to mean “an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.” An “unmanned aircraft system” (UAS) is the unmanned aircraft and its “associated elements (including communications

---

8 PRESIDENTIAL MEMORANDUM: PROMOTING ECONOMIC COMPETITIVENESS WHILE SAFEGUARDING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN DOMESTIC USE OF UNMANNED AIRCRAFT SYSTEMS (Feb. 15, 2015) [hereinafter Presidential Memorandum on UAS].
10 U.S. CONST. art. I, §8, cl. 3.
15 P.L. 112-95, §331, 126 Stat. 72.
links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system. UAS, commonly referred to as “drones,” can range from the size of an insect—sometimes called nano or micro drones—to the size of a traditional jet. Drones can be outfitted with an array of sensors, including high-powered cameras, thermal imaging devices, license plate readers, and laser radar (LADAR). In the near future, drones might be outfitted with facial recognition or soft biometric recognition, which can recognize and track individuals based on attributes such as height, age, gender, and skin color. In addition to their sophisticated sensors, the technical capability of drones is rapidly advancing. For instance, the Defense Advanced Research Projects Agency (DARPA), the technology research arm of the U.S. military, is working on a drone that can enter a building through a window and fly at speeds up to 20 meters/second without communication to the operator and without GPS waypoints. As discussed below, these advanced sensors and capabilities have the capacity to heighten privacy risks posed by drones.

Authorization and Uses

Currently, all UAS operators who do not fall within the recreational use exemption (discussed below) must apply directly to the FAA for permission to fly. The process for obtaining permission to operate differs depending on whether the operator is a public operator or a private commercial operator.

Public Operators

UAS operated by federal, state, or local agencies must obtain a certificate of authorization or waiver (COA) from the FAA. After receiving COA applications, which can be completed online, the FAA conducts a comprehensive operational and technical review of the UAS and can

16 Id.
21 This sensor produces three-dimensional images, and has the capability to see through trees and foliage. U.S. Army, UAS CENTER FOR EXCELLENCE, “EYES OF THE ARMY” US ARMY ROADMAP FOR UNMANNED AIRCRAFT SYSTEMS 2010-2035, at 83 (2010).
23 The issue of weaponizing drones, which presents unique legal issues, is beyond the scope of this report.
25 Id.
place limits on its operation in order to ensure its safe use in airspace. COAs are not generally publicly available, but have been released in response to Freedom of Information Act (FOIA) requests. The most recent FOIA request on the FAA’s website revealed 426 UAS COA files.

**Customs and Border Protection**

The most prominent domestic user of UAS among federal agencies is the Department of Homeland Security’s (DHS’s) U.S. Customs and Border Protection (CBP). As of September 2013, CBP was reported to own 10 UAS, which are operated by CBP’s Office of Air and Marine (OAM). The bulk of CBP’s flight missions involve patrolling the nation’s borders, interdicting persons and contraband illegally entering the United States. CBP’s COA allows it to operate in an airspace that covers a 100 mile corridor along the northern border and within 20 to 60 miles along the southern border, excluding urban areas. In addition to its border missions, CBP has provided unmanned aerial support to various federal and state agencies, including the Drug Enforcement Administration (DEA), Immigration and Customs Enforcement (ICE), the U.S. Marshals Service, the U.S. Coast Guard, the Bureau of Land Management, and the Texas Department of Public Safety, among others. In one prominent case, CBP used one of its Predator drones to assist local police in North Dakota to monitor an individual suspected of cattle theft and threatening police officers. The number of these “loan” operations has steadily increased each year since 2010. For instance, CBP flew one flight for the DEA in 2010, 19 flights in 2011, and 66 in 2012.

**Department of Justice**

The other primary federal agency currently using UAS in its operations is the Department of Justice (DOJ), the nation’s chief law enforcement agency. In 2013, DOJ’s Office of the Inspector General issued a report reviewing the various UAS programs underway within DOJ. All of the UAS purchased by DOJ so far have been what the FAA calls “small UAS,” those 55 pounds or less. The Federal Bureau of Investigation (FBI) has been the most prominent component of DOJ to use UAS in the field and has been doing so since 2006. The FBI noted in a July 2013 letter to Senator Rand Paul that it had used UAS in 10 operations, including those related to search and rescue, drug interdictions, kidnapping, and fugitive investigations. The Bureau of Alcohol,

---

28 Before operating a UAS in the national airspace, CBP, as with any other governmental entity, must obtain a Certificate of Authorization (COA) from the FAA. See CRS Report R42940, for a discussion of FAA’s UAS licensing process.
32 Customs and Border Protection Drone Flight List, supra note 30.
34 Id. at 5.
35 Letter from Stephen D. Kelly, Office of Congressional Affairs, Federal Bureau of Investigation to Senator Rand Paul (continued...)
Tobacco, Firearms and Explosives (ATF) has plans to use UAS in its future operations but has not done so yet. And while the DEA and the Marshals Service have purchased several UAS, as of 2012 they had no plans to use them in future operations. This might be attributed to the DEA and Marshals Service use of CBP drones in their operations.

**Other Federal Uses**

In addition to DHS and DOJ, the FAA has issued COAs to various other federal entities—both military and civilian. On the defense side, COAs have been issued to DARPA, the U.S. Army, the Navy, the Marine Corps, and the Air Force, for operations in U.S. airspace. On the civilian side, COAs have been issued to the Departments of State, Interior, and Energy, the National Aeronautics and Space Administration (NASA), and the National Institute of Standards and Technology (NIST).

**State and Local Governmental Operations**

Like their federal counterparts, state and local governmental entities must obtain a COA in order to conduct drone operations. As of 2012, the FAA has issued several hundred COAs to state and local governmental entities to operate UAS. These have included state and city governments, such as Houston, Texas, and the Colorado Department of Transportation; local fire and police departments, including the Miami-Dade Police Department; and state and local universities, like Indiana University.40

**Private Operators**

Until the FAA finalizes its small UAS rule as required under FMRA, there are currently only a limited number of ways to gain authorization for private commercial use of UAS. A private operator may obtain a special airworthiness certificate in the experimental category issued by the FAA. These certificates have been issued on a limited basis for flight tests, demonstrations, and training. The second means of authorization is under FMRA’s Section 333, which permits the FAA to authorize certain UAS flights before the FAA issues a final small UAS rule. These Section 333 exemptions have been issued for such purposes as movie productions, precision agriculture, flare stack inspection, and bridge inspections. Finally, certain recreational UAS users may fall within FMRA’s model aircraft exception, meaning they are not required to obtain

---

(continued)

(July 19, 2013).

36 DOJ Inspector General Report, supra note 33, at 5.
37 Id. at 6.
39 Id.
40 Id.
42 P.L. 112-95, §333, 126 Stat. 75.
specific authorization from the FAA before flying UAS. Section 336 of FMRA prohibits the FAA from promulgating a rule regarding “model” aircraft if the aircraft is flown “strictly for hobby or recreational use” and meets several other requirements.\footnote{P.L. 112-95, §336, 126 Stat. 77.}

**Privacy Interests Implicated by UAS Operations**

A threshold issue in analyzing drones and privacy is determining what privacy interests might be implicated by drone operations, both public and private. Privacy is an ambiguous term that can mean different things in different contexts, which becomes apparent when attempting to apply traditional privacy concepts to drone surveillance.

**Surveillance**

The first privacy interest implicated by the use of UAS is the initial collection of information about people—what can be called “surveillance”—whether it is conducted by a government or private actor. With respect to UAS operations, surveillance takes place in nearly all flights, as one of their major purposes is to collect information, namely visual surveillance, from the sky above. Surveillance might entail a broad and indiscriminate recording of people on the ground using a camera sensor on the aircraft. For instance, the U.S. Air Force recently rolled out the newest iteration of its “Gorgon Stare” sensor, a remotely controlled, aircraft-based Wide-Area Persistent Surveillance (WAPS) system.\footnote{See Sierra Nevada Corporation Achieves Milestone for USAF’s Advanced Wide-Area Airborne Persistent Surveillance (WAPS) System – Gorgon Stare Increment 2 (July 14, 2014), available at http://www.sncorp.com/AboutUs/NewsDetails/618.} This sensor allows a single UAS to monitor a 100km² area in high resolution for several hours at a time.\footnote{See Sierra Nevada fields Argus-IS upgrade to Gorgon Stare pod, Flight Global (July 2, 2014), available at http://www.flightglobal.com/news/articles/sierra-nevada-fields-argus-is-upgrade-to-gorgon-stare-400978/.} CBP uses a similar sensor while monitoring the U.S. border.\footnote{Privacy Impact Assessment, supra note 29, at 8.} Alternatively, surveillance might consist of more targeted data collection, such as the FBI’s use of a drone in 2013 to monitor a standoff with a child kidnapper.\footnote{See Victor Blackwell & Michael Pearson, FBI: Bombs Found in Alabama Kidnapper’s Banker, CNN (Feb. 5, 2013), available at http://www.cnn.com/2013/02/05/us/alabama-child-hostage/.} Both types of surveillance, to one degree or another, implicate various privacy concepts, including personal control, secrecy, autonomy, and anonymity.

**Personal Control**

One of the leading privacy theories is the right to control information about oneself. According to one prominent privacy theorist, “[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”\footnote{ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).} This paradigm works in some mediums, for example, when we consent to a smart phone app tracking our location: we can decide whether the trade-off to our privacy is worth the service we will receive in exchange. However, with drones and aerial surveillance, however, this theory of privacy breaks down. For instance, should we be able to
control whether people can view us or our activities in public? How are we expected to exercise such control? And should it make a difference if a person sees us from a traditional aircraft versus a drone? Requiring consent before conducting aerial surveillance could undermine many uses of this new technology, making this theory of privacy as applied to drone surveillance unworkable.

Secrecy

Another prominent theory of privacy is the secrecy model. Under this mode, an individual’s privacy is invaded if previously concealed information about them is publicly disclosed; or, put another way, an individual is not entitled to privacy where that information has been revealed to another person.50 The Supreme Court relied on this secrecy model in the three aerial surveillance cases from the 1980s, which held that surveillance conducted in public airspace does not even trigger—let alone violate—the Fourth Amendment’s protection against unreasonable searches.51 Citing to an earlier case, the Court observed in California v. Ciraolo that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”52 In addition to Fourth Amendment case law, the privacy tort intrusion upon seclusion applies this same secrecy model such that most activities revealed to the public would not constitute a violation of this tort.53 If secrecy remains the primary model for the Fourth Amendment and privacy torts, individuals would have little protection from drone surveillance when their location and activities have been revealed to the public.

Autonomy

Another important theory of privacy is personal autonomy. Autonomy generally refers to the ability of an individual to make life decisions free from interference or control by both government and private actors.54 Some have argued that surveillance represents a form of social control, mandating conformity in society, hindering independent thinking, and recording and notating people who stray from acceptable norms.55 One such example is Jeremy Bentham’s Panopticon, a prison facility designed to give inmates the perception of being watched at all times causing them to self-regulate their behavior to the desired norm.56 Of course, some form of social control—say, crime control—is beneficial and expected in every society. As noted by Professor Daniel Solove, “many people desire the discipline and control surveillance can bring.”57

55 See John Gilliam, Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy 3 (2001) (“Surveillance of human behavior is in place to control human behavior, whether by limiting access to programs or institutions, monitoring and affecting behavior within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance.”); Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1426 (2000) (“The point is not that people will not learn under conditions of no-privacy, but that they will learn differently, and that the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines.”).
He notes that “[t]oo much social control, however, can adversely impact freedom, creativity, and self-development.”58 It would appear that potential risks to personal autonomy will depend, at least in part, on the pervasiveness of drone surveillance. Single, targeted operations would not appear to implicate this fear of societal control and harm to personal autonomy. However, some have questioned what effect 24-hour, omnipresent surveillance would have on our public spaces.59 At this point, the shorter flight capabilities of small UAS—the aircraft likely to be most prevalent in the early stages of UAS integration—would limit the ability to conduct such pervasive surveillance. Yet, as this technology becomes more sophisticated and maximum possible flight times are extended, this risk to autonomy may heighten.

Anonymity

Anonymity is a “state of privacy” that “occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance.”60 Professor Christopher Slobogin notes that “the right to public anonymity provides assurance that, when in public, one will remain nameless—unremarked, part of the undifferentiated crowd—as far as the government is concerned. The right is surrendered only when one does or says something that merits government attention, which most of the time must be something suggestive of criminal activity.”61 Others might argue that when we leave our doorstep, and enter into society, we give up this right to anonymity by permitting anyone to view our public movements and whereabouts. Potential blanket UAS surveillance over an urban landscape or a large public event (for instance, the Super Bowl or NASCAR racing), appears to pose a low risk to anonymity. Each person can remain a faceless person in the crowd, free from government identification. Take, for instance, CBP’s surveillance at the border: its Predator-B drones reportedly fly at a minimum of 19,000 feet and are not able to identify specific persons on the ground.62 However, the potential use of sensors such as Automated License Plate Readers (ALPRs)63 or facial recognition technology,64 or UAS surveillance specifically targeted at an individual, may have the capacity to eliminate one’s anonymity when in public.

Post-Collection Activities

The second class of privacy risks posed by drone surveillance are those activities that occur after surveillance has been conducted—the aggregation, use, and retention of that data. In certain

(...continued)

57 Solove, supra note 50, at 494.
58 Id.
60 Westin, supra note 49, at 7.
instances, the initial collection may not directly implicate an individual's privacy interests, but the subsequent manipulation and storage of that data may warrant an alternative privacy analysis.

Aggregation

"Aggregation" is simply the gathering of information about a person whether from one or multiple sources. In the pre-digital era, aggregating information about a person took concerted effort and lots of resources. With computer automation, information can be gathered and aggregated from many sources at the mere push of a button. The privacy theory of aggregation supposes that while the collection of bits of data about a person may not violate his or her privacy interests, extensive collection of information about him or her can rise to the level of a legal privacy intrusion. Professor Solove argues that this unique privacy intrusion arises because "when analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected." This theory was on display in the 2012 GPS tracking case United States v. Jones, where five Justices of the Supreme Court (in two separate concurrences) acknowledged that short-term location monitoring was likely not a Fourth Amendment search, but that 28 days of tracking should be considered a search. Judge Richard Leon of the U.S. District Court for the District of Columbia also applied this aggregation theory when invalidating the National Security Agency's (NSA's) metadata program, observing,

the ubiquity of phones has dramatically altered the quantity of information that is now available and, more importantly, what that information can tell the Government about people's lives. ... Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life.

In the context of UAS operations, aggregation may mean the surveillance of an individual for an extended time, or the combination of drone-obtained data with other independent information. A simple one time fly-over of a residence may not significantly implicate any of the privacy interests described above (e.g., secrecy, autonomy, anonymity), but continuous surveillance of a person may implicate this aggregation interest. Alternatively, aggregating drone-collected data with other seemingly personal information, such as telephone, banking, utility, and other records—all of which can be obtained without a probable cause warrant—might entail a unique privacy infringement beyond the mere collection of those individual data sets.

---

65 See Solove, supra note 50, at 507.
66 Id.
68 Klayman v. Obama, 957 F. Supp. 2d 1, 35-36 (D.D.C. 2013). This case is currently before the D.C. Circuit Court of Appeals.
71 See United States v. McIntyre, 646 F.3d 1107 (8th Cir. 2011); United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *2 (9th Cir. August 24, 1992).
Use

The second post-collection privacy risk is the improper use of data—that is, data collected for an authorized purpose, but subsequently used in an unauthorized way. One commentator has argued that in the era of big data, where we inevitably share troves of personal information with the government and commercial entities, privacy rules that focus on the collection and retention of data are “becoming impractical for individuals, while also potentially cutting off future uses of data that could benefit society.”

He argues that privacy laws should instead focus on controlling the use of that data. Various federal laws embody this principle. For instance, the Privacy Act of 1974 requires any federal agency that maintains a database of personal records to inform each individual about whom it collects information of “the principal purpose or purposes for which the information is intended to be used.” Similarly, the Driver’s Privacy Protection Act of 1994 made it a federal crime “for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted” under that statute. Instead of placing front-end restrictions on drone surveillance, such as requiring warrants before they are operated, policymakers might want to instead regulate how that information is used. For instance, a proposal may permit law enforcement officials to collect information for one purpose—say, traffic control—but prohibit it from using that information for other purposes, such as against an individual in a criminal prosecution absent a court order.

Retention

Another incident of the digital revolution is the near limitless ability of the government and private companies to store and retain information about individuals. The cost of storage has decreased exponentially over the past several decades and is no longer a hindrance to maintaining vast databases of personal data. The Obama Administration’s report on big data highlighted this concern when it noted that “the declining cost of collection, storage, and processing of data, combined with new sources of data like sensors, cameras, geospatial and other observational technologies, means that we live in a world of near-ubiquitous data collection.” This issue of data retention has been one of the drivers behind Europe’s “right to be forgotten” law, which includes a provision requiring that data be retained “for no longer than is necessary for the purposes for which it was collected.”

Generally speaking, when it comes to Fourth Amendment law, once information is lawfully collected, there are no additional constitutional hindrances to it being stored indefinitely. However, in the NSA metadata litigation, Judge Leon acknowledged that unique privacy interests were affected by the long-term storage of everyone’s telephone call records. He observed that in decades past, it was not expected that the government would retain...

---

73 Id.
79 klayman, 976 F. Supp. 2d at 32.
a suspect’s phone records once a case was concluded, whereas “[t]he NSA telephony metadata program ... involves the creation and maintenance of a historical database containing five years’ worth of data.” The privacy impact of retention of UAS-derived data would largely depend on whether people could be identified in the recording. Retention of data that contains personally identifiable information and can be located based on this information would seem to implicate this retention interest.

Various Approaches to UAS Privacy Regulation

In addition to the general privacy concepts implicated by drone surveillance, one might question which government entity, if any, should regulate the potential privacy issues posed by the integration of thousands of UAS into domestic skies. Congress neither mentioned the word “privacy” in FMRA nor has it enacted any substantive privacy rules relating to drones subsequently. The FAA recently issued its proposed rule for operating small drones (55 pounds or less), but failed to include any privacy safeguards. Potentially in response to this dearth of privacy regulations, President Obama recently mandated that all federal agencies evaluate the privacy risks posed by their drone operations. This section will explore different approaches to UAS privacy regulation, focusing on the various government institutions—the courts, the executive branch, Congress, and state governments—that might conduct such regulation.

Courts

As the final arbiter of the Constitution, the courts are frequently relied on to safeguard the privacy rights of Americans, whether through the suppression mechanism in criminal prosecutions, or civil suits against government officials for violations of constitutional rights. The Fourth Amendment, as applied by the courts, will provide a floor of legal protections against government actor use of drones. Likewise, privacy torts, which are given much of their content by the courts, will provide some legal recourse to potential privacy invasions caused by drones operated by private actors.

Fourth Amendment

The Fourth Amendment provides in relevant part: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” This Amendment, like most constitutional protections, applies only to acts by public actors, and, as such, will provide the minimum legal requirements for government use of

\[80\] Id. (emphasis in original).

\[81\] See Marbury v. Madison, 5 U.S. 137, 177 (1803) (“It is emphatically the province and duty of the judicial department to say what the law is.”); Cooper v. Aaron, 358 U.S. 1, 18 (1958) (“Marbury declared the basic principle that the federal judiciary is supreme in the exposition of the law of the Constitution, and that principle has ever since been respected by this Court and the Country as a permanent and indispensable feature of our constitutional system.”).


\[84\] U.S. CONST. amend. IV.

\[85\] Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (“The Fourth Amendment gives protection against unlawful searches and seizures, and as shown in the previous cases, its protection applies to governmental action. Its origin and (continued...)
drones. In order for the Fourth Amendment to apply in a particular situation, a reviewing court must assess whether the government conducted a “search” by asking whether it invaded an individual’s “reasonable expectation of privacy.” Although no court has had the opportunity to apply the Fourth Amendment to drone technology, similar cases regarding traditional aircraft and location monitoring provide insight.

In three cases from the 1980s, the Supreme Court upheld the government’s warrantless use of traditional aircraft to surveil both private and commercial property. In Florida v. Riley, the case most closely resembling potential UAS surveillance, the police flew a helicopter 400 feet above a private residence to determine if marijuana was growing in a greenhouse in the backyard. The Court held that this fly-over was not a Fourth Amendment search, as anyone from the public could have seen the property from that vantage point since the aircraft was in federal airspace. Similarly, in the 1983 case United States v. Knotts, the Court held that it was not a Fourth Amendment search to track a person’s public movements using an electronic tracking device. There is a general consensus among commentators that a strict application of these cases would accord limited privacy safeguards to individuals located on both public and private property from UAS surveillance being conducted from lawful federal airspace.

(...continued)
history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies”).


See Florida v. Riley, 488 U.S. 445, 450-51 (1989) (“Riley could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing aircraft.”); Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986) (“We hold that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment.”); California v. Ciraolo, 476 U.S. 207, 215 (1986) (“In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet. The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.”).

Riley, 488 U.S. at 448.

Ciraolo, 476 U.S. at 213 (“The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer’s observation from a public vantage point where he has a right to be and which renders the activities clearly visible.”).


See Senate Judiciary Hearing, supra note 3, at 94 (2013) (written statement Ryan Calo, Law Professor, University of Washington School of Law) (“The Supreme Court has made it clear through a series of decisions in the nineteen-eighties that there is no search for Fourth Amendment purposes if an airplane or helicopter permits officers to peer into your backyard. I see no reason why these precedents would not readily extend to drones.”); Joseph J. Vacek, Big Brother Will Soon Be Watching—Or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement, 85 N.D. L. REV. 673 (2009) (“Constitutionally, it seems that aerial surveillance by any method of any area in open view from any legal altitude does not implicate the Fourth Amendment, as long as the technology used to obtain the surveillance technology is in general public use and does not penetrate into the home”); Brandon Nagy, Why They Can Watch You: Assessing Constitutionality of Warrantless Unmanned Aerial Surveillance by Law Enforcement, 29 BERKELEY TECH. L. J. 135 (2014) (“Those concerned that increasing law enforcement UAS operations erode personal privacy at the expense of the Fourth Amendment do, indeed, have much to worry about. Current Supreme Court jurisprudence, although not directly addressing the Fourth Amendment implications of UAS surveillance, suggests that law enforcement UAS use, with certain limits, would be
However, several more recent cases demonstrate that the Court has been uneasy about applying decade-old cases to new technology. In Kyllo v. United States, for instance, the use of sense-enhancing technology “not in general public use” to obtain information about the inside of a home was considered a Fourth Amendment search. Similarly, in United States v. Jones, five Justices (in two separate concurrences) would have held that a month-long location monitoring using a GPS device constituted a search, even in the face of Knotts, which upheld the use of a more rudimentary tracking device. The concurring Justices in Jones expressed concern about the sheer ability of these new technologies to collect vast amounts of information about individuals, and their capacity to break down any natural barriers (such as time and resources) to excessive police surveillance. This conundrum of applying old precedent to newer forms of technology is not unique for the federal courts. Several cases currently pending in the federal courts are wrestling with how to apply Smith v. Maryland, a case from the 1970s that addressed the collection of telephone numbers of one individual over several days, to the NSA’s collection of millions of telephone records over a five-year period. With this trend in mind, federal judges may be persuaded that the sophistication and type of sensors used by UAS present a strong enough privacy risk to modify old precedents such as Riley or Ciraolo and adapt them to the new potential reality of UAS aerial surveillance. Additionally, depending on the duration of the surveillance and the amount of data collected on an individual, the courts may be inclined to apply an aggregation-type theory to long-term UAS surveillance.

This issue of the law keeping up with technology is a constantly recurring theme in Fourth Amendment jurisprudence. Some have argued that the judiciary is not the ideal forum for creating adequate privacy rules when fast-moving technology is involved. Courts tend to be backward looking—resolving past factual scenarios between two discrete parties. This characteristic makes courts reactive rather than proactive, leading to privacy rules that might fall behind the particular technology in question. For instance, the Supreme Court has yet to resolve whether individuals are entitled to a reasonable expectation of privacy in their emails, a technology that has been around for decades. Part of the problem is that the Court has been unsure of its role in

(...continued)

found constitutional if challenged under the Fourth Amendment.

95 Id. at 956 (Sotomayor, J., concurring) (“I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.”).
96 Id. at 963-64 (Alito, J., concurring) (“In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.”).
100 See City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (assuming but not holding that individuals have a reasonable (continued...)}
developing privacy rules when technology is in flux, with some Justices preferring that legislatures, rather than the courts, take the lead role. This is not to say that this approach is ineffective: this case-by-case approach allows the courts to formulate rules more cautiously based on concrete facts in an adversarial setting, and reduces the risk of creating rules with potentially unintended consequences.

This hesitancy to confront new technologies head-on might explain the Court’s recent reliance on property rights as the basis for Fourth Amendment decisions, which, incidentally, might boost Fourth Amendment safeguards against UAS surveillance. In Jones, the five-Justice majority led by Justice Scalia rejuvenated a centuries-old property-based theory of the Fourth Amendment by holding that the physical attachment of a GPS device on the undercarriage of a vehicle constituted an invasion of the owner’s “effect” and therefore a Fourth Amendment search. Justice Scalia observed that the Katz reasonable expectation of privacy formula added to, but did not replace, the traditional property-based test. Likewise, in Florida v. Jardines, the Court relied on this property theory in holding that the government’s use of a trained police drug dog to investigate an individual’s home and its immediate surroundings was a “search.” Depending on the flight path of the aircraft, and the height at which it is operating, this property theory might be employed to hold that flying a UAS onto someone’s property with the intent to obtain information is a Fourth Amendment search for which a warrant would be required.

Privacy Torts

Like the Fourth Amendment, a body of laws collectively known as “privacy torts” might create safeguards against privacy invasions by both public- and private-actor use of unmanned aircraft. While some have held up privacy torts as proof that the existing body of case law is sufficient to regulate privacy issues arising from UAS operations, others have asserted that such laws would provide minimal protection from drone surveillance, at least while in public.

(...continued)

expectation privacy in electronic communications).

101 Id. at 759 (“The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”).

102 Jones, 132 S. Ct. at 945 (Alito, J., concurring in the judgment) (“In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.”) (internal citation omitted).

103 Jones, 132 S. Ct. at 949.


105 See John Villasenor, Observations from Above: Unmanned Aircraft Systems and Privacy, 36 Harv. J. L. & Pub. Pol’y 457, 501 (2013) (“Although privacy expectations are greatly reduced outside the home, the non-governmental use of a UAS to capture images and other information taken while the individual is in a public setting could nonetheless constitute an invasion of privacy.”).

106 See Senate Hearing, supra note 3, at 71 (statement of Ryan Calo, Professor, University of Washington School of Law) (“[T]here are even fewer limitations on the use of drones by individuals, corporations, or the press. The common law privacy torts such as intrusion upon seclusion tend to track the constitutional doctrine that there should be no expectation of privacy in public.”).
The genesis of the modern privacy tort sprung from the pens of Justice Louis Brandeis and Samuel Warren in their law review article "Right to Privacy." There, they espoused the view that privacy could form the underpinning of civil liability absent other physical or tortious conduct. This new tort was later broken down into four discrete torts and included in a set of model rules intended for adoption by the states: (1) intrusion upon seclusion; (2) appropriation of one's name or likeness; (3) publicity given to private life; (4) publicity placing person in false light. Of these four, the first and third will likely prove the most applicable to UAS surveillance.

The tort of intrusion upon seclusion, which may vary in its details from state to state, generally provides, "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." This tort applies a "reasonable person standard"—that is, it tests whether a person of "ordinary sensibilities" would be offended by the alleged invasion. Likewise, the intrusion must not only be offensive, but "highly offensive," or as one court put it, "outrageously unreasonable conduct." Generally, a single incident will not suffice; instead, the intrusion must be "repeated with such persistence and frequency as to amount to a course of hounding" and "becomes a burden to his existence...." However, in a few cases a single intrusion was adequate. The invasion of privacy must be intentional, meaning the defendant must desire that the intrusion would occur, or, as with other torts, know with a substantial certainty that such an invasion would result from his actions. An accidental intrusion is not actionable. Finally, in some states, the intrusion must cause mental suffering, shame, or humiliation to permit recovery.

The tort "publicity given to private facts" provides, "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Like the intrusion upon seclusion tort, publicity given to private facts focuses on publicity given to an individual's private, as opposed to public, life. As the comments to the model rules observe, a person cannot complain of someone taking his photograph while walking down the street, but when a photograph is taken without his consent in a private place, and then subsequently published, he will have a valid publicity

---

108 RESTATEMENT (SECOND) OR TORTS §§652B-652E.
109 Id. §652B.
111 RESTATEMENT (SECOND) OF TORTS §652B (emphasis added).
113 RESTATEMENT (SECOND) OF TORTS §652B cmt. d.
115 RESTATEMENT (SECOND) OF TORTS §652B.
118 RESTATEMENT (SECOND) OF TORTS §652D.
119 See id. at cmt. b.
claim. Unlike the intrusion tort, publicity given to private life requires that the information be made available to the public at large, and furthermore, generally prohibits claims that involve matters that are of legitimate public concern.

Under current law, the location of the target of the surveillance largely controls whether someone has a viable claim for both intrusion upon seclusion and publicity given to private life, and this is likely to hold true with drone surveillance. For the most part, using a drone to peer inside the home of another—whether looking through a window or utilizing extra-sensory technology such as thermal imaging—would likely satisfy the intrusion tort, and if photographs were taken and subsequently published, that person would also likely have a claim for publicity given to private life.

The likelihood of a successful claim is significantly diminished, however, if the surveillance is targeted at individuals in a public space, or even while on private property so long as they could be viewed from a public vantage point. Take, for instance, the suit brought by Aaron and

---

120 Id.
121 Id. at cmt. a. d.
123 See Schifano v. Green County, 624 So. 2d 178 (Ala. 1993) (dismissing claim against race track operators who took picture of plaintiffs in winner’s circle); Fogel v. Forbes, 500 F. Supp. 1081, 1084, 1087 (E.D. Pa. 1980) (dismissing claim for photographs taken at airport); Tellado v. Time-Life, 643 F. Supp. 904, 907 (D.N.J. 1986) (dismissing claim for photographs taken on battlefield in Vietnam); International Union v. Garner, 601 F. Supp. 187, 191-92 (M.D. Tenn. 1985) (dismissing claim for photographing license plates); Tedeschi v. Reardon, 5 F. Supp. 2d 40, 46 (D. Mass. 1998) (same); Jackson v. Playboy Enterprises, Inc., 574 F. Supp. 30, 33 (S.D. Ohio 1983) (dismissing claim for photographing person on sidewalk); see also RESTATEMENT (SECOND) OF TORTS §652B cmt. c (commenting that there is generally no liability for photographing or observing a person while in public “since he is not then in seclusion, and his appearance is public and open to the public eye.”); William M. Prosser, Privacy, 48 CAL. L. REV. 383, 392 (1960) (“On the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of his privacy to do no more than follow him about. Neither is it such an invasion to take a photograph in such a place, since this amounts to nothing more than making a record, not differing essentially from a full written description, of a public sight which anyone present would be free to see.”). There have been some successful claims for intrusion upon seclusion involving surveillance conducted in public, see Kramer v. Downey, 684 S.W. 2d 524, 525 (Tex. Ct. App. 1984) ("[W]e now hold that the right to privacy is broad enough to include the right to be free of those willful intrusions into one's personal life at home at work which occurred in this case."); Daily Times Democrat v. Graham, 276 Ala. 380, 381 (1964); Huskey v. National Broadcasting Co., Inc., 632 F. Supp. 1282, 1285 (N.D. Ill. 1986); see also RESTATEMENT (SECOND) OF TORTS §652B cmt. c ("Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze, and there may still be invasion of privacy when there is intrusion upon these matters."); although this is limited to highly embarrassing situations and appears to be the exception rather than the norm. See Jennifer R. Scharf, "Shooting for the Stars: A Call for Federal Legislation to Protect Celebrities' Privacy Rights," 3 BUFL. INT’L PROP. L. 164, 183 (2006) ("Modifying intrusion to apply in public places would be necessary in order to provide any relief.").
124 See McClain v. Boise Cascade Corp., 271 Or. 549, 556 (1975) (dismissing claim where insurance investigator's entered property to take photographs of plaintiff); Mojica Escobar v. Rosa, 926 F. Supp. 30, 32-33 (D.P.R. 1996) (dismissing claim against newspaper for photographing outside of home); GTE Mobiletel of South Texas, LTD Partnership v. Pascouet, 61 S.W. 3d 599, 605 (Tex. Ct. App. 2001) (dismissing claim against company for cell tower workers looking onto property when they serviced nearby cell tower); Alsenson v. American Broadcasting Co., 220 Cal. App. 3d 146, 162-63 (1990) (holding that broadcast of plaintiff while in his driveway and car was not an intrusion upon seclusion); Welling v. Columbia Broadcasting System, 721 F.2d 506, 509 (5th Cir. 1983) (holding that broadcast of the outside of plaintiff’s home taken from public street was not an invasion of privacy); Munson v. Milwaukee Bd. of School Directors, 969 F.2d 266, 271 (7th Cir. 1992) (same).
Christine Boring against Google for photographs taken of their home and subsequently published online as part of Google’s Street View program. 125 To create this program, Google employees attach panoramic cameras to their vehicles and drive around taking photographs of areas along the streets. The Borings, who live on a posted private road, discovered that Google had taken photographs of their private residence and swimming pool from their driveway. The Borings sued, among other claims, for intrusion upon seclusion and publicity given to private facts. Both claims were dismissed by the district court. On appeal, the Third Circuit Court of Appeals affirmed the dismissal on both counts, holding that the photographs failed to meet the “highly offensive” standard required under both privacy torts. The court found that “no person of ordinary sensibilities would be shamed, humiliated, or have suffered mentally as a result of a vehicle entering in his or her ungated driveway and photographing him or her from there.” 126 The view of the Borings’ house, pool, and driveway could “be seen by any person who entered onto their driveway, including a visitor or a delivery man.” 127 Recording someone with a drone in a public place or even on private property that can be viewed from a public vantage point, as in the Google Street View case, would likely not constitute an invasion under either of these privacy torts.

Executive Branch

In addition to the courts, the executive branch is likely to play a significant role in regulating the privacy implications of UAS operations. Although the FAA has attempted to focus on safety and other regulatory issues, privacy remains a perennial topic for the FAA as it leads the federal government’s UAS integration efforts. Some have posited that instead of the FAA, other executive branch agencies, such as DHS and DOJ, should take the lead role in overseeing the privacy implications of their own unmanned operations. 128 President Obama recently issued a new memorandum taking a similar approach, directing all federal agencies to evaluate the privacy impact of their UAS operations and developing policies to mitigate such concerns.

FAA—Privacy Rules at the Test Sites and Beyond

In FRMA, Congress charged the FAA with integrating UAS into the national airspace. 129 Since passage of this legislation, the FAA has become the center of debate on the privacy implications of these new aircraft. Some in the industry and law enforcement have questioned FAA’s authority to regulate privacy at all, arguing that it is both outside its expertise and its legislative grant of authority. 130 Others have argued that precisely because the FAA is charged with integrating UAS

---

126 Id. at 279.
127 Id.
128 Senate Judiciary Hearing, supra note 3, at 51 (answer from Michael Toscano, President and Chief Executive Officer, Association of Unmanned Vehicle Systems International).
130 See, e.g., Press Release, Association for Unmanned Vehicle Systems International, AUVSI to FAA: Focus on your Mission, Proceed with UAS Integration (Nov. 28, 2012) (“As an industry, we support a continued, civil dialogue on privacy, but any such conversations should take place concurrent with the integration. The selection process for the six test sites are a separate issue and should be treated as such. Meanwhile, the FAA should adhere to its mission and do what it does best – focus on the safety of the U.S. airspace – while other, more appropriate institutions consider privacy issues.”), available at http://www.auvsi.org/AUVSINews/AssociationNews.
that it must resolve one of the most pressing issues involved with such integration—privacy.\footnote{See Keith Laing, Markey: FAA Drone Plan ‘Falls Far Short,’ THE HILL (Nov. 7, 2013), available at http://thehill.com/policy/transportation/189603-markey-faa-drone-plan-falls-far-short; Electronic Frontier Foundation, The FAA Creates Thin Privacy Guidelines for the Nation’s First Domestic Drone “Test Sites,” (Dec. 10, 2013), available at https://www.eff.org/deeplinks/2013/12/efa-creates-thin-privacy-guidelines-nations-first-domestic-drone-test-sites.} As a general matter, the FAA has stated that its “mission does not include developing or enforcing policies pertaining to privacy or civil liberties,”\footnote{See FEDERAL AVIATION ADMINISTRATION, INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS (UAS) IN THE NATIONAL AIRSPACE SYSTEM (NAS) ROADMAP 11 (Nov. 7, 2013), available at https://www.faa.gov/aus/legislative_programs/aus_roadmap/media/UAS_Roadmap_2013.pdf.} but several of its obligations in FMRA have kept the FAA enmeshed in this privacy debate.

The first such obligation was FMRA’s mandate that the FAA establish six test sites to help facilitate the integration of UAS into the national airspace. Neither the program requirements nor the list of attributes for selecting the test sites expressly granted the FAA authority to regulate privacy, or even mentioned “privacy” as a general matter of consideration.\footnote{P.L. 112-95, §332(c), 126 Stat. 73-4 (2012).} Nonetheless, the FAA sought public comment on a proposed privacy policy for UAS operations at the sites on February 22, 2013, and issued a final rule on November 14, 2013.\footnote{Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 68360 (Nov. 14, 2013).} The privacy rules, which are contained as a provision in the contracts (known as an “Other Transaction Agreement,” or OTA) between the FAA and each site operator include the following requirements: (1) operations at the test sites must adhere to existing federal, state, and local laws regarding an individual’s right to privacy; (2) the test site operator must develop a publicly available privacy policy that is informed by the Fair Information Practice Principles (a generally accepted set of rules that regulate how data should be stored, used, and disseminated); (3) the site operator must maintain a record of all UAS operating at the test site; and (4) the site operator must require each UAS operator to have a written plan for the operator’s use and retention of data collected by the UAS.\footnote{Id. at 68,364.} The authority to create these rules was purportedly under the FAA’s contracting authority and not its general statutory authority.\footnote{Id. at 68,361 (“The FAA’s authority for including the Final Privacy Requirements in the Test Site OTAs is set forth in 49 U.S.C. §106(f)(6). That statute authorizes the FAA Administrator to enter into an OTA ‘on such terms and conditions as the Administrator may consider appropriate.’ The FAA believes that it is appropriate to comply with the Final Privacy Requirements.”).} Although the FAA retains the authority to rescind an OTA for a site operator in violation of existing privacy laws, ultimately, this privacy policy signals a hands-off approach, leaving the policing of privacy rules to private parties affected by operations at the test sites, to the test site operators themselves, and to local and state government bodies that oversee the test site operators.\footnote{Id. at 68,632 (“The FAA believes that Test Site operators will be responsive to local stakeholders’ privacy concerns and will develop privacy policies appropriately for each Test Site. ... The FAA expects that [the test site operators] will be responsive to stakeholders concerns.”).}

Despite this relatively passive approach to privacy at the test sites, the FAA has recognized the political and legal importance of privacy in both its proposed small UAS rule and its various planning documents required under FMRA. On February 15, 2015, the FAA issued its proposed operating requirements to allow small UAS (less than 55 pounds) to operate for non-hobby or non-recreational purposes.\footnote{Notice of Proposed Rulemaking, Operation and Certification of Small Unmanned Aircraft Systems, Federal}
beyond the scope of this rulemaking." However, the FAA also noted it would participate in the "multi-stakeholder engagement process" (described below) to assist in a privacy framework concerning commercial and private use of drones. Also, in its five-year roadmap required under FMRA, the FAA noted that while its primary mission "does not include developing or enforcing policies pertaining to privacy or civil liberties, experience with the UAS test sites will present an opportunity to inform the dialogue ... concerning the use of UAS technologies and the areas of privacy and civil liberties." Likewise, in its Comprehensive Plan, also required under FMRA, the FAA devoted a whole section to highlighting the privacy and civil liberties concerns that all federal agencies must take into account as UAS are integrated into the national airspace. While safety will undoubtedly remain the top priority of FAA officials as it navigates the difficult task of integrating drones in the national airspace, with its prominent role of testing and licensing both government, commercial, and private use of drones, it will remain a significant voice in the ongoing privacy debate.

President's Memorandum on UAS and Privacy

On February 15, 2015, the same day the FAA issued its proposed small UAS rule, President Obama issued a memorandum entitled "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems." This presidential memorandum establishes two new frameworks relating to the potential privacy implications of drone operations by both government and private actors.

UAS Policies and Procedures for Federal Government Use

The memorandum first observes that all operations conducted by federal agencies must comply with the Constitution, federal law, and other applicable regulations and policies, an obligation to which agencies are already subject. The memorandum requires that, prior to deployment of new UAS technology and at least every three years, all federal agencies must "examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected." Agencies that collect information through UAS shall ensure their policies and procedures adhere to the following requirements:

(...continued)


139 Id. at 36.


142 Presidential Memorandum, supra note 2.

143 Beyond privacy, the President's memorandum requires that agencies shall ensure they have policies in place that prohibit the collection, use, retention, and dissemination of data in a manner that would violate the First Amendment or would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law. See Presidential Memorandum, supra note 2.
(i) **Collection and Use.** Agencies must only collect information using UAS, or UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose.

(ii) **Retention.** Information collected using UAS that may contain PII [personally identifiable information] shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.

(iii) **Dissemination.** UAS-collected information that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements.

To ensure accountability, the memorandum requires, among other things, that agencies develop protocols for receiving, investigating, and addressing potential privacy complaints; ensure they have rules of conduct and training for federal government personnel and contractors; establish meaningful oversight of individuals who have access to sensitive information collected by UAS; develop policies and procedures to authorize the use of UAS in response to a request for UAS assistance of federal, state, tribal, or territorial government operations; and ensure that local entities that purchase UAS through federal funding have policies in place to safeguard privacy and civil liberties prior to expending such funds.

To promote transparency, the memorandum requires agencies to provide notice to the public regarding where the agency’s UAS are authorized to operate; keep the public informed about the agency’s UAS program as well as changes that would significantly affect privacy; and make available to the public, on an annual basis, a general summary of the agency’s UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to state, local, tribal, or territorial governments.

The agencies must report to the President within 180 days from the date of the issuance of the memorandum with a status on the implementation of these policies and procedures, and must make these policies publicly available within one year.

**Multi-Stakeholder Engagement Process for Commercial and Private UAS Use**

The President’s memorandum also charges the Department of Commerce, through the National Telecommunications and Information Administration (NTIA), to initiate “a multi-stakeholder engagement process to develop a privacy framework regarding privacy, accountability, and transparency for commercial and private UAS use.”\(^{144}\) The end result is expected to be a set of voluntary best practices for privacy issues implicated by commercial and private UAS use.

---

\(^{144}\) Presidential Memorandum, *supra* note 8.
Privacy Impact Assessments and Privacy Working Groups

Prior to the President’s memorandum, several federal agencies had taken steps to assess and address the privacy impacts of their UAS operations. In September 2013, DHS’s Chief Privacy Officer, in conjunction with CBP’s Office of Air and Marine, issued a Privacy Impact Assessment (PIA) primarily evaluating the privacy impact of its operations at the U.S. border.\footnote{Privacy Impact Assessment, supra note 29.} This was prompted, in part, by statutory obligations under federal law.

Under the E-Government Act of 2002, federal agencies must conduct a PIA before (1) “developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form”; or (2) “initiating a new collection of information that will be collected, maintained, or disseminated using information technology ... [and] includes information in an identifiable form permitting the physical or online contacting of a specific individual.”\footnote{44 U.S.C. §3501 (note).} Specific to the Department of Homeland Security, under the Homeland Security Act of 2002, DHS must conduct PIAs “of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected.”\footnote{6 U.S.C. §142.} More generally, the Privacy Officer of DHS is required to coordinate with the Officer for Civil Rights and Civil Liberties to ensure that “(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and (B) Congress receives appropriate reports on such programs, policies, and procedures.”\footnote{6 U.S.C. §142(a)(5).}

DHS’s PIA evaluated the various uses of UAS in DHS’s operations, including its operations at the border, and concluded that such operations have minimal privacy impact. Because current DHS operations limit flights to an altitude of 19,000 feet, the report noted that cameras on UAS do not permit the operator to specifically identify people on the ground nor do they use technology that sees through walls or collects information regarding the interior of buildings. The report noted that personally identifiable information (PII) is generally not retrieved, but that images may later be associated with specific individuals if they are apprehended and the surveillance feed is associated with them. Acknowledging that UAS can stay in flight longer than traditional aircraft, the report concludes that the privacy impact of this technological difference is mitigated by various safeguards including well-defined flight operations, restrictions on accessing collected data, and security protocols for storing data. It is likely that DHS will utilize this PIA when developing any new policies and procedures required by the President’s new memorandum.

In addition to PIAs, in late 2012, DHS’s Office for Civil Rights and Civil Liberties and its Privacy Office spearheaded the “Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department’s Use and Support of Unmanned Aerial Systems.”\footnote{Dep’t of Homeland Security, Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department’s Use and Support of Unmanned Aerial Systems (Sept. 14, 2012), available at https://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information-memorandum-09142012.pdf.} The working group was intended to assess all active and planned uses of UAS by the various components of DHS and flag any privacy or civil liberties issues potentially raised by such operations. The goal
was to develop a set of best practices for safeguarding these various legal interests, and it was reported in September 2014 that such a document would be out by the end of 2014.\textsuperscript{150} DHS has yet to release this best practices document. It may be that this document will be subsumed into the larger obligations placed on DHS through the President’s new memorandum.

**DOJ Inspector General UAS Report**

There has been some debate within DOJ concerning the extent to which unmanned aerial surveillance differs from manned aerial surveillance, and whether these differences warrant new rules for deploying UAS in law enforcement operations. A report issued by DOJ’s Office of Inspector General explained that both the FBI and ATF did not see a practical difference in how UAS collect evidence as compared to their manned counterparts.\textsuperscript{151} As such, these entities did not see a need to develop specialized UAS privacy protocols. DOJ’s Inspector General disagreed with the assessment of the FBI and ATF and concluded the following in its interim report:

> We found that the technological capabilities of UAS and the current, uncoordinated approach of DOJ components to UAS use may merit the DOJ developing consistent, UAS-specific policies to guide the proper use of UAS. Unlike manned aircraft, UAS can be used in close proximity to a home and, with longer-lasting power systems, may be capable of flying for several hours or even days at a time, raising unique concerns about privacy and the collection of evidence with UAS. Considering that multiple components are using or have the potential to use UAS, we believe the Office of the Deputy Attorney General (ODAG), which has the primary responsibility within DOJ for formulating cross-component law enforcement policies, should consider the need for a DOJ-wide policy regarding UAS uses that could have significant privacy or other legal implications.\textsuperscript{152}

This conclusion that unmanned operations pose a unique and potentially greater privacy threat than manned operations mirrors that of the President’s new memorandum on UAS operations. Even when DOJ, like all other federal agencies using UAS, adopts specific policies and procedures addressing the privacy impact of its UAS operations, this inevitably prompts the question whether federal agencies should be left to police their own surveillance activities. While praising the White House drone memorandum as “an important and welcome step in advancing drone technology,” one commentator noted that the memo itself “does not establish strong privacy and transparency drone standards for agencies, leaving it up to the agencies to develop these standards.”\textsuperscript{153} He continues: “Because the memo’s requirements are not specific, the drone policies the agencies set for themselves will be key to how individuals’ privacy is actually protected. Congress still has a role to play in setting strong privacy and transparency standards for drone use.”\textsuperscript{154}

\textsuperscript{151} DOJ Inspector General Report, supra note 33, at ii.  
\textsuperscript{152} Id.  
\textsuperscript{153} Harley Geiger, White House Drone Memo Right to Focus on Privacy, Center for Democracy and Technology (Feb. 15, 2015), available at https://cdt.org/press/white-house-drone-memo-right-to-focus-on-privacy/.  
\textsuperscript{154} Id.
Congress

Several measures were introduced in the 113th Congress that would have restricted both public- and private-actor domestic UAS operations, and reintroduction of these bills is likely in the 114th Congress. The proposed regulations in these bills range from warrant requirements for law enforcement operations to comprehensive data collection and minimization statements to privacy-tort-like prohibitions against private-actor intrusions. Additionally, Congress has utilized its oversight authority to hold hearings and probe executive branch agencies to disclose when and where they are using drones and the potential privacy implications of such uses.

Legislation

Drone Aircraft Privacy and Transparency Act of 2013 (S. 1639, H.R. 2868)

In the 113th Congress, Senator Ed Markey and Representative Peter Welch introduced nearly identical legislation entitled the Drone Aircraft Privacy and Transparency Act of 2013 (S. 1639, H.R. 2868). These bills would have amended FMRA to create a comprehensive scheme to regulate both government and private-actor use of drones, including data collection requirements, a warrant requirement for law enforcement, and various enforcement mechanisms.

First, these bills would have required the Secretary of Transportation, with input from the Secretary of Commerce, the Chairman of the Federal Trade Commission, and the Chief Privacy Officer of the Department of Homeland Security, to study any potential threats to privacy protections posed by the introduction of drones in the national airspace. They would have prohibited the FAA from issuing a license to operate a drone unless the application included a “data collection statement.” This statement would have had to include a list of individuals who would have the authority to operate the drone; the location in which the drone would be used; the maximum period it would be used; and whether the drone would be collecting information about individuals. If the drone would be used to collect personal information, the statement would have had to provide the circumstances in which such information would be used; the kinds of information collected and the conclusions drawn from it; the type of data minimization procedures to be employed; whether the information would be sold, and if so, under what circumstances; how long the information would be stored; and the procedures for destroying irrelevant data.

The statement also would have had to include information about the possible impact on privacy protections posed by the operation under that license and steps to be taken to mitigate this impact. Additionally, the statement would have had to include the contact information of the drone operator; a process for determining what information had been collected about an individual; and a process for challenging the accuracy of such data. Finally, the FAA would have been required to post the data collection statement on the Internet.

In addition to the data collection statement, any law enforcement agency which operates a drone would have had to file a “data minimization statement” with the FAA. This statement would have required adoption of policies by the agency that minimize the collection of information and data unrelated to the investigation of a crime under a warrant; required the destruction of data that is

no longer relevant to the investigation of a crime; established procedures for the method of such
destruction; and established oversight and audit procedures to ensure the agency operates a UAS
in accordance with the data collection statement filed with the FAA.

S. 1639 and H.R. 2868 would have provided several enforcement mechanisms. First, the FAA
could have revoked a license of a user that did not comply with these requirements. The Federal
Trade Commission would have had the primary authority to enforce the data collection
requirements. Additionally, the Attorney General of each state, or an official or agency of a state,
would have been empowered to file a civil suit if there was reason to believe that the privacy
interests of residents of that state had been threatened or adversely affected. These bills would
have also created a private right of action for a person injured by a violation of this legislation.

These bills would also have prohibited a governmental entity from using a drone, or obtaining
information from another person using a drone, for protective activities, or for law enforcement or
intelligence purposes, except with a warrant. This prohibition would not apply in “exigent
circumstances,” which was defined to mean imminent danger of death or serious physical injury
or high risk of terrorist attack as determined by the Secretary of Homeland Security.

**Preserving Freedom from Unwarranted Surveillance Act of 2013 (S. 1016, H.R. 972)**

Senator Rand Paul and Representative Austin Scott’s companion bills, the Preserving Freedom
from Unwarranted Surveillance Act of 2013 (S. 1016, H.R. 972), would have focused exclusively
on government drone operations.\(^{156}\) These bills would have required any entity acting under
the authority of the federal government to obtain a warrant based upon probable cause before
conducting drone surveillance to investigate violations of criminal law or regulations. S. 1016 and
H.R. 972 included several exceptions to this warrant requirement: (1) when necessary to prevent
or deter illegal entry of any persons or illegal substances into the United States; (2) when a law
enforcement officer possesses reasonable suspicion that under particular circumstances “swift
action to prevent imminent danger to life or serious damage to property, or to forestall the
imminent escape of a suspect, or destruction of evidence” is necessary; or (3) when the Secretary
of Homeland Security determines credible intelligence indicates a high risk of a terrorist attack by
a specific individual or organization. H.R. 972 would have created a right to sue for any violation
of its prohibitions. Unlike H.R. 972, S. 1016 included an express exclusionary rule for evidence
obtained in violation of the act.

**Preserving American Privacy Act of 2013 (H.R. 637)**

Representative Ted Poe introduced the Preserving American Privacy Act of 2013 (H.R. 637),
which would have regulated both public and private use of drones under various mechanisms.\(^{157}\)
As to law enforcement use, H.R. 637 would have created a general prohibition on the use of
drones to collect covered information or disclose covered information so collected. “Covered
information” was defined as “information that is reasonably likely to enable identification of an

---


\(^{157}\) H.R. 637, 113\(^{th}\) Cong. (2013).
individual” or “information about an individual’s property that is not in plain view.” This prohibition was subject to the following exceptions: (1) law enforcement obtains a court-issued warrant and serves a copy of the warrant on the target of the search within 10 days of the surveillance. However, notice need not be provided if it would jeopardize an ongoing criminal or national security investigation. (2) Law enforcement obtains a court-issued order based upon “specific and articulable facts showing a reasonable suspicion of criminal activity and a reasonable probability” that the operation “will provide evidence of such criminal activity.” The order may authorize surveillance in a stipulated public area for no more than 48 hours which may be renewed for a total of 30 days. Notice of the operation must be provided to the target no later than 10 days after the operation. Alternatively, notice may be provided not less than 48 hours before the operation in a major publication, on a government website, or with signs posted in the area of the operation. (3) Operation is within 25 miles of national border. (4) The targeted individual has provided prior written consent. (5) Emergency situation involves danger of death or serious physical injury, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime, where a warrant cannot be obtained with due diligence. Law enforcement must then obtain a warrant within 48 hours of such operation. Any evidence obtained in violation of this act would not have been admissible in any trial or adjudicative proceeding.

Additionally, H.R. 637 would have required any governmental entity applying for a certificate or license to operate a UAS to also file a data collection statement with the Attorney General, which would have included the purpose for which the UAS will be used; whether the UAS is capable of collecting covered information; the length of time the information will be retained; a point of contact for citizen feedback; the particular unit of governmental entity responsible for safe and appropriate operation of the UAS; the rank and title of the individual who may authorize the operation of the UAS; the applicable data minimization policies barring the collection of covered information unrelated to the investigation of crime and requiring the destruction of covered information that is no longer relevant to the investigation of a crime; and applicable audit and oversight procedures.

Under H.R. 637, the Attorney General would have been empowered to request that the Secretary of Transportation revoke the license or certificate of any entity that fails to file a data collection statement. Further, H.R. 637 contained a provision permitting administrative discipline against an officer who intentionally violates a provision of this act.

H.R. 637 would also have made it unlawful to intentionally operate a private UAS to capture images in a manner highly offensive to a reasonable person where the person is engaging in a personal or familial activity under circumstances in which the individual has a reasonable expectation of privacy, regardless of whether there is a physical trespass.158

**Oversight**

In addition to its authority to enact federal law, Congress can and has utilized its oversight function to shape the debate surrounding the privacy implications of drone surveillance. For instance, both the Senate and House Judiciary Committees held hearings in the 113th Congress specifically addressing the privacy impact of drone operations. Additionally, individual members probed executive branch officials on when and where they were using drones and the potential

---

privacy implications of such uses. One such example of this oversight function is demonstrated by correspondence between the Senator Rand Paul and the FBI in the summer of 2013. In a July 25, 2013, letter to FBI Director Mueller, Senator Paul asked how the Bureau defined “reasonable expectation of privacy” in the context of UAS surveillance, as Paul feared that “an overbroad interpretation of this protection would enable more substantial information collection on an individual in a circumstance they might not have believed was subject to surveillance.”159 The FBI responded by arguing that based on the Supreme Court’s three aerial surveillance cases from the 1980s, it need not obtain a warrant for any surveillance “open to public view” and that the “Fourth Amendment principles applicable to manned aerial surveillance discussed in these cases apply equally to UAVs.”160 Similar oversight is likely to continue in the 114th Congress.

States

Justice Brandeis once observed that “it is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.”161 Some have argued that under this theory of federalism, the states are best situated to experiment with various UAS policies to determine the most appropriate legal framework for their state.162 Others have countered that applying a patchwork of 50 different privacy regimes would be overburdensome on both public and private users of UAS. According to the National Conference of State Legislatures (NCSL), by the end of 2014, 20 states had enacted laws addressing UAS issues.163

State laws in this area have mainly come in three forms. The first, and perhaps most numerous, are laws that create broad prohibitions on their own state law enforcement entities, subject to various exceptions that differ from state to state.164 These exceptions include obtaining a warrant based upon probable cause; countering a high risk of terrorist attack; responding to threats of imminent harm of human life; locating a missing person; and conducting crime scene and traffic photography, among others. The second category relates to use restrictions of data collected by UAS. For instance, Illinois requires law enforcement to destroy all information gathered by a UAS within 30 days of collection unless there is reasonable suspicion that the information contains evidence of criminal activity or the information is relevant to an ongoing criminal investigation.165 While the relevancy standard is a very low evidentiary threshold, it does prevent limitless retention of private data. Similarly, Alaska prohibits the retention of records collected by drones unless it is required as part of an investigation or prosecution, is used for training purposes, or is required by federal or state law.166 Images that are retained under Alaska’s statute are considered confidential and not subject to the state’s public records laws. The third category

162 See Bennett, supra note 12; Kaminski, supra note 12.
164 See, e.g., ALASKA STAT. §18.65.902; FLA. STAT. ANN. §934.50.
165 725 ILL. COMP. STAT. §167/20.
166 ALASKA CODE §18.65.902.
relates to regulation of private actors, generally through the creation of private causes of action for privacy invasions caused by UAS surveillance. For instance, Idaho prohibits recording individuals on their residence without their consent, or from photographing an individual for the purpose of publishing or otherwise publicly disseminating such photograph no matter where the target is located.\textsuperscript{167} Undoubtedly, this third category of proposals creates tension between the public’s First Amendment right to gather news and the individual privacy interests at stake, requiring legislatures to fine tune this balance when enacting UAS legislation.

**Author Contact Information**

Richard M. Thompson II  
Legislative Attorney  
rthompson@crs.loc.gov, 7-8449

\textsuperscript{167} \textit{Idaho Code} §21-213.
ARTICLES

THE FOURTH AMENDMENT FUTURE OF PUBLIC SURVEILLANCE: REMOTE RECORDING AND OTHER SEARCHES IN PUBLIC SPACE

MARC JONATHAN BLITZ

Public video surveillance is changing the way police fight crime and terrorism. This was especially clear in the aftermath of the Boston Marathon bombing when law enforcement found images of the two suspects by analyzing surveillance images gathered by numerous public and private cameras. Such after-the-fact video surveillance was equally crucial to identifying the culprits behind the 2003 London subway bombing. But the rise of camera surveillance, as well as the emergence of drone-based video monitoring and GPS-tracking methods, not only provides an important tool for law enforcement, but also raises challenges for constitutional law. As police gain the ability to technologically monitor individuals’ public movements and activities, does the Fourth Amendment’s prohibition against “unreasonable searches” place any hurdles in their way?

In the 2012 case, United States v. Jones, five justices, in two separate concurring opinions, signaled that it does—at least when the monitoring becomes too intense or prolonged. Their suggestion, however, raises two significant problems. First, it provides no principled basis for marking the point at which public surveillance morphs from a means by which police monitor public space into a Fourth Amendment “search.” Under the “mosaic theory” embraced by the D.C. Circuit, such surveillance becomes a search only when it captures enough detail to reveal that an individual’s public life to construct a detailed picture (or “mosaic”) of her movements and associations. But how detailed may such a picture be before it is too detailed? Do police engage in a search simply by watching someone continuously, even if they do so without drones, GPS units, or other advanced technology? Second, the concurring opinions do not explain why the Fourth Amendment, if it covers public surveillance of this kind, does not also cover the information-collecting police do when they simply watch a pedestrian or a driver. As Justice Scalia wrote in Jones, “[T]he Court has to date not devoted to the understanding that mere visual observation does not constitute a search.”

This Article proposes a solution to each of these challenges by offering a two-part definition of a Fourth Amendment “search” in a public space. Police engage in a search when they (1) not only observe, but also record, images or sounds of people or events outside police presence; or (2) magnify details on a person or document or other items the person is carrying and thereby reveal information that would not otherwise be apparent without a pat-down or a stop-and-search of a person’s papers or effects.

This technology-based or design-based definition of what constitutes a “search” avoids the problems that arise when the Fourth Amendment analysis regarding what constitutes a “search” is based on an investigation’s duration or intensity. Under the technology-based or design-based definition, police engage in a search as soon as they begin recording remote events or magnifying otherwise invisible details, whether they have done so for minutes or two weeks. Additionally, under this approach, Fourth Amendment constraints only apply to surveillance that goes beyond ordinary visual surveillance. This is more workable and more in accord with Fourth Amendment logic. Recording is a search because, more than any other element of public surveillance, it allows police to engage in dragnet-style investigation of all activities in a public space. By transforming ephemeral occurrences into permanent records, recording allows government officials to search public lives frame by frame, much like they might search documents file by file. Certain types of magnification could also constitute a search because, just as a telescope focused on a home may be functionally equivalent to a home intrusion and search, certain types of magnification may be functionally equivalent to a physical search of persons, papers, or effects.
INTRODUCTION

Public surveillance technology is changing the way police fight crime and terrorism. This was clear in the aftermath of the Boston Marathon bombing when law enforcement quickly found images of the two suspects by "stitching together a mountain of footage" gathered by public and private cameras. It was also clear in the aftermath of the 2005 London subway bombings, when the suspects were quickly identified using video surveillance. Touting these breakthroughs, cities have rushed to embrace camera systems, especially in the years after the 9/11 attacks. Police in Washington, D.C., Chicago, and New York now use camera networks to track a person strolling down the street. They can magnify and video record her movements, actions, and the details of her vehicle's license plate, or the items she is carrying out of a store. In fact, government officials do not have to make do with cameras mounted on lamp posts or buildings. They can watch and record citizens from drones that hover in the skies and glide at the command of a distant operator to a new and better vantage point.

This evolution in surveillance technologies not only provides an important boon for law enforcement. It also raises an important challenge for constitutional law. As police gain the ability to monitor citizens' public movements and activities with increasingly powerful cameras, does the Fourth Amendment's protection against "unreasonable searches" place any hurdles in their way? Do police need to obtain a warrant based on probable cause or to satisfy some other constitutional test of reasonableness before they use a drone to track a person's movements or reconstruct those movements using video footage from public cameras?1


3. See Jeremy Borden, Pin, Tap, Zone: Reversing the Use of Video Surveillance of Public Places, 25 BERKELEY TECH. L.J. 755, 767–68 (2009) (explaining that "police have praised video surveillance as an effective tool" and have increasingly employed more sophisticated surveillance).


5. See William M. Burke, Chicago's Camera Network & Expansions, WALL ST. J. (Nov. 17, 2009), http://online.wsj.com/article/SB12530007897372987539910412921756.html ("A gun web of video-surveillance cameras has spread across Chicago, allowing police in the pursuit of criminals from crime scenes and even from their homes.


7. See, e.g., Chicago's High-Tech Camera System Nears Approval, PROGRESS (Feb. 8, 2011), http://www.progresstimes.com/2011/02/chicago-high-tech-camera-system-

8. See Tom Reavey, UAV Video Surveillance Drivers, Prepped for TakeOff, SECURITY NEWS wire (Feb. 2012), http://www.securitynewswire.com/2012/02/05/uav-video-surveillance-drivers-prepared-for-takeoff/ ("Drivers ... may soon be filling our skies, engaged in myriad video surveillance tasks.

9. For a longer discussion of legal challenges to drone use, see generally Borden, supra note 3.

Only a few years ago, most courts and lawyers would have answered "no." The Fourth Amendment protects people—and their "houses, papers, and effects"—from being subject to "unreasonable searches and seizures" by government officials. Supreme Court Justices as well as legal scholars have generally interpreted this provision as protecting individuals in the home, or some other space that is objectively and reasonably private or personal. The Fourth Amendment bars the government, for example, from spying upon citizens in their living rooms and bedrooms, prying into their wallets, purses, or other closed "containers," and opening sealed envelopes or closed drawers to read their private letters and diaries. More generally, as Justice Harlan emphasized in Katz v. United States, the government generally does not need a warrant any time it watches us, but only when it observes us or examines our belongings after entry into places or circumstances in which we have a "reasonable expectation of privacy.

By contrast, the open and public space that we share with others—in streets, public squares, and parks—is not a private environment. We cannot exclude fellow citizens from this space nor command them to close their eyes and ears to what is going on around them. For example, when a person drives on a highway, she might be seen or even followed by other drivers, and some of these other drivers might be police officers. The Supreme Court held in United States v.

9. See, e.g., United States v. Cuevas-Perez, 649 F.3d 272, 274, 276 (7th Cir. 2011) (holding that GPS surveillance on public roads is not a search); United States v. Carter, 629 F.3d 604, 609, 610 (4th Cir. 2010) (same); United States v. Miranda, 525 F.3d 1212, 1214, 1217 (9th Cir. 2008) (same); United States v. Mares, 525 F.3d 604, 609 (4th Cir. 2008) (same); United States v. DeCesare, 474 F.3d 994, 998 (7th Cir. 2007) (same); United States v. Gonzalez, 329 F.3d 945, 948 (9th Cir. 2003) (explicitly stating that the Fourth Amendment does not protect "eavesdropping already visible to the public.

10. 1 U.S. CONG. 1915. 6.

11. See, e.g., Oliver v. United States, 466 U.S. 170, 184-85 (1984) (finding that, while the Fourth Amendment limits police investigation of homes and the curtilage surrounding the home, it has no application to "open fields"); Ortiz v. S. Kerr, Appleby v. Fourth Amendment to the Kitty. A General Approach. 102 NIUS. L. REV. 1595, 1596 (1980) (explaining that the Fourth Amendment does not protect conduct that is "in the open, unrequited and enclosed space it seems a search.

12. See, e.g., California v. Acevedo, 500 U.S. 502, 503 (1991) (White, J., dissenting) ("Every citizen deserves an interest in the privacy of the contents of her bag, locker, handbag or any other container that conceals personal papers and effects from public scrutiny. That privacy interest has been recognized in cases requiring more than a century."); As explained below, individuals do receive Fourth Amendment protections from searches in the cars, purses, record lockers, or other areas in public space from which they can exclude casual observers; but this does not give them protection from monitoring of their activities in the open. See infra text accompanying notes 93-96.


14. See id. at 508-09 (Holmes, J., concurring).

Knott's example of individuals having no reasonable expectation of privacy in their movement on public roadways. Thus, people cannot raise Fourth Amendment complaints when their actions are open to the public, including law enforcement officers, even if these officers use hidden location-tracking devices or other technology to do so. While people may create some measure of constitutionally protected privacy, even in public spaces, by closing their car doors or keeping documents and other items inside a briefcase, purse, or some other container, people cannot constitutionally shield the actions they leave visible or audible. As one judge said in a recent Global Positioning System (GPS) tracking case: "The practice of using... devices to monitor movements on public roads falls squarely within the Court's consistent teaching that people do not have a legitimate expectation of privacy in that which they... leave open to view by others."

Or so the Supreme Court and other courts insisted—until a year ago. In the 2012 case of United States v. Jones, five Justices, in two separate concurring opinions, indicated that it is time for a doctrinal change. These five Justices suggested that an important constitutional line is crossed—and the constraints of the Fourth Amendment are triggered—when public surveillance becomes too intense or prolonged. Justice Alito, for example, argued that, while "relatively short-term monitoring of a person's movements on public streets" is generally free from Fourth Amendment restriction, "use of longer term GPS monitoring in investigations of most offenses

16. Id. at 281.
17. See id. at 282.
18. See generally J. Sotomayor. (concurring), 505 U.S. 565, 589 (1993) (White, J., dissenting) (restating that all citizens have a clear privacy interest in the contents of personal articles).

20. United States v. Jones, 132 S. Ct. 945 (2012). In this case, the Federal Bureau of Investigation and D.C. Metropolitan Police Department came to suspect a high-level source, Antoine Jones, of drug trafficking and used multiple surveillance measures—including visual surveillance and wiretapping—to gather more information. Id. at 948. The government also obtained a warrant to attach a GPS device, within ten days of the warrant's issuance, to Jones's vehicle while it was in Maryland rather than the District. Id.

21. As stated in 951 (Sotomayor, J., concurring) (noting that the Supreme Court should consider reissuing some of the fundamental premises of Fourth Amendment law in light of technological developments); at 958 (Alito, J., concurring in the judgment) (illustrating that the majority's reasoning was based on an incorrect conception of the Fourth Amendment).

22. Id. at 955 (Sotomayor, J., concurring) (agreeing with Justice Alito that "longer term GPS monitoring constitutes a search in most cases").
impinges on expectations of privacy" and should constitute a Fourth Amendment search.\footnote{23} The justices did not, however, clearly identify how long or how intensively public surveillance must be to cross the constitutional dividing line.\footnote{24} They did not have to do so because the majority opinion relied on a different rationale to require a warrant. The majority emphasized that the installation of a GPS device on a car prior to tracking was a trespass.\footnote{25} Because the Supreme Court did not hold that the tracking of public movements alone violated the Fourth Amendment, it did not need to specify the point at which public tracking may violate the Fourth Amendment.\footnote{26} While this particular instance of public tracking began with a "trespassory" planting of a GPS device,\footnote{27} other kinds of public surveillance—including most forms of video surveillance—do not. The public street cameras that capture a car's movements, or those that do so from a drone hovering overhead, do not require police to touch the car—let alone alter it—to surveil its movements.\footnote{28} When the justices confront a case like this, they may have to clearly delineate the constitutional boundary line between a search and non-search. This Article proposes a way to mark that line. It does not so by asking how long, or how intensely, police focus on a particular person or event, but rather by suggesting a different criterion. Whether public surveillance is a search depends not on duration or the quantity of information gathered by a surveillance method, but rather on that method's nature or design.\footnote{29} More specifically, public

\footnotesize{\textit{The Fourth Amendment Future}}

\footnotesize{27}

\footnotesize{\textit{American University Law Review}}

\footnotesize{28}

\footnotesize{[Vol. 65:21}

\footnotesize{surveillance should count as a search when it takes one of two forms. First, police engage in a Fourth Amendment search, even in public space, when they are not merely observing but also recording images or sounds of people. Additionally, the police must obtain these images and sounds from events and people outside the recording officer's presence. In other words, the government does not conduct a search whenever an officer simply turns on an iPhone camera or a camcorder and then records what is happening in front of him. Rather, a public search occurs when recording technology allows officials to record events that would otherwise not be able to be seen or heard.\footnote{30} Second, a search can also occur in public when police magnify and observe details on a person, or the documents or other items he is carrying, so as to reveal information that would otherwise have been apparent without a pat-down or some other stop-and-search of a person's papers or effects.\footnote{31} Such a technological form-based or design-based test,\footnote{32} avoids the key difficulty that plagued an approach that tried, in Justice Alito's words, to exempt "relatively short-term monitoring of a person's movements" from Fourth Amendment restriction, but places constitutional limits on "longer term GPS monitoring" or other surveillance in public.\footnote{33} It spares the courts the task of seeking some elusive or arbitrary point in the duration or intensity of a search at which such monitoring morphs from being just another means by which police watch over public space into a possible violation of the Constitution.\footnote{34} After police begin recording events outside of their...}
presence, it does not matter whether they do so for two minutes or two weeks. Police engage in a search simply by using technology with the capacity to create a record of people’s movements and aiming it at certain individuals. Defining searches in public spaces in this manner parallels the way that courts typically define Fourth Amendment searches in private spaces. Police are immediately bound by the Fourth Amendment when they enter a person’s house, open up and flip through the pages of a diary, or tap a phone line. These investigations do not become a search only after they have lasted a certain length of time; rather, the search begins with an entry or intrusion, even if the stay or investigation lasts only seconds or minutes. To be sure, the brevity of a search may, in some cases, make it more likely to count as a “reasonable” and permissible search. Nevertheless, brevity alone cannot transform such a search into a non-search that is entirely free from Fourth Amendment restriction. The same should be true of public surveillance technologies that involve remote recording or magnification of details normally invisible without a physical search of a person, her documents, or the items she is carrying. Courts obtain a second advantage by focusing on the nature or design of the investigatory method. The proposed test avoids transforming all police monitoring into a constitutional matter. As Justice Harlan wrote in a 1971 dissent, there is a constitutionally significant difference between monitoring and recording. When the government audio records someone’s words, it does something...

theory," which is a Fourth Amendment approach under which investigatory actions that do not count as a search in isolation count as a search when aggregated).

35. See, e.g., Kello v. United States, 539 U.S. 27, 47 (2002) (“[T]here is certainly no exception to the warrant requirement for the officer who happens to catch the front door and sees nothing but the non-intrusive rug on the vestibule floor.”); Patton v. New York, 465 U.S. 575, 590 (1984) (noting that, except in exigent circumstances, the Fourth Amendment requires police to obtain a warrant as soon as they cross the “line” that marks the entrance to the house).

36. See United States v. Place, 462 U.S. 696, 706 (1983) (stating that searches, no matter how brief, must be based on probable cause).

37. See, e.g., Terry v. Ohio, 392 U.S. 1, 24-25 (1968) (holding that police stop-and-frisk practices, while entailing a search and seizure, require only “reasonable suspicion” and not a warrant or probable cause just because they “invade” the “privacy” of the subject searched).

38. See United States v. White, 401 U.S. 780, 785-86 (Harlan, J., dissenting) (asserting that the plurality ignored the differences between third-party monitoring and recording); see also Christopher Sobogin, Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity, 72 Minn. L. Rev. 215, 270 (2000) (taking note, but expressing doubts, that the Supreme Court would accept the argument that although “we assume the risk that others will view our public conduct, we do not assume the risk that our public actions will be reduced to a photograph or film”).

30 AMERICAN UNIVERSITY LAW REVIEW [Vol. 63:21

far more invasive than simply listening to them. It creates a record that not only is “free of the possibility of error and oversight that inheres in human reporting” but also allows officials to review a person’s life in far more detail than they could if they relied only on the fading memories of listeners.

The lesson of Harlan’s contrast is not that recording requires constitutional oversight simply because it reduces our privacy to a greater extent than mere listening or watching. Rather, it is that recording changes the nature of police surveillance in such a way that it threatens privacy as well as other Fourth Amendment interests more deeply. Consider video recording. Such recording does not necessarily reduce an individual’s privacy at the time it occurs: if no one watches the video footage, as it is recorded or afterwards, then the actions captured in the tape remain just as private as they would be had no one seen or captured them. If an officer does watch the scenes captured by the cameras, then an individual’s privacy is compromised to some extent—but the fact that recording is occurring does not make that officer’s live observation any more intrusive than it would otherwise be.

Even unmonitored recording, however, raises a significant threat to Fourth Amendment purposes. It takes ephemeral occurrences in our lives and transforms them into permanent records. Through recording technology of this sort, the government can scan its collection of footage of any person’s minute-to-minute activities in hopes of finding something incriminating. Recording, in other words, potentially allows the government to track through digital images and audio records in search of evidence that justifies subjecting individuals to state power. Such probing is precisely the kind of dragnet-style investigation that the Fourth Amendment is supposed to restrict—and does restrict at roadblocks and airports.

39. Cf. Klay, 401 U.S. at 787 (Harlan, J., dissenting) (elaborating that thirdparty beeping “undermine[...its] (i.e., confidence and sense of security in dealing with one another that is characteristic of individual relationships between citizens in a free society.”)

40. See id. at 787-89 (indicating that allowing government officials to monitor private conversations through a willing third-party assistant would compromise the insulators discourse “that liberates daily life”).


42. See, e.g., J. Daniels v. U.S. Dist. Court, 477 U.S. 997, 1007 (1986) (Douglas, J., dissenting) (stating that, according to the court’s reasoning, “taping within the State is not illegal” even though it may be “a monstrous abuse of power”).
At such checkpoints, police have limited authority to make suspicionless stops (and searches) to assure safety in these transportation channels. What they may not do under the Fourth Amendment is search for other evidence of crime that such a checkpoint is able to strain out. But a dragnet that catches thousands of travelers or other citizens is not the only kind of sweeping investigatory technique that offends Fourth Amendment purposes. For example, dragnet investigations under which officers rummage through properties or drawers of documents without justification also offend these purposes, even when the hunt for unknown contraband occurs within a single home and focuses on the property of a single homeowner. A government "fishing expedition" should likewise be deemed to be subject to Fourth Amendment constraints when the data that officials sift through comes not from personal documents, but from the trail of data people leave behind in a world in which every action or movement is recorded for potential review at a later date.

To be sure, public surveillance can threaten Fourth Amendment purposes, even when police are not recording what they see. Police can use telescopes or extremely powerful zoom lenses to scrutinize details on a person's clothing, or on items or documents removed from a wallet or briefcase, that would be invisible even to bystanders just a few yards away. Certain courts have suggested that such telescopic magnification would constitute a Fourth Amendment search when pointed at the windows of a home, and if that is true, it is certainly possible that telecope-aided scrutiny should also be a search when it is aimed at the other subjects of Fourth Amendment protection—namely, an individual's "person, . . . papers, and effects." High magnification of a detail on a person or her property may thus, like recording, bring police observation in public onto Fourth Amendment territory.

That such public surveillance is a Fourth Amendment search does not mean that it will always be a Fourth Amendment violation. A search of a house, person, paper, or effect is prohibited by the Fourth Amendment only when it is "unreasonable." Just as police, Federal Bureau of Investigation (FBI) agents, and other law enforcement officials frequently use wiretaps by obtaining a warrant or absent such a warrant when circumstances make a wiretap reasonable, police should be able to capture and examine video records or to closely magnify details of public action when use of these methods count as reasonable.

Part I of this Article discusses why courts have found the Fourth Amendment analysis of public surveillance to be so challenging and describes how they have thus far met this challenge. Part II offers a new test for determining when public surveillance constitutes a search: the government's actions require Fourth Amendment scrutiny when it records remote events or uses an analogous method of investigation, or, in certain instances, when it employs magnification or sound amplification in a public space. Other kinds of police surveillance in public generally are not searches, even if they employ sophisticated technology. Part III explains why this approach is preferable to various alternatives that scholars, and judges themselves, have considered as they have struggled with how Fourth Amendment law should apply in public. In the course of doing so, Part III describes why police officers will be able to use video surveillance technology, even without a warrant, so long as the police meet Fourth Amendment reasonableness standards that assure the technology is not used in a way that unnecessarily diminishes individuals' freedom from state monitoring.

45. See, e.g., City of Indianapolis v. Edmond, 531 U.S. 32, 46-49 (2000) (striking down an unconstitutional road block program under which police investigated each car not only for drunk drivers but also for evidence of drug-related contraband); United States v. Albiero, 452 F.2d 798, 805 (2d Cir. 1971) (expressing concern about "the possibility that the purpose of the aerial search [to prevent terrorism] may degenerate from the original search for weapons into a general search for contraband"); see also infra notes 62-105 and accompanying text.

46. See Andreen v. Maryland, 427 U.S. 403, 480 (1976) (recognizing that the Fourth Amendment forbids "general exploratory rummaging in a person's belongings" (quoting Coolidge v. New Hampshire, 403 U.S. 443, 461 (1971))).

47. See, e.g., United States v. Taborda, 653 F.2d 131, 138-39 (5th Cir. 1981) ("The use of teleoscopic viewing into the interior of a home is thus a risk of observation not only of what the householder should realize might be seen by unattended viewing, but also of immense details of a person's private life, which he legitimately expects will not be observed either by naked eye or enhanced vision.").
I. THE NATURE OF THE PROBLEM AND THE SUPREME COURT'S INITIAL STEPS TOWARD A SOLUTION

A. The Problem of Public Surveillance

Whether public video surveillance is a search may seem deceptively simple. Since 1967, the Supreme Court has adopted the rule from Justice Harlan’s concurrence in Katz, under which the government engages in a Fourth Amendment search any time it intrudes upon an "expectation of privacy . . . that society is prepared to recognize as 'reasonable.'” Members of a free society do not expect to be subject to continuous government surveillance, even as they walk or drive on public pathways. As a result, this kind of surveillance should be subject to constitutional limits. Not only do many Americans share this expectation, but they also likely view it as reasonable and justified, as was clear in the legislative reaction to law enforcement officials’ increasing use of drones. The Florida legislature, for instance, recently enacted a law tightly restricting the use of drone surveillance within the state’s borders: the Freedom from Unwarranted Surveillance Act. Additionally, some U.S. Senators and Congressmen have suggested that federal restrictions might also be justified because, as Senator Chuck Grassley explained, “[t]he thought of government drones buzzing overhead, monitoring the activity of law abiding citizens, runs contrary to the notion of what it means to live in a free society.”

But the task of fitting public surveillance into Fourth Amendment jurisprudence is, for a number of reasons, more challenging than simply taking note of these intuitions. First, there is the line-drawing problem that confronted the concurrence-writers in Jones. While it

56. See, e.g., Christensen v. Caro, 483 F.3d 604, 609 (9th Cir. 2007) (per curiam) (noting that a police officer did not conduct a search under the Fourth Amendment when he "followed (individually) in his own car as they drove through busy traffic on a route between a home and the post office")
57. See, e.g., United States v. Garcia, 680 F.3d 994, 997 (10th Cir. 2012) ("[T]he police followed a car around, observe its route by means of cameras mounted on the hood of a police car")
J r 2  

THE FOURTH AMENDMENT FUTURE 35

Judges are unlikely to provide consistent answers to these questions. This was evident in the case of United States v. Cuestas-Perez, in which the U.S. Court of Appeals for the Seventh Circuit attempted to apply the D.C. Circuit's Fourth Amendment analysis without expressly endorsing it. The majority concluded that Maynard's "mosaic" rule simply did not apply to the facts before it because the police had followed Cuestas-Perez for sixty hours, not for twenty-eight days as in Maynard, and had tracked his movements on a "single journey," rather than on multiple trips. The dissent, by contrast, pointed out that monitoring of the defendant on a "60-hour Odyssey across 1,650 miles" is far from the kind of brief trip that might be too insignificant to require Fourth Amendment constraints.

The problem is that no apparent principle explicates whether, or why, sixty hours is short enough to remain free from Fourth Amendment restraints. After all, if the danger raised by ongoing GPS surveillance is that it allows police to "connect the dots" of a person's movements and draw inferences about her private plans, a sixty-hour period is probably sufficient time to draw such a connection and make inferences based on the data gathered. To take the D.C. Circuit's own example from Maynard, a woman's visit to a baby supply store may certainly come within sixty hours of her visit to a gynecologist; thus, observers will hardly need twenty-eight days, or even a week, to learn details about that woman's life that are unlikely to be apparent to others in public space. This uncertainty about how much police can learn in a day, or a week, also provides reason to question the Virginia Supreme Court's conclusion that Maynard's mosaic theory should not apply to GPS tracking that lasts less than a week. It is not clear that a week-long monitoring period is short enough to avoid the dangers of aggregated information that concerned the D.C. Circuit.

The Fourth Amendment line-drawing challenges courts face in public spaces is, in many ways, analogous to the one that Professor Orin Kerr recently addressed in proposing a Fourth Amendment

regime for Internet communications. As Kerr pointed out, the key problem in determining whether Internet surveillance constitutes a search is that the natural marker that generally delineates what constitutes a Fourth Amendment search in physical space—namely, the distinction between an enclosed, private space and an observable, public environment—does not exist on the Internet. "The distinction between government surveillance inside and government surveillance inside," Kerr writes, "is probably the foundational distinction in Fourth Amendment law because the government does not need any cause or order to conduct surveillance outside," but "entering enclosed spaces ordinarily constitutes a search that triggers the Fourth Amendment." However, the Internet does not fit nicely into this model because there is no outside/inside division to rely upon. Everything on the Internet is considered to be enclosed and inside. Kerr therefore argued that Fourth Amendment law needs a new, functionally equivalent distinction to mark the boundary between searches and non-searches. He proposed that courts should rely on the distinction between content and non-content in e-mails or other Internet communications.

When investigators intercept and read the contents of a person's e-mail, for example, they are conducting a Fourth Amendment search and must first obtain a warrant or otherwise show their search is reasonable. Conversely, when investigators merely want to look at the address information on the e-mail, they are doing the equivalent of looking at the outside of an envelope, not the letter inside, and this monitoring of non-content information is therefore not a Fourth Amendment search. If Internet surveillance raises a Fourth Amendment problem because everything is "inside," public surveillance raises a similar problem because everything is outside. Public surveillance is "public" because it focuses on the outside world and, more specifically, on visible behavior in it. Here too, then, Fourth Amendment law needs

70. See generally Kerr, supra note 11.
71. Id. at 1009-10.
72. Id. at 1010.
73. Id. at 1010-11.
74. Id. at 1011.
75. Id. at 1007-08.
76. Id. at 1009.
77. Id. at 1010; or see also Matthew J. Toksem, The Content/Envelope Distinction in Network Law, 50 WASH. & L. REV. 2115-16 (2005) (proposing, based on case law, the existence of a content/non-content distinction between searches and non-searches in Internet communications).
a replacement for the outside/inside distinction. It needs a new boundary line to demarcate parts of the outside world that deserve to be treated like inside spaces for Fourth Amendment purposes—parts of our life in public that, like our living rooms and bedrooms, deserve to be constitutionally insulated from government scrutiny.

The lack of a replacement for the outside/inside distinction in public space leaves judges without a key resource for determining what counts as a search in public space. Without such a line, it is difficult for courts to pronounce long-lasting public surveillance to be a search on the basis that certain forms of it seem disturbingly intrusive.79 These invasions do not, by themselves, tell us how to distinguish investigations that are invasive enough to require constitutional oversight from those that are not.

There is a second difficulty in treating public surveillance as a search: if courts subject police to significant constitutional limits in monitoring public space, they risk crippling law enforcement’s efforts to do what it is charged with doing. Police are not only generally as free as other citizens to watch the streets they patrol, they are duty-bound to do so. So it seems counterintuitive to require police to obtain a warrant before showing the vigilance they are required to show as a condition of their work.

One might suggest that courts should impose Fourth Amendment requirements only on focused investigations of public space and not on casual observations that police make while on patrol. But even this approach arguably restricts police too tightly. Because law enforcement is generally barred from conducting warrantless investigations of homes and other private spaces, it needs to begin an investigation somewhere else—in the public space outside of the home. As the Supreme Court noted in California v. Ciraolo,80 in order to obtain the probable cause required to obtain a warrant, police must begin investigating and collecting evidence before they have probable cause.81 Thus, there needs to be some place to start.82 In short, if courts and scholars extend Fourth Amendment protection beyond homes, private drawers, and journals into the realm of public and visible activity, they have to recognize that they are extending it into a realm that is, in many ways, and to a far greater extent than the

80. Id. at 215.
81. Id. (recognizing that the chance to make observations from the public space is "practically what a judicial officer needs to provide a basis for a warrant").
82. United States v. Garcia, 471 F.3d 994, 998 (7th Cir. 2007).
84. See, e.g., Ciraolo, 470 U.S. at 215 (treating what an individual knowingly exposed to the public is well protected by the Fourth Amendment).
85. See, e.g., United States v. Kanno, 660 U.S. 705, 721 (1984) (holding that investigations do not constitute a search when they are observing that which can be seen by the public); United States v. Knotts, 460 U.S. 276, 281 (1983) (explaining that tracking near public streets voluntarily conveys information to anyone who might be watching with the naked eye or with the assistance of technology).
86. See Ciraolo, 470 U.S. at 215-16 (holding that investigations do not violate the Fourth Amendment when they observe property from public airspace and members of the general public flying overhead could make the same observations); Holmes v. Green, 408 U.S. 215, 219 (1966) (finding that the Environmental Protection Agency's fly-by assessment of an industrial complex to observe whether it
radio transmitters and chartered airplanes became a common feature of everyday life, the Supreme Court—in a 1924 decision written by Justice Holmes—made clear that "the special protection accorded by the Fourth Amendment to the people in their persons, houses, papers and effects" is not extended to the open fields. The "open fields" doctrine later seemed to come to an end with the Court’s holding in Katz, in which the majority held that electronic eavesdropping is a Fourth Amendment search even when it targets someone making a call from a public phone booth on a street. The Katz majority had called into question the notion that everything we do in public may be monitored free of constitutional restraint, declaring that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." But the Supreme Court later made clear that the open fields doctrine remains a central part of the Fourth Amendment law. In Oliver v. United States, the Court squarely rejected a property owner’s claim that the police had violated the Fourth Amendment when they located a marijuana field on his land. Unlike a realm where individuals might reasonably expect privacy, said the Court, "open fields do not provide the setting for those intimate activities that the Amendment is intended to shield from government interference or surveillance." Courts have understood this "open fields" doctrine to mean that police are free to observe not only what is visible in a field, but also what they can see in public streets and roads.

Such an approach still leaves individuals with an opportunity to find sanctuaries for privacy in public space, but only when they find pockets of "inside" space somewhere in the public, visible world. People might, for example, hide items they bring onto a street within a purse or briefcase. They might keep confidential conversations secret by engaging in them only from a closed phone booth or from

was in compliance with environmental regulations did not constitute a Fourth Amendment search).

91. See id. at 177, 185-86.
92. Id. at 179.
94. See, e.g., Katz, 389 U.S. at 353 (finding the government engaged in a search when it eavesdropped "the privacy upon which [the defendant] justifiably relied while using the telephone booth").
95. See, e.g., Delaware v. Prouse, 440 U.S. 648, 656-59, 663 (1979) (holding that stopping an automobile and requesting the driver’s license and registration involves a search and is only permissible under the Fourth Amendment where there is reasonable articulable suspicion to do so).
97. Id. at 663.
98. See id. (requiring that officers may only stop and detain motorists if there is at least articulable and reasonable suspicion that the motorist has violated the law).
99. See Terry v. Ohio, 392 U.S. 1, 24-25 (1968) (highlighting the need to grant police a means of determining whether a person poses a threat of physical harm and a way to neutralize that risk).
100. See generally United States v. Jones, 129 S. Ct. 945, 953 (2009) ("This Court has done no more than conclude that mere visual observation does not constitute a search.");
101. 19 Howell’s State Trials 1799 (C.P. 1750).
102. Id., in 19 Howell’s State Trials 1799, 1799 (C.P. 1750).
103. See Bond v. United States, 116 U.S. 616, 626-27 (1886) (explaining that during the Revolutionary Period, American soldiers were familiar with Katz, the "manifestance of English freedom," and its proprieties were unquestionably in the minds of the Framers as they created the Fourth Amendment).
As Justice Scalia noted in Janez, "This Court has to date not devised from the understanding that mere visual observation does not constitute a search." When police search inside of a home or another private environment, of course, they engage in more than mere observation. They first enter the space, thereby transforming their subsequent observations into a search requiring a warrant (or some other showing of constitutional reasonableness).

By contrast, in public spaces, police can often observe an individual's movements and other activities without having to set foot on anyone else's property. To the extent they invade the privacy of the person they watch, they often do so simply through observing.

A second advantage of denying Fourth Amendment protections to observations of what is visible in public is its simplicity and clarity. It draws a clear line for police officers and citizens. What is inside a home or office is protected; what is outside in public space is not. To be sure, this kind of simple division does not line up perfectly with individuals' expectations of privacy. Individuals may well be more eager to hide certain activities they conduct in public life, such as travelling to a psychotherapist's office or visiting an R-rated movie theater, than they are to hide many mundane activities in their home life, such as their choice of what to have for breakfast. But perhaps it is not plausible to calibrate Fourth Amendment protections to the privacy that individuals expect in each discrete activity.

The Supreme Court has certainly not tried to adjust the degree of protection on an activity-by-activity basis in applying the Fourth Amendment to in-home activity. On the contrary, as the Court emphasized in Kyllo v. United States,84 "[i]n the home, . . . all details are intimate details, because the entire area is held safe from prying government eyes.89" It therefore does not matter that the activities the government observes in gathering information from a home are not particularly embarrassing or sensitive.

The Fourth Amendment err on the side of protecting the privacy of all in-home activity; perhaps it should err in the other direction outside the home. If the public needs some protected space where it can count on privacy without worrying about whether a particular activity is or is not sufficiently intimate to be shielded from government officials might also need some space where they can watch potentially illegal activities without worrying, during each observation, whether the activity they are watching is too private to look at (for too long) without a warrant. Such a bright-line rule arguably would not only provide certainty for police, but also reassure the population that relies on them that law enforcement will be able to act proactively and effectively to investigate and thwart criminal activity.

It is perhaps therefore not surprising that while the D.C. Circuit in Maynard ventured to extend Fourth Amendment limits to public surveillance,81 the other circuits to address the issue have found that GPS tracking is a non-search by virtue of the fact that the information it collects comes solely from a driver's public and observable activity. The Seventh Circuit, for example, noted in 2007 that while GPS surveillance may threaten our privacy, it does not do so in a way that makes it a Fourth Amendment search.82 Rather, it is a high-tech analogue for visual tracking of a kind police have long done free from constitutional restrictions.83 "If police follow a car around, or observe its route by means of cameras mounted on lampposts or of satellite imaging as in Google Earth, there is no search, and when police "follow" the same car with GPS tracking technology, they are "on the same side" of this constitutional divide." The Seventh Circuit reaffirmed this position on GPS tracking after Maynard was decided, noting again that so long as GPS tracking is limited to public space, it reveals no more than what is already visible.84 The Eighth 105. Janez, 132 S. Ct. at 995.
106. See id. at 34–35 (Stevens, J., concurring).
107. See id. at 349–50 (majority opinion).
109. Id. at 37 (holding that the use of thermal imagers to detect the heat emissions coming from a house is a search under the Fourth Amendment).
110. Arguably, this clear division of inside "protected areas" and outside unprotected ones is at odds with the Court's oft-repeated language in Katz that "[t]he Fourth Amendment protect[s] personal, not places," and the key question is therefore not where a person is, but what that person reasonably expects will remain private from the government. Katz v. United States, 389 U.S. 347, 500, 351–52 (1967) (holding that "What a person reasonably expects to be secure, even in an area accessible to the public," is constitutionally shielded). But the inconsistency may be only apparent. If we preserve privacy in public by encasing our property or action inside of a hidden space, and expose our action in the home by leaving it visible to prying on the street, then Katz still tracks the outside-inside distinction quite well. We lose our privacy inside the home when we leave an in-home activity visible to those in the outside world, and we can gain a measure of privacy in public by finding a way to avert to some kind of enclosed container or other space.
112. See, e.g., United States v. Marquez, 605 F.3d 604, 609–10 (9th Cir. 1991); United States v. Varela-Moreno, 391 F.3d 1212, 1219 (9th Cir. 2004); United States v. Pineda-Moreno, 391 F.3d 1212, 1219 (9th Cir. 2004); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).
113. Garcia, 474 F.3d at 998.
114. Id.
115. Id.
116. Id. at 997.
and Ninth Circuits likewise applied Supreme Court precedent to conclude that police no more engage in a Fourth Amendment search when they track a car in public space using GPS technology than when they track a car by following it.117 Video surveillance would, for example, not only show that a particular car parked near a doctor’s office, but also that a particular person emerged from the car, went inside the office, and perhaps came out carrying a worried look on her face. It would indicate not only that a person parked near a particular bookstore or DVD store, but also, perhaps, what book or movie she carried out of the store.118 These activities, of course, take place in public where a person might be seen by others nearby, including police officers. But in a world without ubiquitous public surveillance, others are unlikely to focus on, let alone remember, activities of strangers that have no significance to them. A video archive, by contrast, gives interested officials a way to scrutinize (and review) such acts after the fact, even if they have no probable cause or other reasonable basis to track them.119 In short, if public and visible space remains a Fourth Amendment-free zone, it provides room not only for police to vigilantly watch the streets (as we expect them to do), or perhaps notice and scrutinize activities that seem suspicious, but it also provides them with unlimited space to record, track, and review the minute-by-minute activities of individuals they have no reason to suspect of a crime. This includes activities that, although occurring in public, deal with medical issues, reading preferences, or other traditionally private information.120

117. See, e.g., Marquis, 605 F.3d at 609-10 (citing that no search occurs when the use of GPS technology does not infringe upon a person’s privacy); Rhodes-Moss, 591 F.3d at 1216 (explaining that GPS technology serves as a substitute for physically following a car on public roads and therefore similarly does not constitute a Fourth Amendment search).

118. See generally Adam Schwartz, Google’s Video Surveillance Camera: A Precursor and Prophet of Unlawful Surveillance? 116 U. Pa. L. Rev. 21, 25 (2008) (“Without meaner rendition, each of us must wonder whether the government is watching and recording us when we walk into a book store, a political meeting, or a psychiatrist’s office.”).

119. See Blatt, supra note 45, at 1566 (describing how a video archive can allow the government to virtually “randomly stop and closely scrutinize numerous people,” exactly the type of search the Fourth Amendment prevents).

120. See United States v. Jones, 565 U.S. 467, 484 (2012) (listing examples of public misconceptions that could reveal private details (citing People v. Weaver, 998 N.E.2d 1195, 1199 (N.Y. 2010))).

121. See, e.g., Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (noting that using satellite surveillance technology might require a warrant in order to be constitutional).

122. See infra notes 124-124 and accompanying text (reviewing the Court’s discussion of potential constitutional issues with magnification).

123. See infra notes 120-120 and accompanying text (reviewing the Court’s cases related to tracking devices).


125. See Dow Chem. Co. v. United States, 476 U.S. at 238 (explaining that the magnification at issue in the case was not strong enough to expose “intimate details,” which would raise constitutional concerns).


127. Id. at 239.
magnification revealed small items such as a "class ring" or "identifiable human faces or secret documents captured in such a fashion as to implicate more serious privacy concerns."

Similarly, in *Crawford*, which was decided on the same day as *Dow Chemical Co.*, the Court hinted at the same "intimate details" protection against public surveillance. It held that police did not violate reasonable expectations of privacy when they used a fly-over airplane to observe marijuana in the defendant's backyard. But it also stressed that the State itself had acknowledged that such fly-over observation might well be a search when it employs "modern technology" to reveal "those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens." It included the same hint in *Florida v. Riley*, even as it refused to find the police engaged in a Fourth Amendment search when they hovered over the defendant's greenhouse in a helicopter and peered through a crack in its roof to verify that it contained marijuana plants. The Court made clear that there was no evidence that the State's aerial observation revealed any "intimate details connected with the use of the home or curtilage." In short, where the State uses magnification to reveal intimate details in a home's curtilage, it may well be engaged in a search—even if those details are visible from public airspace. The same might be true of magnification that is aimed, not at a home's curtilage, as in *Crawford* and *Riley*, or a business's property, as in *Dow Chemical Co.*, but at activities in streets, parks or open fields.

The Supreme Court also suggested, even before the concurrences in *Jones*, that ongoing location tracking may reveal hidden details and thus become a search. In its 1985 *Knotts* decision, the Court held that police do not engage in a search when they use a radio transmitter to track a driver's movements on public roads, while acknowledging that more invasive location tracking might be a protected search.

The Court noted the concern that finding the police conduct at issue

129. *Id.* at 255 n.5.
130. See *Crawford*, 476 U.S. at 215 & n.3 (noting that the use of technology to aid the naked-eye view does not change Fourth Amendment analysis).
131. *Id.* at 215.
132. 408 U.S. 445 (1972)
133. See id. at 450–51 (plurality opinion) (explaining why an expectation of privacy from the air was unreasonable).
134. *Id.* at 452.
135. See *United States v. Knotts*, 460 U.S. 276, 284 (1983) (discussing the Sixth Circuit's finding that "surveillance" surveillance could be prohibited by the Fourth Amendment but noting the limited invasiveness of the search used in this case).

in *Knotts* to be within constitutional limits would mean that police would likewise be free of all constitutional restraint if they conducted "twenty-four hour surveillance of any citizen" on a whim. Such a "dragnet-type law enforcement practice[,]" suggested the Supreme Court, might be subject to Fourth Amendment limits, even if limited location tracking with a radio transmitter is not. In *Maryland*, the D.C. Circuit seized upon this reasoning and held that a twenty-day period of continuous GPS surveillance was precisely the kind of ongoing surveillance that the Court in *Knotts* explained would be constitutionally problematic.

Taken by themselves, these dicta do not provide ready-to-apply Fourth Amendment rules for identifying searches in public spaces. First, they do not provide the kind of identifiable boundary line between searches and non-searches that law enforcement officers need in order to know whether a particular search technique requires a warrant. As noted earlier, there is no guiding principle for when location tracking or video surveillance has occurred for too long of a period—or collected too much information—to remain free of constitutional limits. The same problem arises for a rule that constitutionally shields "intimate" activities from magnification technologies but leaves other types of activities, such as movements on a road, free-for-the-taking. While certain activities, such as those involving family interactions, romantic relationships, or medical appointments, may intuitively be inappropriate for a state official to spy upon, the fact is that people are different. What may be personal and private for one person may not be so for another. People are idiosyncratic, and what is truly private is a matter of social context.

For example, if a person is seeking a new job, he may want to buy books on switching careers or visit a resume workshop without his employer discovering these actions. These kinds of activities may be all that private for other people, such as a college student who, like many others about to graduate, has to prepare herself for the job market. But, those actions may be private for a long-time employee who wants to, and perhaps must, hide his plans for a career-change from a current boss. Courts are ill-equipped to make these distinctions. Unlike a line that divides all content-based information

136. *Id.* at 388–89 (deferring constitutional analysis of such practices).
137. *Id.* at 394.
139. See supra text accompanying notes 29–34.
140. See supra note 95, at 7412 (giving examples of sensational and individual factors that can influence the level of privacy desired).
in an e-mail from non-content based information, such as an e-mail address, a line that divides some kinds of "intimate" content from other kinds of content is a hard line for courts to mark.

Still, the Supreme Court's dicta about magnification and location provides a foundation to build upon. The suggestion in its aerial surveillance cases—that some types of magnification would count as a search—captures a widely shared intuition: namely, that even in public space, we may desire, and should still be able, to keep certain details of our lives from being seen by others with whom we share that space. Even in the outside world, certain details of our activity may be so difficult for others to notice that they are akin to details we have enclosed in a bag or a car. These activities are essentially invisible because of their small size, the distance, or the limits of natural human vision and human attention. These factors can hide them almost as effectively as the invisibility created by a wall or enclosure that blocks light. Details that cannot typically be seen without magnification, because of size, distance, or visual limitations, might constitute one category of outside information that should be treated as "inside" for Fourth Amendment purposes.

The same is arguably true of information about us that can be obtained only by aggregating numerous public observations of our activity taken from a wide swathe of public space. This is the argument at the heart of the mosaic theory that the D.C. Circuit used in Maynard to find that GPS surveillance was a search.141 The D.C. Circuit held:

[The information the police discovered in this case—the totality of Jones's movements over the course of a month—was not exposed to the public; unlike one's movements during a single journey, the whole of one's movements over the course of a month is not already exposed to the public because the likelihood anyone will observe all those movements is effectively nil.] 142

Just as magnification reveals information that is effectively invisible to observers in public space, so too did GPS surveillance in this case. This information therefore also might be deemed to be akin to "inside" information, which is generally not available to individuals who make only surface-level observations of the activity around them and do not deepen their observations with the aid of sophisticated technology or a large coordinated team of observers.

141. See Maynard, 615 F.3d at 362 (discussing the government's use of the mosaic theory to justify collecting information for national security purposes).

142. Id. at 368.
described above. Once courts assure themselves that police are using this advanced technology, any resulting investigation would be classified as a "search," regardless of its duration or detail.

Not would such searches involve "mere visual surveillance." While the "eye cannot be guilty of Fourth Amendment violations," electronic monitoring of otherwise inaccessible data can be unconstitutional. Such electronic monitoring, for example, often counts as a "search" when it is used to intercept conversations. It should likewise count as a search when it is used to record individuals' movements and activities in public space.

Another reason to focus on the recording of remote activities as a trigger for Fourth Amendment protection is based on the fact that courts and scholars alike often identify the central purpose of the Fourth Amendment as protecting privacy. For example, Professor Sherry Colb, a Fourth Amendment expert, made this claim in responding to the notion that the Fourth Amendment only protects privacy in a limited way—by protecting the privacy we receive from control we exercise over our homes, cars, or other property. The Framers' goal in the Fourth Amendment, she wrote, can best be understood as protecting "privacy in all of its incarnations." Such an emphasis on privacy is understandable given the Supreme Court's interpretation of the Fourth Amendment since 1967. Under the definition of "search" the Court has used since Katz, Fourth Amendment protections are triggered only when government invades "a reasonable expectation of privacy." As a result, judges and commentators often have understandably assumed that it is precisely such an expectation of privacy, whether tightly linked to property or not, that the Fourth Amendment is intended to protect. Thus, Justice Alito's concurrence in Jones focused on understanding whether the GPS tracking in that case intrudes upon a "constitutionally protected sphere of privacy." Even critics of the Katz test, such as Professor Anthony Amsterdam, have spoken in similar terms about Fourth Amendment purposes, arguing that its core function is to prevent government attacks on privacy and freedom that would be "inconsistent with the aims of a free and open society."

But in the Katz majority itself observed, "privacy" is too general a description of what the Fourth Amendment protects. The "Fourth Amendment," it observed, "cannot be translated into a general constitutional 'right to privacy.'" Rather, it protects privacy against "certain kinds of governmental intrusion." The challenge facing courts then is to pinpoint which types of governmental invasions into privacy implicate Fourth Amendment purposes and which do not. This is an important question for courts to ask as they analyze public surveillance. After all, every time a police officer stops a person who is standing on the street or driving on the road, that officer is, in some small measure, lessening that person's privacy vis-à-vis the state. He is watching activity that might otherwise go unnoticed by any representative of the state. The same is true if an officer at a police center watches a monitor displaying images from a remote street camera. These are invasions of privacy, but that alone does not make them violations of the Fourth Amendment. Rather, courts must also assess whether the state's reduction in our privacy in these cases is accomplished by the "kinds of governmental intrusion" that the Fourth Amendment prohibits.

Unfortunately, the test that courts rely on most heavily to address this challenge—the reasonable expectations of privacy test—sounds precisely like a test for implementing the general right of privacy that
the Katz majority had sought to distinguish from the Fourth Amendment right against unreasonable searches. Rather than limit Fourth Amendment safeguards to certain government intrusions into privacy, that test subjects all such intrusions that interfere with the privacy that individuals reasonably rely upon to constitutional limits.

Judges have sometimes emphasized that the requirement for reasonable reliance is itself a limit. Even if a person expects privacy on a public street (satisfying the first prong of the reasonable expectations test), such an expectation is not one society is prepared to recognize as reasonable (failing the second prong). But this limit is not at all that helpful. First, the privacy we reasonably rely upon can be easily diminished, as Professor Amsterdam has highlighted, and the Supreme Court soon after acknowledged, by government action itself. By putting people on notice that they will be subject to GPS monitoring, for example, the government could make it unreasonable to expect freedom from such monitoring. Moreover, the test also seems to place Fourth Amendment law on quickly shifting sands. An expectation of privacy can change quite rapidly as technology advances, and social norms change from year to year. Perhaps for this reason, the Supreme Court has often interpreted "reasonable expectation of privacy" in a way that seems at odds with common intuitions about when citizens can expect privacy and, as Professors Christopher Slobogin and Joseph Schumacher have shown, with empirical data about such expectations.

Still, there is reason to take seriously—and try to better elaborate upon—the Supreme Court's statement in Katz that the Fourth Amendment protection against unreasonable searches is narrower than a general "right of privacy." As the legal scholar William Stuntz powerfully argued, it would be odd to see the Fourth Amendment as providing such a right against government collection of our information through surveillance, when the modern regulatory state permits (indeed, even requires) collection of much of the same information in so many other ways. Stuntz noted that "much of what the modern state does outside of ordinary criminal investigation intrudes on privacy just as much as the kinds of police conduct that Fourth and Fifth Amendment law forbids." While the focus of this Article is not on the purpose of the Fourth Amendment, it is useful to at least propose one alternative way of identifying the subset of privacy violations that also constitute possible Fourth Amendment violations. The best way to identify such governmental intrusion is to begin with the paradigmatic type of intrusion that the Fourth Amendment protects us from: the police "fishing expedition." This is a kind of investigation that af|
designed to bar, allowing law enforcement to treat individuals they have no reason to suspect of a crime as potential criminals who, as such, must reveal all of their possessions and papers, as well as their persons, for thorough examination. Airport checkpoints can and are, of course, permissibly used to conduct certain kinds of suspicionless searches—namely, searches of every air traveler for weapons or items that might be used for terrorism. However, such searches are subject to tight constitutional limits.

The constitutionality of types of observations by officials can be defined by this kind of paradigmatic analysis. After all, it is not the case that every state intrusion into an individual’s privacy, even privacy that we reasonably rely upon, necessarily subjects us to the functional equivalent of the general search or dragnet investigation that was the focus of the Fourth Amendment’s protections. Rather, what constitutes a general search is not only that it intrudes upon an individual’s privacy, but that it does so in a way that alters an individual’s relationship with the state. It converts that individual into a suspected criminal.

This is a concern that is, to some extent, at the core of the key alternatives to a privacy-based account of Fourth Amendment purpose. The Fourth Amendment’s purpose is not simply to preserve a certain amount of privacy; it is rather to assure that individual citizens are ordinarily able to keep a certain amount of distance between themselves and the coercive machinery of state power—and live with a certain level of freedom from that power—and freedom from fear of being subjected to it on an official’s whim. Professor William Stuntz, for example, argued that the central evil that Fourth Amendment law was designed to combat was not police observation, but police coercion. *168* “[P]rivacy protection,” Stuntz wrote, “has little to do with the worst aspects of police misconduct,” which are about violence towards, or intimidation of, suspects. Using a vehicle search as an illustration, Stuntz argued that when police stop a driver and ask for consent to search the car for drugs, the most worrisome consequence of such a stop for an innocent person subject to the

166. See United States v. Alarcon, 494 P.2d 798, 805 (64 Cal. 1974) (describing the purpose behind airport searches.

167. See 524, 525 O.J. Carney, 873 F.2d at 1265–66 (explaining that airport security searches cannot be used to search for contraband generally or things that “merely look suspicious”.

168. See Stuntz, supra note 160, at 1029 (arguing that criminal procedure law’s focus on information gathering over police coercion comes at the expense of protecting values.

169. Id. at 1078.

search is not that the police will see or examine whatever happens to be in the car; it is “the indignity of being publicly singled out as a criminal suspect and the fear that flows from being targeted by uniformed, armed police officers.” In a similar vein, Professor Jed Rubenfeld has reasoned, based in large part on the Fourth Amendment’s text, that the Amendment’s central purpose was not to assure privacy but security—to protect people from “stifling apprehension and oppression that people would justifiably experience if forced to live their personal lives in fear of appearing ‘suspicious’ in the eyes of the state.” Another scholar, Scott Sundby, likewise offered an alternative to the conventional privacy-based account. He stated that the purpose of the Fourth Amendment “is founded upon the idea that integral to the Constitution and our societal view of government is a reciprocal trust between the government and its citizens.” Police, he argued, should not be permitted in our constitutional system to act in ways that treat each citizen as a potential criminal. For example, police should not be permitted to search for contraband in the trash cans of individuals they have no reason to suspect of criminal wrongdoing.

While the exact implications of these non-privacy-based approaches to the Fourth Amendment depend on how they are elaborated, it seems likely that each would justify putting some limits on when and how closely police can track or scrutinize individuals’ activities in a public space. A society where the state tracks a person’s every move, even when it has no good reason to believe he is a criminal, is arguably not showing the kind of trust in its citizenry that Sundby insisted the Fourth Amendment demands. Nor is it likely to leave people feeling secure that, if they obey the law, the government will leave them free from its coercive grasp. A person who feels that the government is always watching for any hint of a legal misstep is likely to feel that a police interrogation and arrest is always a possibility. So Stuntz might find that unconstrained drone tracking carries some of the same harms as arbitrary car searches. And Rubenfeld might find that such ever present drone monitoring generates in its target an

170. Id. at 1064.


173. See generally id. at 181–12 (summarizing the argument for an approach to Fourth Amendment jurisprudence based on the concept of government-coercion trust.

174. See id. at 1788-95 (discussing the lengths the Supreme Court went to in order to justify finding that use of surveillance was outside the Fourth Amendment).

175. See id. at 181-12 (explaining that the true-based approach better aligns with democratic principles).
intense "fear of appearing 'suspicious' in the eyes of the state"—the precise fear the Fourth Amendment’s protections are designed to spare us. 176

Although these accounts often offer an emphasis on trust, security, or freedom from police abuse as an alternative to a privacy-based account of Fourth Amendment purposes, they are perhaps better understood as refinements of such a privacy-based account. State surveillance that threatens Fourth Amendment values does so in large part because it wrestles privacy away from citizens, leaving the private details of their lives exposed to review and examination by an outside observer. Such a privacy violation is a necessary condition for a state measure to implicate Fourth Amendment interests, at least when the state avoids the kind of trespassary or other interference with property that itself counts as a Fourth Amendment search, but it is not a sufficient condition. Rather, a privacy intrusion generally violates the Fourth Amendment only when it treats an innocent individual as a suspected criminal and thereby makes her more vulnerable to the state’s power of coercion and punishment.

A police investigation that generates and stores records of our public movements and activities creates the effect of treating society as suspected criminals. It not only reduces the privacy of those it records. It also, as Justice Sotomayor explained, allows the government "more or less at will" to review innumerable details of an individual’s life for evidence of possible wrongdoing. 177 As a result, people may be subjected to "arbitrary exercises of police power." 178

B. Recording as a Dividing Line Between Searches and Non-Surveys

Recording should thus be central to Fourth Amendment law because, in the context of public surveillance, it allows authorities to sift through sensitive information about our movements and activities. A recording transforms an ephemeral event into a permanent record. It thus frees authorities from the burden (and cost) of having to observe the public's movements and activities as they occur. It also removes the challenge of having to remember those movements well enough to compare or combine them with other observations in order to build a larger picture. For example,

176. Bubenfield, supra note 171, at 127.
177. See United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring) (discussing the importance of considering a GPS device’s ability to allow recording and aggregation of the details of a person’s movements in determining if there is a reasonable expectation of privacy).
178. Id.

the kind of "precise, comprehensive record of a person’s public movements" cannot be easily created unless a GPS unit not only transmits information to police about a person’s whereabouts, but also captures that information in electronic memory. 179 In fact, Sotomayor explained in her concurrence that the fact that the GPS device allows recording and aggregation is precisely what allows the government to discover the private details of public activities.

Recording is also usually indispensable to creating the kind of detailed "mosaic" of a person’s life, which the D.C. Circuit found so concerning and identified as a basis for subjecting GPS surveillance to Fourth Amendment limits. As the D.C. Circuit emphasized, with a record of a person’s movements over a several day long period, police can learn things about a person’s life that would be unknown to all other passersby who happen to see that person on roads or streets:

Repeated visits to a church, a gym, a bar, or a bookstore tell a story not told by any single visit, as does one’s not visiting any of these places over the course of a month. The sequence of a person’s movements can reveal still more; a single trip to a gynecologist’s office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another’s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts. 180

The D.C. Circuit did not emphasize the difference between recording and merely observing activities in its opinion. But the difference is important for its argument: it is far more laborious for police to aggregate these details of a person’s activities unless it records each movement or action for later comparison with others. If, in the above example, a particular official does not have a record of the first visit to a gynecologist’s office, it is far less likely he will be able to combine it with the subsequent visit to the baby supply store to infer that the woman is expecting a child. And it is unlikely that he will have access to the earlier detail, unless he is doing all of the tracking himself or working with a team of officers that are constantly sharing information that they have recorded. It is conceivable that even without any recording device, officials could draw an inference

179. Id. at 905.
180. See id. at 906 (arguing that this factor is important in determining society’s expectation of privacy).
from the woman’s two visits. However, this becomes more implausible when an investigation aggregates not only two, but tens or hundreds of events.

The latter type of investigation, as Justice Alito stated in his Jones concurrence, could hardly have happened in a world before GPS surveillance without “a large team of agents, multiple vehicles, and perhaps aerial assistance.”182 Even in a pre-GPS form of extended location tracking, officials would need to create records of their target’s movements in order to share their observations with others on the team.183 At least one recent state court decision has treated the fact that one can imagine a more primitive analogue of automated recording as evidence that it cannot be a search. In City of Boston v. Commonwealth,184 the Court of Appeals of Massachusetts held that because “a police officer could have followed and personally recorded the movements of the van” without conducting a search, the use of a GPS recording device to track the van was not a search.185 But this is not the inevitable conclusion one might draw from such an analogy. It would be extraordinarily difficult for a single officer to follow a van as continuously as a GPS device: it would be an unusual officer, able to forego a significant amount of sleep, who could follow a van driver’s every (unpredictable) movement over the course of an entire week. A team of policemen, as Justice Alito recognized, would likely be required, and the fact that one can imagine a much more expensive and complicated low-technology analogue for GPS recording does not mean that GPS recording is not a search.186

Recording is even more of a game-changing technology for video surveillance than it is in location tracking. When police not only use video cameras on street lamps or drones for real time monitoring, but also to create video surveillance footage that may be subject to later review, they allow for a kind of investigation that is far more intrusive—and far more like a dragnet search—than real-time monitoring. Not only can police aggregate and compare different events or actions, as they can in the context of location tracking, but they can also pause on a particular frame, examine it closely, and notice small details of a person’s appearance or actions that they would be very unlikely to notice if they had only one chance to perceive and remember an event as it occurred.

At the extreme, a recording could create the kind of science fiction world Lewis Padgett depicted in the story, “Private Eye.”187 This is a world in which every action we take is recorded and stored in police-owned video footage and in which officials can therefore watch the day-to-day existence of any individual the way most people watch a DVD or downloaded movie—by watching it unfolded on a screen and pausing to rewind and review sequences that they did not fully perceive or understand the first time through.188 If officials subjected an individual who they have no reason to suspect of a crime to this kind of video review just to see if the video record happened to reveal anything suspicious, there is little question that they would be poring over personal details of that person’s life in much the same way they do in a more traditional “dragnet” search.

Moreover, what is significant about video recording for Fourth Amendment purposes is not only the way it allows authorities to aggregate and compare many small details of our day-to-day lives, but also the power it gives them to pause on or review the same detail over and over again. We normally miss a good deal of what is happening in a scene in front of our eyes. Typically, people do not consciously perceive elements of a scene that they have no need to notice.189 Video recording, by contrast, captures the information our perception misses. It replaces our flawed natural memory with an artificial replacement that lacks its imperfections and allows police to overcome its limits.190 In large part, for this reason, Justice Harlan wrote that even a form of surveillance that is not normally a search,

182. Jones, 559 U.S. at 965 (Alito, J., concurring in the judgment).
183. See supra Part II.C (describing the type of traditional police work necessary to record as much information as a GPS device).
185. See id. at 291–95 (reasoning that the use of GPS technology did not provide a substitute for police behavior that would otherwise violate a right to privacy because the police could have followed and personally recorded the movements of the van).
187. See Bitt, supra note 45, at 1350–59 (citing Lewis Padgett, Private Eye, in THE MIRROR OF INFINITY: A CRITICAL ANTHOLOGY OF SCIENCE FICTION 59 (Robert Silverberg ed., 1990)) (proffering that science fiction can give us a view of the potential future of government surveillance and the need to reconsider the approach to the Fourth Amendment).
188. See Padgett, supra note 187, at 100 (describing a fictional “coordinates” that stored a fiftyyear history of light and sound images and was “a device for looking into the past.”)
189. See CHRISTOPHER CHAMBER & DANIEL SIMON, THE INVISIBLE GORILLA: HOW OUR INATTENTIVE BEHAVIOR DEPENDS ON SOCIAL HINTS (2010) (reporting on an experiment in which individuals who were unaware that they were being observed by another person smiled and waved in a game of ‘chicken’)
190. See Bitt, supra note 45, at 1356 (describing how video recordings can be as intrusive as stop-and-frisks).
such as government use of an informant to gather information about a suspected drug dealer or other criminal, should be a search when the informant does not simply listen and remember what he is told, but also electronically transmits and records it. There is a constitutionally significant difference, he stated, between "third-party monitoring and recording which insures full and accurate disclosure of all that is said, free of the possibility of error and oversight that inheres in human reporting." In a world in which individuals gossip about or share what they have observed, our privacy is threatened, but in a way that is often tolerable.

Much off-hand exchange is easily forgotten and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record. In a world of unrestrained recording, by contrast, there is no comfort in knowing that small and obscure aspects of our conversation will escape notice because recordings can be played over and over again to multiple listeners. We do not have the power to "reformulate a conversation" by offering our own account. The audio recording will provide an authoritative, and virtually indisputable, account. It is thus inevitable, said Justice Harlan, that in a world of unrestrained recording "words would be measured a good deal more carefully and communication inhibited."104

In discussing audio recording, Justice Harlan focused primarily on its threat to privacy and its possible chilling effect on communication.105 For Fourth Amendment purposes, however, what is most worrisome about unconstrained video surveillance (or location tracking for that matter) is not simply that it substantially diminishes our privacy and leads us to refrain from taking spontaneous actions we worry may become part of a permanent record. Instead, it is how this specific kind of diminution of privacy affects each individual's relationship with state power. While recording by anybody else (including other private individuals)

101. See United States v. White, 401 U.S. 745, 787-89 (1971) (Harlan, J., dissenting) (noting that transmitting or transcribing conversations is potentially more damaging to free society than the risk of an informant later reporting on a conversation).
102. Id. at 787.
103. Id. at 787-88.
104. Id. at 787-89.
105. Reduces our privacy to some degree, systematic recording by the government diminishes it even more. It allows the government to systematically analyze aspects of our lives, which, in a liberal, individual rights-based society, are not the government's business. Furthermore, it permits the government to do so with the aim of finding, by chance, some basis for subjecting a person to the far greater degree of police power that has traditionally been reserved for those individuals who officials have reason to think are engaged in criminal activity.

Given these observations about the effects of recording, one might wonder why the test proposed in this Article does not make all government recording a search and instead requires that, to constitute a search, an officer's recording must be "remote," meaning outside the realm that the recording officer can perceive with his eyes, ears, and other senses. After all, Justice Harlan's great worries about recording seem to apply not just to a drone's recording of events occurring far from the drone's operator, but also to recordings that a police officer makes of what is happening in front of him.106 Even in a public space, the presence of a government-recording device may chill a citizen's speech or other expressive activity—even if a single police officer operates the device and it is not a part of a massive, surreptitious, surveillance system. However, for Fourth Amendment purposes, there is an important difference between a police officer recording his own interactions, and that which the government gathers from pedestrians and drivers throughout public space. As suggested above, the point of the Fourth Amendment is not simply to protect privacy, but to prevent the state from engaging in the kind of privacy violation that occurs in a dragnet investigation or other "general search" where the state reaches out and subjects individual actions to extensive or pervasive analysis.107 By contrast, where recording is not remote—where a camera mounted on a police car simply captures footage of a police officer's interactions at a traffic stop, or a police officer uses an iPhone (or a camera in his uniform) to capture events that occur on a street around him—then the recording is far less amenable to being used to create a searchable archive of an individual's detailed movements and activities. By contrast, "uniform ears" tiny cameras

106. See generally id. at 787 (failing to differentiate between transmitting and transcribing of conversations).
107. See supra notes 156-72 and accompanying text (explaining that the Fourth Amendment's right to privacy is much narrower than the common understanding of the right to privacy and that the Fourth Amendment only seeks to protect unreasonable invasions of privacy, such as police fishing expeditions with no limits).
The larger concern about uniform or dashboard cams is not the privacy threat they raise in each encounter they record, but rather what police might do by technologically enhancing or aggregating such image-capture. If police combine—into a central, searchable data collection—the images that each of them captures on a uniform or dashboard-mounted camera, such action could begin to mimic the effects of a larger recording system. However, if the term "search" broad enough include any action that could threaten privacy, in combination with other surveillance measures, would cover far too much ground: Virtually any kind of police observation could be, in combination with other measures, threaten our privacy and perhaps even allow arbitrary fishing expeditions. A technological form-based or design-based test of the kind proposed in this Article would be of little import if it were this broad.

To be sure, one can imagine scenarios in which police uniform cams or dashboard cams are designed not to serve their current purpose of preserving records about each police officer's encounters with the community, but rather to sweep in, and preserve for later review, evidence about citizens' actions and movement. Imagine, for example, that instead of mounting a camera that records merely what is in front of the car, police mount a camera like the rotating cameras mounted on top of Google's Street View vehicles, that constantly captures footage from the 360-degree field surrounding the police car each minute and magnifies each part of this visual field to reveal details of every person and car passing by. Although such a police car camera technically only captures data from the realm that the officer can potentially see and hear, it might still collect a worrisome amount of data about individual citizens. In fact, such a video surveillance system threatens Fourth Amendment values in the same way as a citywide system of video recording carried out from stationary cameras or aerial drones. The cameras simply happen to be mounted on police cars rather than on lampposts or drones. In such a circumstance, courts should find that police do engage in a search when they use the combined, programmatic use of police car cameras to create, and later review, ongoing records of citizens' movements.

C. Extensions: When Magnification—and Recording—Should Count as Searches and When They Should Not

This Article so far has argued that police conduct a Fourth Amendment search when they remotely record a person's actions or movements, whether they do so with a drone-based camera, a network of street cameras, or a GPS-tracking device. As noted earlier, such recording enables government officials to search public lives frame-by-frame, much in the way it might search documents file-by-file. But while remote recording is the clearest type of search in a public space, it is not necessarily the only type. Even in the absence of any recording, police might take advantage of other surveillance technologies to circumvent the traditional Fourth Amendment protection for our "persons, houses, papers, and effects." Using a high-powered telescope, for example, officials gather information from the inside of a person's home that they might otherwise obtain only by entering the house or the curtilage.

There is certainly precedent for the Supreme Court to classify a form of surveillance as a "search" when it is the functional equivalent of surveillance that would be a search. In Kyllo, the Court found that police engaged in a search of a home when they pointed a thermal imager at the home from the street outside to measure the heat emissions in order to determine if there likely was a marijuana-growing lamp within. This was not, of course, a traditional home search: the officers never entered the house. They simply measured the heat leaking through its walls from a public street where they had every right to be without a warrant. The Supreme Court held that the officers had engaged in a search of the home by "amplifying the normal electromagnetic emissions of the house," which is a search of the "intimate sector of Fourth Amendment space."
Court nonetheless held that these heat measurements from the outside were a search, largely because their intrusion into the home was functionally equivalent to a home entry. In fact, this concept of functional equivalence was built into the test that the Supreme Court proposed for how to apply the Fourth Amendment to the use of "sense enhancing" technologies to observe the home. The Court held that the use of such technology counts as a search when it is employed to obtain information that otherwise could have been obtained only through "physical intrusion into a constitutionally protected area." The Court added the caveat that this applies only to technology that "is not in general public use." So while police are subject to Fourth Amendment constraints when collecting heat measurements from the home with a thermal imager, they might be free of such limits if they instead look at the home's walls with the same kind of binoculars available to bird watchers, sports fans, or amateur astronomers. Perhaps this is because unlike thermal imagers, which people do not expect to have pointed at their houses in the course of their normal day-to-day existence, binocular viewers are a common part of life in modern society, and individuals who wish to safeguard their privacy cannot expect that their activities will always escape magnification by others in their neighborhood. Still, the Supreme Court made clear that it will not allow police to circumvent the Fourth Amendment command that searches of a home be reasonable, invading the home technologically from outside its walls is as much a Fourth Amendment search as invading it physically.

Public surveillance might sometimes cross a Fourth Amendment line and trigger reasonableness requirements, not only when it involves magnification of in-home activities, but also when it is the functional equivalent of other categories of searches. For example, if

---

205. See id. at 55-56 (basing their finding on the fact that the sensors provided information that otherwise could have been obtained only by physical intrusion).
206. Id. at 54 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961) (internal quotation marks omitted)); see also Florida v. Jardines, 133 S. Ct. 1340, 1348 (2013) (Kagan, J., concurring) (finding that use of a drug-sniffing dog to alert to drugs outside the house uses a sense-enhancing "device" to invade the home in a way equivalent to a home entry).
207. Jardines, 133 S. Ct. 1340 at 1348.
208. It is not clear how the Supreme Court would rule on this. In Kyllo, the Court noted that use of technological enhancement had not been completely resolved. Id. at 53. In upholding the use of magnification in Doe Chemical Co., the Court noted that an important factor was that the area photographed was not near a home. Doe Chem. Co. v. United States, 476 U.S. 229, 237 n.3 (1986).
209. See id. at 54 (noting the search of a home using thermal images for reasonableness).
210. The Fourth Amendment does not require that a police officer enter the home to obtain evidence. See, e.g., Brown v. New York, 445 U.S. 590, 598 (1980) ("[T]he Fourth Amendment does not require that a police officer cross the threshold of the home or medically examine a person in order to obtain evidence.")
into the home. If, as the Supreme Court has sometimes phrased it, a backyard or other curtilage surrounding the home receives Fourth Amendment protection because it is an "extension of [the] home," then why treat its protection as variable? Why understand the curtilage's Fourth Amendment shield to protect some of the activity that police can observe from a public vantage point but not other kinds of activities that occur in the same location and are just as open to observation? One possible answer is that, if the Court protects intimate details in the curtilage from scrutiny by high-powered drone cameras, it is because they are the kinds of details that police could not traditionally and typically learn without searching a person, her house, her documents, or her effects. Such a rule might also make sense because just as people cannot prevent certain evidence of in-home activities from leaking out—for example, in the form of heat emissions—they also cannot completely and continuously conceal their private documents and personal items from exposure to the outside world. Individuals in the modern world will occasionally have to read an e-mail or mark-up a memo as they ride on a subway or sit in an airport. They will occasionally read a book as they rest in a park or a plaza or check the readings on a personal fitness monitor as they walk through a public space.

The fact that individuals have little choice but to bring these items into public space, where powerful cameras may magnify them and give officials a closer look, does not mean that they are fair game for untrammeled official scrutiny. The Supreme Court noted in New Jersey v. T.L.O. that even when students enter the closely supervised and monitored environment of a school, they often have no choice but to bring with them numerous personal items, including "keys, money, and the necessities of personal hygiene and grooming," as well as "photographs, letters, and diaries." The Court emphasized that these items remain protected from arbitrary searches, even in the tightly controlled confines of a school. It is hard to see why students (or other individuals) would lose such protection in a public space.

The same is true of cell phone conversations. Conversations that once took place entirely over phone lines between home phones, office phones, and pay phones now increasingly take place over cell phones, often as one or both speakers are walking down the street, waiting at an airport, or sitting in a coffee shop. It seems odd to think that a modern-day Katz could be constitutionally subjected to electronic eavesdropping by government officials armed with parabolic microphones or other sound amplification devices because the private conversation he had to conduct from a phone booth on the street in 1967 would today take place over a cell phone call from the same street. Thus, Professor Wayne LaFave's proposal that the Fourth Amendment be understood to protect against use of hidden microphones or recording devices, even in public space, seems justified.

To be sure, Kyllo's doctrine of functional equivalence should be applied with caution: Every police method that uncovers details about a suspect is, at a high level of generality, functionally similar to other methods of uncovering the same details. Police unable to obtain evidence of a drug conspiracy from a suspect's home will have to try to find evidence of the conspiracy elsewhere, such as in public space or in third-party records. The match between evidence sought outside the home, and that which is inside the home, does not—and should not—automatically transform the public, or third-party record, surveillance into a search.

One key advantage of the technological form-based or design-based test proposed in this Article is that it provides a clearer line between searches and non-searches in a public space—and this line would be easily blurred if the doctrine of functional equivalence were applied too freely. Consider, for example, the difficulties that might arise if courts not only accepted this Article's proposal to count remote recording as a search, but also classified as a search all techniques they found to have effects equivalent to remote recording. Consider, for example, the type of search that Justice Alito identified

---

214. See Florida v. Jardines, 569 U.S. 1, 133 S. Ct. 1409, 185 L. Ed. 2d 499 (2013) ("The curtilage of the home ... serves protection as part of the home itself."); United States v. Jones, 563 U.S. 49, 131 S. Ct. 1346, 179 L. Ed. 2d 1048 (2011) (denying the historical origins of the idea of curtilage in common law); see also id. at 507 (Breyer, J., dissenting) (arguing that curtilage is the area which extends the intimate activity associated with a man's home and the premises of life (quoting Oliver v. United States, 639 F.2d 170, 178 (6th Cir. 1980)) (internal quotation marks omitted).


216. Id. at 330.

217. See id. at 329-32 (noting a balance in schools between permitting entirely arbitrary searches and requiring warrants for every search).

218. See 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 456-45 (3d ed. 1996) (suggesting that privacy expectations are more reasonable for private conversations that take place in a public place than for actions that take place in a private space); and see Susan Freywald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 ALA. L. REV. 9, 36 (2004) (considering a "presence of electronic surveillance" test under which "any conversation a police officer could overhear without would not be private, but those that required a wiretap or abug would be constitutionally protected").
as an earlier-era equivalent of GPS tracking: an operation that follows a suspect’s movements with a team of officers, multiple vehicles, and aerial observation.219 Even without a recording device, such tracking may threaten to impose a temporary dragnet on an individual. By following his movements and activities from place to place, police may make an observation that gives them justification to move in for a pat-down or an arrest. Or, consider a simpler version of such tracking: one officer tails a person’s vehicle, observes what the suspect does when he exits the vehicle and whether he goes into any particular offices or homes. The officer then reports his observations by cell phone to another officer at the station house, who writes down any observations that either of the officers believes to be of interest. Such observation and dictation might produce, with less advanced technology, records equivalent to those captured with automated video recording or location tracking.220 Or, in a situation more akin to the GPS tracking in Jones, police could use a GPS-tracking device that transmits to the police station, but does not record, the location that a car is in at a particular moment.

In such circumstances, it is plausible that a court intent on safeguarding Fourth Amendment interests would classify the systematic tracking that takes place as a search, even in the absence of an automated recording. Doing so may seem necessary to block police from circumventing the limits that apply to recording. However, it is not clear, why, if police become subject to Fourth Amendment requirements when they follow a person with multiple vehicles for a day, they do not likewise engage in a Fourth Amendment search for twenty minutes. All such tracking potentially raises some of the same dangers raised by ongoing recording of a person’s movements. But that does not mean all of it should count as a “search.” And the same problems that make the mosaic theory problematic also confront a proposal to count police tracking as a search only when it goes on long enough or involves a certain number of vehicles or officers.


220. Indeed, when Justice Harlan insisted that there is a constitutionally significant difference between “third-party monitoring and recording,” United States v. White, 401 U.S. 745, 797 (1971) (Harlan, J., dissenting), the “recording” that so disturbed him was this kind of intimate record creation. Instead of secretly audio recording his conversation with the targets of the investigation, the informant wore a bee that transcribed the conversation to an officer outside who surreptitiously listened and then recorded after the informant disappeared. Id. at 746–47 (plurality opinion).

III. OBJECTIONS, ALTERNATIVES, AND LIMITS: DIFFERENT WAYS OF DEFINING A “SEARCH” (AND A “REASONABLE SEARCH”) IN PUBLIC

There are two major objections one might offer against this definition of what kinds of investigatory methods count as a “search” in a public space. First, one might argue that it is too restrictive or that it would leave police unable to effectively investigate and deter crime. Second, one might argue that it is not restrictive enough; it places too much police work outside of the Constitution’s search and seizure limits, which presents a serious threat to privacy.

A. The Objection that the Test Leaves Police Needing Greater Freedom To Investigate

This objection requires a brief examination of how Fourth Amendment reasonableness standards apply to police investigative methods. Focusing on what kind of police activity the Fourth Amendment covers is only the first step in the two-step inquiry courts must undertake to decide if police activity violates the Constitution. The fact that the Constitution and its requirements cover a particular investigatory method does not mean that the search violates the Constitution. Rather, a search is constitutionally impermissible only when it is “unreasonable.”221 So, even if GPS tracking or video surveillance in public counts as a search, courts will allow such surveillance when it is reasonable.222 Traditional searches, such as home entries, are reasonable only if police first obtain a warrant based on probable cause.223 This was also what the Supreme Court assumed police would have to do if they wished to attach a GPS device to a car to track the driver’s movements, as they did in Jones.224 However, obtaining a warrant will not always be practical. In fact, it is implausible to require camera operators to obtain a warrant each time they record citizens’ activities in public streets. Some existing camera systems collect data continuously and such warrantless operation of video surveillance is often necessary to its effectiveness. Police cannot be expected to seek a warrant for video images the value of which is apparent only after a crime has occurred, as was the

221. Maryland v. Buie, 494 U.S. 543, 551 (1990) ("It goes without saying that the Fourth Amendment bars only unreasonable searches and seizures."); see U.S. CONST. amend. IV.


224. See Jones, 565 U.S. at 598–99 (finding that a valid warrant is necessary for a Fourth Amendment search to be reasonable).
case in the 2013 Boston Marathon bombing investigation and in the earlier July 2005 investigation of the London subway bombings. One possible response is to argue that this kind of video surveillance should not count as a search at all because, unlike the GPS surveillance in Jones, it does not target any particular person. Instead, it routinely collects information from the streets in the event that the camera’s images reveal a crime, a threat to public safety or capture evidence later needed for a criminal investigation.

The problem with this objection is that it ignores the ways in which general collection of evidence can bring the state one step away from a targeted investigation and undermine Fourth Amendment interests even before it reaches that targeting stage. Consider, for example, a hypothetical police program which uses a thermal imager to collect heat measurements from all houses in a particular region in the event that police, at a later time, decide to search the information for evidence of marijuana-growing heat lamps or other evidence of criminal activity that might be found in the heat measurements. If, as the Supreme Court ruled in Kyllo, police engage in a search when they point a thermal imaging device at a single house they suspect of housing marijuana, they must also engage in a search when they point that device at many houses and lack any particular suspicion about the residents of those houses. Even if they do not intend to examine the heat measurements they collect until some unspecified later date and are not sure what they will find, they still will have crossed the line that, according to Kyllo, makes their investigatory activity a search. Their general search has collected evidence from the interior of a home that they could not otherwise have obtained except by entry into the home. Likewise, if instead of attaching a GPS unit to a particular car as they did in Jones, police surreptitiously tacked such units onto hundreds of cars parked in a city sidewalk to see (at some unspecified later time) if any of them moved in patterns characteristic of a drug dealer or purchaser, it is hard to see why the


For general version of such an investigation would be any less a search than the targeted variant that actually occurred in Jones. Indeed, some courts have argued that it was this type of general surveillance that the Supreme Court in Kyllo suggested would be especially problematic. In Kyllo, the Court stated that while it was not a search to track a driver on public roads with use of a single beeper, it might be a search if police used such technology to conduct "drag-net-type" surveillance involving "twenty-four hour surveillance of any citizen of this country." Consequently, if video or other recording of remote activities is a search when it targets a particular individual, it should be just as much a Fourth Amendment search when police record many individuals’ activities and movement before (even long before) they decide upon whom to focus.

That does not mean, however, that police absolutely need a warrant or individualized suspicion to record activity in public space. As Christopher Slabogin argued, courts analyzing video surveillance could adapt certain aspects of their case law on roadblocks, where courts have relaxed warrant and individualized suspicion requirements; in these circumstances, they nevertheless insisted that officials incorporate privacy protections into their searches. Likewise, as argued previously, if obtaining a warrant is impossible for police using ongoing video surveillance, they might instead have to satisfy the kind of "constitutionally adequate substitute for a warrant" that the Supreme Court has sometimes demanded in certain school cases, or other situations where officials are using searches to meet a need beyond ordinary law enforcement purposes.

See, e.g., Jones, 132 S. Ct. at 952 & n.6 (deciding the case on a trespassory standard but noting that under a "reasonable expectation of privacy standard, Kyllo indicates that "drag-net" type law enforcement practices, like those involved in GPS tracking, might be problematic (quoting United States v. Knights, 460 U.S. 706, 714 (1983))).

Jones, 460 U.S. at 734–35.

See Terry v. Ohio, 392 U.S. 1, 20 (1968) (explaining that warrant and probable cause requirements may not apply in certain types of searches or police activities because such requirements are impractical under the circumstances); see also New Jersey v. T.L.O., 469 U.S. 325, 338–39 (1985) ("seizing and requiring in school settings, but refusing to lower the standard to that applicable in the prison setting.

But in Terry and its progeny, the police had to reasonably suspect a warrantless search was needed in order to reach such a conclusion.


225.
THE FOURTH AMENDMENT FUTURE

71

requiring that police have individualized suspicion, the Supreme Court has required other, system-wide privacy protections. These protections often emphasize (1) standardization, (2) unintrusiveness, and (3) clear necessity given a serious security risk. This ensures that officers have minimal discretion in their searches and that the searches are brief, reveal little information, and can often be avoided easily, given the obvious necessity, determination by a neutral magistrate would be excessive under the circumstances. While this Article does not explore how such "warrant substitutes," which have typically applied outside of the criminal context, would apply to police use of public surveillance to pursue law enforcement objectives, such an adaptation is possible. Classifying video surveillance as a search does not mean that it will be an option only when police already have the probable cause that they believe the video surveillance itself will give them.

B. The Objection that the Test Leaves Government with Too Much Opportunity for Unjustified Surveillance

1. Expanding the definition of a "search" to cover other privacy intrusions by government

While this Article argues for an extension of the Fourth Amendment to cover public surveillance, the potential for significant amounts of public surveillance that the proposed test would not cover. Consider, for example, a situation in which a police officer decides to spend an hour following a person whom she notices traveling down the street. Imagine that, while doing so, the officer snaps a picture or takes some video footage with an iPhone or digital camera, but does not use an optical zoom lens to magnify the camera's image. While such image capture would involve recording, the officer would not be recording remote activities; she would not be recording events outside of her presence. Nor would she be engaging in the functional equivalent of remote recording when she engages in close observation only of events within her field of view.

For some scholars, judges, or lawyers, this limit on Fourth Amendment coverage may well be unjustified. Indeed, Christopher

254. See Christopher Slobozian, Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Moser's Theory, 8 NW. J. C. & TECH. 1, 13-15 (2012) (suggesting that courts define a Fourth Amendment "search" as a "reason to think," but that a proportionality principle should apply when determining the necessity of a warrant or other protective measures).

255. See generally id. at 9-12 (analyzing Fourth Amendment jurisprudence and rules, redelineating "search," laying out a statutory scheme, and commencing on the proposed provisions).

256. Id. at 5-6, 9-18 (rejecting property as the best foundation for privacy laws and advocating for a broader definition akin to Katz's reasonable expectation of privacy standard); see also Slobozian, supra note 58, at 217 (framing the issue in terms of a right to privacy).

257. See Slobozian & Schumacher, supra note 199, at 732 (explaining the need for empirical study and reflection on this issue); see also Slobozian, supra note 58, at 271-72, 275-80 (detailing a further study similar to that conducted by Slobozian and Schumacher).

258. See Slobozian, supra note 211, at 51-53 (noting that in many cases, "a rougher sense exists between the Court's holdings and our subject: intrusiveness rankings"); see also Slobozian, supra note 58, at 271-72, 275-80 (detailing his more recent empirical study).

259. Slobozian, supra note 211, at 51-53.
Slobogin’s statutory proposal is even more extensive. The definition of “search,” in a well-drafted surveillance law, he argued, should cover any “effort by government to find or discern evidence of unlawful conduct.” It does not matter whether a police officer looks for such evidence with the aid of technology or “with the naked eye.” The officer who watches an individual walking down the street to see what transpires is conducting a search under this definition whether she does so with her unaided vision, binoculars, closed-circuit television, or a drone. Slobogin emphasized that focusing on a statutory formulation freed him to “[g]o[ ] beyond anything the Fourth Amendment requires, in either scope or detail.” He suggested, however, that this model statute might also help guide and sharpen thinking about Fourth Amendment rules for public surveillance.

Such a broad definition of a search certainly has some advantages. It is, as Slobogin and other scholars observe, closer in many respects to the way a layperson would define the word “search.” In common usage, a person is typically described as “searching” for something when he is engaged in a focused attempt to find it, regardless of whether he is attempting to do so in a house or an open field or whether he has any sophisticated technology to aid him. A person can search for a coin dropped on the sidewalk, for example, simply by scanning his surroundings. Moreover, this broad definition of a search deprives unscrupulous—or heavily pressured—government officials of the temptation to circumvent Fourth Amendment requirements simply by shifting to technologies or strategies that are unfamiliar to the courts. Under Slobogin’s all-

---

243. Id. at 17.
244. Id. at 5.
245. Id. at 4–5 (indicating that one purpose of his article was to resolve debates about which Fourth Amendment theories might serve as alternatives to the “mosaic theory”).
246. See Abhik Reed Amstutz, Fourth Amendment First Principles, 107 Harv. L. Rev. 767, 768 (1994) (arguing that “searching [a] vessel...in public, counts as a ‘search’ but that such a search is clearly constitutional”; Stephen F. Mead, Ruminating: Nothing New Under the Sun? A Technologically Radical Doctrine of Fourth Amendment Search, 96 Mem. L. Rev. 507, 544 (2003) (arguing that search and seizure “are (and were, at the time of the Founding) ordinary, commonplace words” and should “bear that ordinary meaning”).
247. Id. at 15–17.
251. U.S. Const. amend. IV.
252. Slobogin, supra note 236, at 17.
subjective motives—of precisely the sort that the Supreme Court has been intent on avoiding in the context of determining whether police have probable cause for a traffic stop and automobile search.235 A more modest expansion for the test described above would apply Fourth Amendment limitations to all recordings, or record creation in general, rather than covering only remote police recording. Even when an officer simply snaps an iPhone photo of what is directly in front of her, one might argue, she engages in a search. The Fourth Amendment might give her more leeway to conduct such a simple, relatively unintrusive search than it gives a team of officers operating a drone-based camera or collecting and reviewing footage from a citywide surveillance system. But such leeway would still be limited by search and seizure protection that would, for example, forbid capturing iPhone pictures of people or events that she has no reason to suspect have any connection to criminal activity.

There is, however, a problem with a rule that makes any police observation a search as soon as it is accompanied by even the simplest kind of record creation. Police activity that precisely mirrors that which individuals engage in every day would be converted into a matter of constitutional law. Thanks to the miniaturization of cameras and their incorporation into cell phones, individuals can carry cameras with them almost everywhere, and there are few activities in public spaces that are off-limits to phone and video recording. In fact, police have often found themselves being video recorded by citizens wielding iPhone cameras or other recording devices, and a number of appellate courts have found that individuals have a First Amendment right to record police in this way.236 It is conceivable that the same individual who has a constitutional right to record police officers also has a constitutional right to avoid being视频 recorded by the same police officers they are video recording.

235. See Whren v. United States, 517 U.S. 806, 811-13 (1996) (asserting that the Court has never invalidated a Fourth Amendment search based on an officer's subjective motive and that the Fourth Amendment provides the appropriate protections for challenging discriminatory police behavior).

236. See, e.g., United States v. Jacobsen, 369 F.3d 858, 866-87 (7th Cir. 2004) (holding that an Illinois eavesdropping statute that would ban nonconsensual audio-recording of public officials likely fails intermediate scrutiny and infringes on First Amendment rights); Glik v. Centennial, 665 F.3d 78, 82 (2d Cir. 2011) (emphasizing that there is a constitutional right to record police in the course of their public duties because public recording of government officials can play an essential role in sustaining "the free discussion of governmental affairs" and protection of freedom (citing Mills v. Alabama, 384 U.S. 214, 217 (1966)); Smith v. City of Cumming, 212 F.3d 1352, 1355 (11th Cir. 2000) (explaining that "'[t]he First Amendment protects the right to gather information about what public officials do on public property, and specifically, a right to record matters of public interest," including a right "to photograph or videotape police conduct").
insist that police be free from Fourth Amendment limits any time they use a technology that is generally available to private citizens. That would mean that, even as enhancements to aerial drones and GPS units make these devices a greater threat to privacy, their use by police would paradoxically become subject to less Fourth Amendment oversight—as long as private citizens are able to purchase and use such surveillance technology for their own purposes.

Use of these remote recording technologies should count a Fourth Amendment search, but this is not because these technologies are—for the moment at least—less widely used, or available to private citizens, than SmartPhone cameras. Rather, it is because remote recording technologies allow police to do something they cannot easily do with a SmartPhone, which is to generate a "precise, comprehensive record of a person's public movements"—a digital archive they can later use to engage in a frame-by-frame search.

The government might conceivably subject U.S. citizens to such a dragnet investigation even without automated recording technology that can follow an individual far from where an officer is positioned. But doing so is likely to be costly and burdensome for police. As Justice Alito stated in Jones, tracking an individual over a period of days without GPS technology is likely to require significantly more man power and police resources and is likely to be a far more complex operation.250 As Justice Breyer explained in Kinnan v. Louisiana,251 such an investigation may be in less need of constitutional restraint because its costs make it subject to heavy practical restraints.252

2. More general technology-centered approaches

Other scholars have explored ways of defining searches in public space that are less expensive but still arguably more grounded than the proposed definition offered in this Article. Another set of recent and promising proposals, for example, come from scholars who argued for a technology-based approach to what counts as a search. In contrast, however, they analyze it at a higher-level of
degenerality than in this Article, which focuses on public recording (remote or otherwise) and certain types of magnification and amplification. Professors David Gray and Danielle Citron, for example, argued for a "technology-centered approach" to determine which investigations count as Fourth Amendment searches.253 Their test would classify any technology as a search if it "has the capacity to facilitate broad programs of indiscriminate surveillance that intrude upon reasonable expectations of quantitative privacy."254 Among the technologies that enable such "pervasive surveillance" are "aerial drones, GPS-enabled tracking, and digital dossiers."255 These technologies, Gray and Citron claim, raise the same specter of authoritarianism for modern citizens that "broad and indiscriminate use of physically invasive searches and seizures" did for our predecessors.256

Another similar approach that inspired Gray and Citron's proposal is Susan Freiwald's proposal. Freiwald stated that courts can mark a line between searches and non-searches with a four-factor test that the Supreme Court and other courts have developed over the last four decades in cases addressing wiretapping or video surveillance in homes, offices, or other private spaces.257 Under this test, a method of public surveillance would count as a search when it is characterized by each (or perhaps, most) of the following elements: it is (1) hidden, in that the target is unaware of it; (2) intrusive, in the sense that it "affords law enforcement agents access to things people consider private"; (3) continuous, in that it represents an ongoing "series of intrusions" rather than a single intrusion by the state; and (4) indiscriminate, in that it "gathers up more information than necessary to establish guilt."258 GPS surveillance, she argued, will typically count as a search under these criteria because GPS units are typically hidden, record myriad details about a person's movements and activities, do so over an extended period of time, and gather

251. Id. at 434–35 (Alito, J., concurring in the judgment).
252. See id. at 436 (Alito, J., concurring in the judgment).
253. See id. at 426, 428 (Alito, J., concurring in the judgment).
254. Id. (emphasis in original).
255. See id. at 430 (Alito, J., concurring in the judgment).
256. See id. at 437 (Alito, J., concurring in the judgment).

257. See Freiwald, First Principles, supra note 32, ¶¶ 8–11 (outlining the details of the Four Factor Test, its derivation from case law, and how it supports the goals of the Fourth Amendment's protection of privacy); see also Freiwald, First Principles, supra note 32, ¶ 11 (noting that courts could apply lesser standards to those surveillance methods that do not share all four factors).
much information unrelated to criminal activity. Surveillance by an unseen drone would count as a search for the same reason. Video surveillance by street cameras is not hidden to the same extent, as pedestrians can often see the cameras on buildings or poles. But it otherwise shares the features that make GPS tracking and drone surveillance a search.

Interestingly, the earlier cases that Freiwald relies upon, which applied similar principles to cases of wiretapping and video surveillance, did not use these criteria to determine whether a certain investigatory technique was a search or a non-search. Rather, courts employed these factors to justify imposing certain "heightened procedural hurdles," beyond a showing of probable cause, on certain types of unusually threatening electronic searches.

Still, although these criteria were used to determine what hurdles the government had to overcome to make a search reasonable, they can be adapted to the task of determining what public monitoring should count as a search at all. Although police surveillance in public has traditionally been entirely outside the Fourth Amendment's coverage, when it raises the same risks for privacy and autonomy as the more intrusive forms of inside surveillance, such as wiretapping or video recording from cameras hidden in homes or businesses, then it makes sense to bring such public surveillance into Fourth Amendment territory so that courts can guard against its possible abuses. Thus, when public surveillance is hidden, intrusive, continuous, and indiscriminate (under Freiwald's test) or capable of broad and indiscriminate surveillance (under Gray and Citron's), it is, just as wiretapping and bugging—subject to constitutional limits.

Such an approach has two advantages that might, to some, make it seem preferable to a test that focuses on recording capacity, magnification, or some other specific technological feature. First, it has the virtue of offering a single standard that courts can apply not only to surveillance in public spaces, but to all kinds of wide-scale government surveillance, from wiretapping, to thermal imaging and GPS tracking. Second, like Slobogin's all-methods-covered approach above, Gray, Citron, and Freiwald's approaches are broad enough that they easily apply limits to alternative technologies (or low-tech analogues) that the government employs to circumvent Fourth Amendment limitations. For example, if police try to circumvent a Fourth Amendment restriction on remote recording by sending out officers to continuously record activities on dashboard cameras and then storing them for later analysis, Gray and Citron's test would likely still give courts all of the doctrine they need to classify such recording as a search based on its potential for broad and indiscriminate investigation of citizens' public movements or actions. Freiwald's test would also likely classify such widespread recording as a search, because it is intrusive, continuous, indiscriminate (and, if people do not see the cameras in the police cars, also hidden). Courts thus would not have to analogize this multi-officer use of individual recording devices to hidden surveillance from drones or street cameras.

271. See Gray & Citron, supra note 37 (manuscript at 5, 12-15, 50) (noting that their technology-based approach to the Fourth Amendment should serve as a guide to present and future government recording of the public and limit "broad programs of indiscriminate surveillance"); Freiwald, supra note 32, at 10, 11 (basing her test on video surveillance cases). Police could use video surveillance technology to continuously record the public in much the same way that drones might. See Freiwald, supra note 32 (applying the four-factor test and concluding that law enforcement officials should seek a warrant before engaging in GPS tracking).

273. Such general approaches offer yet another possible benefit: they may be broad enough to cover government collection and analysis of third-party video recordings. Much of the video used in the Boston Marathon investigation, for example, came from the video cameras of private businesses and individuals filming the Boston Marathon (or the aftermath of the bombings) with their own smart phone cameras. Kelly, supra note 1. Third-party records could be of similar benefit in location tracking. As Stephen Henderson has written, location data has immense value to private businesses, since it allows them to discover customer habits and patterns. Stephen E. Henderson, Learning From All Fifty States: How to Apply the Fourth Amendment and its State Analogues To Protect Third Party Information from Unreasonable Search, 50 CATH. L. REV. 375, 385-86 (2006). For example, a "business would probably like to know that customers spend an average of fifteen minutes in the store." Id. at 383-84. Furthermore, a third party's natural interest in location-tracking combined with the location-tracking capacities of "inherently ineluctable," or "cell phone" technology, make it likely that police will find all the information they need to track an individual in records already collected by private parties. Id. at 385. It is thus understandable that the constitutional justices in Jones were worried not only about official use of public cameras or government-installed GPS devices, but also about government collections of data from third-party-generated data. Justice Alito, for example, noted that ""[i]n most circumstances we are equipped with devices that permit us to ascertain the car's location at any time and that, if properly employed, can aid in the accurate navigation to and identification of the location of the car." United States v. Jones, 132 S. Ct. 945, 950 (2012) (Alito, J., concurring in the judgment). Justice Sotomayor explained that a robust approach to privacy in public may require the Supreme Court "to reconsider the premise that an individual

279. Freiwald, supra note 32.
There are, however, two disadvantages to the more abstract approach. One is the opposite of the advantage discussed above. The same generalization that allows these approaches to more easily cover a wide range of investigatory techniques also makes it less predictable which techniques will be covered by the Fourth Amendment. Consider, for example, some of the questions courts would face in assessing whether certain video- or image-capture technology is capable of broad and indiscriminate use (under Gray and Citron’s test) or ‘intrusive’ (under Freiwald’s). In defining how broad, indiscriminate or intrusive a technology is, should courts consider any technological or administrative safeguards (e.g., a rigorously enforced restriction on access) that a police department builds into its video surveillance system? Should they consider use of a surveillance technology to be a search if that technology is relatively unharrowing in its typical form but can be easily repurposed so as to let police engage in more intrusive searches? Do police engage in a search, for example, if they use recording systems that blur faces, but have no reasonable expectation of privacy in information voluntarily disclosed to third parties? If so, it is worthwhile to consider that these systems may still meet the test of ‘incidental’ surveillance that facilitates ‘statistical programs of indiscriminate surveillance’ under Gray and Citron’s test. Gray and Citron suggested that their approach would at least cover situations where a police party was acting as a state agent, and ‘that in most cases where government levering of private data resources would raise [Fourth Amendment] concerns, one or more of the [S]tate’s agents’ would be present. Id. (footnote omitted). Of course, such a state agency test would likely solve the same problem under the narrower approach suggested in this Article.

If it did not do so, Justice Stewart thus remained correct that effective Fourth Amendment protection of privacy requires a reformulation of the third-party doctrine, and that such a change is not consistent with the existing doctrine’s rationale and guidance providing why and when video footage captured in open spaces could constitute Fourth Amendment privacy interests even when it occurs in public and observable space. All in all, if we do not have any account of why it might be constitutionally problematic for the government to routinely telecopse public activities by itself, it would not be clear why it is any more problematic for it to obtain the same information from others. We thus need some approach, like the one that this Article offers, to explain when and why government recording of citizens’ activities would cross a constitutional line; the approach would also have to explain when and why authorizing the same information from third parties’ recordings might be sufficiently intrusive. Although a more general technological-oriented approach can certainly serve this role, too can a narrower non-technical approach to the problem of recording and certain instances of magnification or amplification to Fourth Amendment scrutiny.

274. See Gray and Citron, supra note 32 (manuscript at 5) (describing its test as one that looks to the potential uses and abuses of the technology as a basis for incurring Fourth Amendment scrutiny); Freiwald, Four Factor Test, supra note 32 (considering potential limits on GPS tracking).

275. See Freiwald, Four Factor Test, supra note 32 (viewing GPS tracking as a search and therefore potentially any attempt by police to track drivers as a search for the same reason).

276. See Freiwald, First Principles, supra note 32, ¶ 69 (focusing instead on the common nature of a search, not on a specific length of time, and incorporating three additional factors into the test).

277. See id. ¶¶ 50, 60 (stating that the courts should still make clear decisions on what the Constitution demands before law enforcement begins using new technologies).
this Article to classify as a "search" visual observation by police officers that is unaided by cameras or other technology.

Still, the approaches offered by Gray, Citron, and Freiwald might well end up leading courts to define the Fourth Amendment territory that the proposal here covers. Remote recording is certainly capable of the broad and indiscriminate use that, for Gray and Citron, is the hallmark of a Fourth Amendment search. Remote recording is also, as a general matter, likely to be hidden from the view of the target; the police officer doing the recording is not present (and the device doing the recording is often not visible). It is certainly continuous, and it indiscriminately captures significant amounts of information unrelated to crime. So it also satisfies Freiwald’s test. High-level magnification of reading materials or other items we assume are private is also likely to occur without our knowledge and to be intrusive and indiscriminate.278

Thus, it is plausible to view the proposal set forth in this Article as a specific application of the approaches discussed by Gray, Citron, and Freiwald, which advocate that the Supreme Court count as a search all public surveillance that eliminates the possibility for "private or anonymous action" in public space.279 Recording remote events and close magnification of details are only two examples of surveillance technologies that raise such concerns.

Yet Courts might offer greater clarity—not just to law enforcement agents but to other courts—if they start with such abstract criteria, but rather with a test that marks remote recording and high-level magnification as searches. This more modest approach also adheres more closely to the Supreme Court’s own precedent on surveillance in public spaces.280 As noted above, the Supreme Court has already stated in its tracking cases that location-monitoring technology may count as a search when used in conjunction with data-based information-gathering devices; this might include any device, like GPS, that records a person’s movements from one place to another. It has noted in its aerial surveillance cases that even when police observe a home’s curtilage or a business’s open premises from a place where the public has a right to be, their surveillance might still be a

search when it reveals intimate details about a person’s life.281 Building on such precedent in future cases on public surveillance, the Supreme Court may eventually build the framework that masks particular investigatory techniques as searches or non-searches based upon their general level of intrusiveness or their capacity to indiscriminately and continuously capture information. If and when such a framework emerges, this might also allow a link between the Court’s emerging Fourth Amendment jurisprudence on surveillance in public spaces and its jurisprudence on surveillance of Internet and phone communications. Nevertheless, even if the Supreme Court takes a more cautious and minimalist approach, there is a technological form- or design-based approach that allows it to proceed in extending Fourth Amendment protection to public surveillance.

CONCLUSION

In recent years, judges seeking to apply Fourth Amendment law to emerging surveillance technologies have faced a dilemma. On the one hand, if they continue to insist on the simple rule that public space is a Fourth Amendment-free zone, they seem to betray Fourth Amendment purposes.282 While the Fourth Amendment does not, as the Supreme Court noted in Katz, establish a "general constitutional ‘right to privacy,’"283 it does protect us from government fishing expeditions whereby police invade the private realms of our life in search of details that would justify subjecting us to an arrest or other seizure.284 Police cannot arbitrarily sift through the items in our house or the documents in our briefcase,285 so it is not clear why they should be able to create, and then sift through, video frames of people’s daytime movements through public space, especially because even acts that occur in a public space may betray aspects of their lives that are deeply private and personal. In fact, roadside cameras or drones might capture evidence not only of citizens’

278. Whether it is continuous is less clear. See Blitz, supra note 45, at 1583-84 (indicating that magnification of images caught on video surveillance implicates serious concerns, even if the Supreme Court refuses to find much relevance to such concerns); see also Freiwald, First Principles, supra note 32, ¶ 69-70 (examining the continuousness requirement in relation to such devices).

279. Blitz, supra note 45, at 1596.

280. See e.g., United States v. Jones, 565 U.S. 400, 413 (2012) (government violates the Fourth Amendment if it uses a "birdhouse" or a "dirt bike" to conduct surveillance from a driveway or a street).

281. See supra notes 124-133, 207 and accompanying text.

282. See, e.g., United States v. Jones, 565 U.S. 400, 413 (2012) (Sotomayor, J., concurring) (emphasizing that the Court must view the Fourth Amendment "as a dynamic, evolving reply to the changing technologies and social customs of each era"); United States v. Jones, 565 U.S. 400, 412 (2012) (Kagan, J., concurring) (noting that the Fourth Amendment “prohibits the government from using new technologies to surveil the specifics of an individual’s daily life without a warrant’’).


284. See Camara v. Municipal Court, 387 U.S. 523, 534-35 (1967) ("[T]he Fourteenth Amendment protects the individual against arbitrary governmental invasions.").

285. See, e.g., U.S. CONST., amend. IV (stating that the government cannot arbitrarily search a person’s "papers, and effects", without probable cause).

movements, but of their private thoughts. They might give hints about personal internal demons individuals are struggling with when they visit a psychotherapist, twelve-step group, or library. This is especially true if the state not only has a record of its citizens’ movements, but also video footage that captures facial expressions, demeanor, gait, and perhaps (with powerful magnification) the documents held in their hands.

On the other hand, if courts extend the Fourth Amendment into the realm of the public and visible, it is not at all clear how this extension should go. It seems wrong to say that every glance by police or every event they observe in the street suddenly activates a constitutional force field protecting the subject of their attention; it also seems wrong to assume that if police look a bit closer—whether by staring for a longer time, donning a better pair of glasses, or using their binoculars or iPhone—Fourth Amendment protections immediately apply. The concurring opinions in United States v. Jones rightly did not let this difficulty deter them from concluding that the Fourth Amendment applies to public space, but they also did not find a way to resolve the issue. Rather, they assumed that there is a vague, yet-to-be-identified line between public surveillance that is sufficiently brief to avoid judicial scrutiny of any kind and longer surveillance that might count as a "search."

This Article has proposed a way out of the dilemma. First, whether public surveillance counts as a Fourth Amendment search depends not on its duration or intensity, but rather on whether it uses technology that attempts to do what the Fourth Amendment was meant to stop: dragnet surveillance that creates records of activities that police can then sift through for evidence that might justify subjecting us to the coercive powers of the state. In short, this means that the Fourth Amendment should first bar the government from recording with technologies that inescapably follow citizens through public space and record them remotely whenever they can be found—no matter how far they may be from the sight or hearing of a police officer. Whether that recording lasts only a few seconds or a month, it is still a search because, by turning it on, police are...

---

286. Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) ("I would not assume that all information voluntarily disclosed to some member of the public for a lawful purpose is, for that reason alone, discoverable to Fourth Amendment purposes."); id. at 960–61, 964 (Alito, J., concurring in the judgment) (arguing that the determining factors for Fourth Amendment protection should include the duration of the intrusion and reasonable expectations of privacy, not the presence of a physical trespass).

287. Id. at 964 (Alito, J., concurring in the judgment).
Panel VII:

The Future of Nuclear Non-Proliferation

Moderator:
David Koplow
Statement for the Record

Worldwide Threat Assessment of the US Intelligence Community

Senate Armed Services Committee

James R. Clapper

Director of National Intelligence

February 26, 2015
STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT
of the
US INTELLIGENCE COMMUNITY

February 26, 2015

INTRODUCTION

Chairman McCain, Ranking Member Reed, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community’s 2015 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community’s extraordinary men and women, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America’s interests anywhere in the world.

Information available as of February 13, 2015 was used in the preparation of this assessment.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>GLOBAL THREATS</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td>1</td>
</tr>
<tr>
<td>Counterintelligence</td>
<td>4</td>
</tr>
<tr>
<td>Terrorism</td>
<td>4</td>
</tr>
<tr>
<td>Weapons of Mass Destruction and Proliferation</td>
<td>5</td>
</tr>
<tr>
<td>Space and Counterspace</td>
<td>7</td>
</tr>
<tr>
<td>Transnational Organized Crime</td>
<td>8</td>
</tr>
<tr>
<td>Economics and Natural Resources</td>
<td>9</td>
</tr>
<tr>
<td>Human Security</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGIONAL THREATS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Middle East and North Africa</td>
<td>13</td>
</tr>
<tr>
<td>Iraq</td>
<td>13</td>
</tr>
<tr>
<td>Syria</td>
<td>13</td>
</tr>
<tr>
<td>Islamic State of Iraq and the Levant</td>
<td>14</td>
</tr>
<tr>
<td>Iran</td>
<td>14</td>
</tr>
<tr>
<td>Libya</td>
<td>15</td>
</tr>
<tr>
<td>Yemen</td>
<td>15</td>
</tr>
<tr>
<td>Lebanon</td>
<td>15</td>
</tr>
<tr>
<td>Egypt</td>
<td>16</td>
</tr>
<tr>
<td>Tunisia</td>
<td>16</td>
</tr>
<tr>
<td>Europe</td>
<td>16</td>
</tr>
<tr>
<td>Turkey</td>
<td>16</td>
</tr>
<tr>
<td>Key Partners</td>
<td>17</td>
</tr>
<tr>
<td>Russia and Eurasia</td>
<td>17</td>
</tr>
<tr>
<td>Russia</td>
<td>17</td>
</tr>
<tr>
<td>Ukraine, Moldova, and Belarus</td>
<td>18</td>
</tr>
<tr>
<td>The Caucasus and Central Asia</td>
<td>19</td>
</tr>
<tr>
<td>Region</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>East Asia</td>
<td>19</td>
</tr>
<tr>
<td>China</td>
<td>19</td>
</tr>
<tr>
<td>North Korea</td>
<td>20</td>
</tr>
<tr>
<td>South Asia</td>
<td>20</td>
</tr>
<tr>
<td>Afghanistan</td>
<td>20</td>
</tr>
<tr>
<td>Pakistan</td>
<td>21</td>
</tr>
<tr>
<td>India</td>
<td>21</td>
</tr>
<tr>
<td>Sub-Saharan Africa</td>
<td>22</td>
</tr>
<tr>
<td>West Africa</td>
<td>22</td>
</tr>
<tr>
<td>Sudan</td>
<td>22</td>
</tr>
<tr>
<td>South Sudan</td>
<td>22</td>
</tr>
<tr>
<td>Nigeria</td>
<td>23</td>
</tr>
<tr>
<td>Somalia</td>
<td>23</td>
</tr>
<tr>
<td>Lord's Resistance Army</td>
<td>23</td>
</tr>
<tr>
<td>Central African Republic</td>
<td>23</td>
</tr>
<tr>
<td>The Sahel</td>
<td>23</td>
</tr>
<tr>
<td>Latin America and the Caribbean</td>
<td>24</td>
</tr>
<tr>
<td>Cuba</td>
<td>24</td>
</tr>
<tr>
<td>Central America</td>
<td>24</td>
</tr>
<tr>
<td>Venezuela</td>
<td>24</td>
</tr>
<tr>
<td>Haiti</td>
<td>25</td>
</tr>
</tbody>
</table>
GLOBAL THREATS

CYBER

Strategic Assessment

Cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology (ICT) networks that support US Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a “Cyber Armageddon” scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.

- A growing number of computer forensic studies by industry experts strongly suggest that several nations—including Iran and North Korea—have undertaken offensive cyber operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises.

Risk. Despite ever-improving network defenses, the diverse possibilities for remote hacking intrusions, supply chain operations to insert compromised hardware or software, and malevolent activities by human insiders will hold nearly all ICT systems at risk for years to come. In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed. Moreover, the risk calculus employed by some private sector entities does not adequately account for foreign cyber threats or the systemic interdependencies between different critical infrastructure sectors.

Costs. During 2014, we saw an increase in the scale and scope of reporting on malevolent cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information (PII) compromised, or remediation costs incurred by US victims. For example:

- After the 2012-13 distributed denial of service (DDOS) attacks on the US financial sector, JPMorgan Chase (JPMorgan) announced plans for annual cyber security expenditures of $250 million by the end of 2014. After the company suffered a hacking intrusion in 2014, JPMorgan’s CEO said he would probably double JPMorgan’s annual computer security budget within the next five years.

- The 2014 data breach at Home Depot exposed information from 56 million credit/debit cards and 53 million customer email addresses. Home Depot estimated the cost of the breach to be $62 million.

- In 2014, unauthorized computer intrusions were detected on the networks of the Office of Personnel Management (OPM) as well as its contractors, US Investigations Services (USIS) and KeyPoint
Government Solutions. The two contractors were involved in processing sensitive PII related to national security clearances for Federal Government employees.

- In August 2014, the US company, Community Health Systems, informed the Securities and Exchange Commission that it believed hackers “originating from China” had stolen PII on 4.5 million individuals.

**Attribution.** Although cyber operators can infiltrate or disrupt targeted ICT networks, most can no longer assume that their activities will remain undetected. Nor can they assume that if detected, they will be able to conceal their identities. Governmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions.

- In May 2014, the US Department of Justice indicted five officers from China’s Peoples’ Liberation Army on charges of hacking US companies.

- In December 2014, computer security experts reported that members of an Iranian organization were responsible for computer operations targeting US military, transportation, public utility, and other critical infrastructure networks.

**Deterrence.** Numerous actors remain undeterred from conducting economic cyber espionage or perpetrating cyber attacks. The absence of universally accepted and enforceable norms of behavior in cyberspace has contributed to this situation. The motivation to conduct cyber attacks and cyber espionage will probably remain strong because of the relative ease of these operations and the gains they bring to the perpetrators. The result is a cyber environment in which multiple actors continue to test their adversaries’ technical capabilities, political resolve, and thresholds. The muted response by most victims to cyber attacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation. Additionally, even when a cyber attack can be attributed to a specific actor, the forensic attribution often requires a significant amount of time to complete. Long delays between the cyber attack and determination of attribution likewise reinforce a permissive environment.

**Threat Actors**

Politically motivated cyber attacks are now a growing reality, and foreign actors are reconnoitering and developing access to US critical infrastructure systems, which might be quickly exploited for disruption if an adversary’s intent became hostile. In addition, those conducting cyber espionage are targeting US government, military, and commercial networks on a daily basis. These threats come from a range of actors, including: (1) nation states with highly sophisticated cyber programs (such as Russia or China), (2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea), (3) profit-motivated criminals, and (4) ideologically motivated hackers or extremists. Distinguishing between state and non-state actors within the same country is often difficult—especially when those varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber tools.

**Russia.** Russia’s Ministry of Defense is establishing its own cyber command, which—according to senior Russian military officials—will be responsible for conducting offensive cyber activities, including
propaganda operations and inserting malware into enemy command and control systems. Russia’s armed forces are also establishing a specialized branch for computer network operations.

- Computer security studies assert that unspecified Russian cyber actors are developing means to access industrial control systems (ICS) remotely. These systems manage critical infrastructures such as electric power grids, urban mass-transit systems, air-traffic control, and oil and gas distribution networks. These unspecified Russian actors have successfully compromised the product supply chains of three ICS vendors so that customers download exploitative malware directly from the vendors’ websites along with routine software updates, according to private sector cyber security experts.

**China.** Chinese economic espionage against US companies remains a significant issue. The “advanced persistent threat” activities continue despite detailed private sector reports, public indictments, and US demarches, according to a computer security study. China is an advanced cyber actor; however, Chinese hackers often use less sophisticated cyber tools to access targets. Improved cyber defenses would require hackers to use more sophisticated skills and make China’s economic espionage more costly and difficult to conduct.

**Iran.** Iran very likely values its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes, as well as a sophisticated means of collecting intelligence. Iranian actors have been implicated in the 2012-13 DDOS attacks against US financial institutions and in the February 2014 cyber attack on the Las Vegas Sands casino company.

**North Korea.** North Korea is another state actor that uses its cyber capabilities for political objectives. The North Korean Government was responsible for the November 2014 cyber attack on Sony Pictures Entertainment (SPE), which stole corporate information and introduced hard drive erasing malware into the company’s network infrastructure, according to the FBI. The attack coincided with the planned release of a SPE feature film satire that depicted the planned assassination of the North Korean president.

**Terrorists.** Terrorist groups will continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers will probably conduct low-level cyber attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors.

**Integrity of Information**

Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data-deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e. accuracy and reliability) instead of deleting it or disrupting access to it. Decisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.
• Successful cyber operations targeting the integrity of information would need to overcome any institutionalized checks and balances designed to prevent the manipulation of data, for example, market monitoring and clearing functions in the financial sector.

COUNTERINTELLIGENCE

We assess that the leading state intelligence threats to US interests in 2015 will continue to be Russia and China, based on their capabilities, intent, and broad operational scopes. Other states in South Asia, the Near East, and East Asia will pose increasingly sophisticated local and regional intelligence threats to US interests. For example, Iran’s intelligence and security services continue to view the United States as a primary threat and have stated publicly that they monitor and counter US activities in the region.

Penetrating the US national decisionmaking apparatus and Intelligence Community will remain primary objectives for foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions dealing with defense, energy, finance, dual-use technology, and other areas will be a persistent threat to US interests.

Non-state entities, including transnational organized criminals and terrorists, will continue to employ human, technical, and cyber intelligence capabilities that present a significant counterintelligence challenge. Like state intelligence services, these non-state entities recruit sources and perform physical and technical surveillance to facilitate their illegal activities and avoid detection and capture.

The internationalization of critical US supply chains and service infrastructure, including for the ICT, civil infrastructure, and national security sectors, increases the potential for subversion. This threat includes individuals, small groups of “hacktivists,” commercial firms, and state intelligence services.

Trusted insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2015. The technical sophistication and availability of information technology that can be used for nefarious purposes exacerbates this threat.

TERRORISM

Sunni violent extremists are gaining momentum and the number of Sunni violent extremist groups, members, and safe havens is greater than at any other point in history. These groups challenge local and regional governance and threaten US allies, partners, and interests. The threat to key US allies and partners will probably increase, but the extent of the increase will depend on the level of success that Sunni violent extremists achieve in seizing and holding territory, whether or not attacks on local regimes and calls for retaliation against the West are accepted by their key audiences, and the durability of the US-led coalition in Iraq and Syria.
Sunni violent extremists have taken advantage of fragile or unstable Muslim-majority countries to make territorial advances, seen in Syria and Iraq, and will probably continue to do so. They also contribute to regime instability and internal conflict by engaging in high levels of violence. Most will be unable to seize and hold territory on a large scale, however, as long as local, regional, and international support and resources are available and dedicated to halting their progress. The increase in the number of Sunni violent extremist groups also will probably be balanced by a lack of cohesion and authoritative leadership. Although the January 2015 attacks against Charlie Hebdo in Paris is a reminder of the threat to the West, most groups place a higher priority on local concerns than on attacking the so-called far enemy—the United States and the West—as advocated by core al-Qaeda.

Differences in ideology and tactics will foster competition among some of these groups, particularly if a unifying figure or group does not emerge. In some cases, groups—even if hostile to each other—will ally against common enemies. For example, some Sunni violent extremists will probably gain support from like-minded insurgent or anti-regime groups or within disaffected or disenfranchised communities because they share the goal of radical regime change.

Although most homegrown violent extremists (HVEs) will probably continue to aspire to travel overseas, particularly to Syria and Iraq, they will probably remain the most likely Sunni violent extremist threat to the US homeland because of their immediate and direct access. Some might have been inspired by calls by the Islamic State of Iraq and the Levant (ISIL) in late September for individual jihadists in the West to retaliate for US-led airstrikes on ISIL. Attacks by lone actors are among the most difficult to warn about because they offer few or no signatures.

If ISIL were to substantially increase the priority it places on attacking the West rather than fighting to maintain and expand territorial control, then the group’s access to radicalized Westerners who have fought in Syria and Iraq would provide a pool of operatives who potentially have access to the United States and other Western countries. Since the conflict began in 2011, more than 20,000 foreign fighters—at least 3,400 of whom are Westerners—have gone to Syria from more than 90 countries.

**WEAPONS OF MASS DESTRUCTION AND PROLIFERATION**

Nation-states’ efforts to develop or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and allies. Syrian regime use of chemical weapons against the opposition further demonstrates that the threat of WMD is real. The time when only a few states had access to the most dangerous technologies is past. Biological and chemical materials and technologies, almost always dual-use, move easily in the globalized economy, as do personnel with the scientific expertise to design and use them. The latest discoveries in the life sciences also diffuse rapidly around the globe.

**Iran Preserving Nuclear Weapons Option**

We continue to assess that Iran’s overarching strategic goals of enhancing its security, prestige, and regional influence have led it to pursue capabilities to meet its civilian goals and give it the ability to build
missile-deliverable nuclear weapons, if it chooses to do so. We do not know whether Iran will eventually decide to build nuclear weapons.

We also continue to assess that Iran does not face any insurmountable technical barriers to producing a nuclear weapon, making Iran’s political will the central issue. However, Iranian implementation of the Joint Plan of Action (JPOA) has at least temporarily inhibited further progress in its uranium enrichment and plutonium production capabilities and effectively eliminated Iran’s stockpile of 20 percent enriched uranium. The agreement has also enhanced the transparency of Iran’s nuclear activities, mainly through improved International Atomic Energy Agency (IAEA) access and earlier warning of any effort to make material for nuclear weapons using its safeguarded facilities.

We judge that Tehran would choose ballistic missiles as its preferred method of delivering nuclear weapons, if it builds them. Iran’s ballistic missiles are inherently capable of delivering WMD, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Iran’s progress on space launch vehicles—along with its desire to deter the United States and its allies—provides Tehran with the means and motivation to develop longer-range missiles, including intercontinental ballistic missiles (ICBMs).

**North Korea Developing WMD-Applicable Capabilities**

North Korea’s nuclear weapons and missile programs pose a serious threat to the United States and to the security environment in East Asia. North Korea’s export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance to Syria’s construction of a nuclear reactor, destroyed in 2007, illustrate its willingness to proliferate dangerous technologies.

In 2013, following North Korea’s third nuclear test, Pyongyang announced its intention to “refurbish and restart” its nuclear facilities, to include the uranium enrichment facility at Yongbyon, and to restart its graphite-moderated plutonium production reactor that was shut down in 2007. We assess that North Korea has followed through on its announcement by expanding its Yongbyon enrichment facility and restarting the reactor.

North Korea has also expanded the size and sophistication of its ballistic missile forces, ranging from close-range ballistic missiles to ICBMs, while continuing to conduct test launches. In 2014, North Korea launched an unprecedented number of ballistic missiles.

Pyongyang is committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States and has publicly displayed its KN08 road-mobile ICBM twice. We assess that North Korea has already taken initial steps toward fielding this system, although the system has not been flight-tested.

Because of deficiencies in their conventional military forces, North Korean leaders are focused on developing missile and WMD capabilities, particularly building nuclear weapons. Although North Korean state media regularly carries official statements on North Korea’s justification for building nuclear weapons and threatening to use them as a defensive or retaliatory measure, we do not know the details of Pyongyang’s nuclear doctrine or employment concepts. We have long assessed that, in Pyongyang’s view, its nuclear capabilities are intended for deterrence, international prestige, and coercive diplomacy.
China's Expanding Nuclear Forces

The People’s Liberation Army’s (PLA’s) Second Artillery Force continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China’s strategic deterrent by providing a second strike capability. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines, armed with JL-2 SLBMs, will give the PLA Navy its first long-range, sea-based nuclear capability. We assess that the Navy will soon conduct its first nuclear deterrence patrols.

Russia’s New Intermediate-Range Cruise Missile

Russia has developed a new cruise missile that the United States has declared to be in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. In 2013, Sergei Ivanov, a senior Russian administration official, commented in an interview how the world had changed since the time the INF Treaty was signed 1987 and noted that Russia was “developing appropriate weapons systems” in light of the proliferation of intermediate- and shorter-range ballistic missile technologies around the world. Similarly, as far back as 2007, Ivanov publicly announced that Russia had tested a ground-launched cruise missile for its Iskander weapon system, whose range complied with the INF Treaty “for now.” The development of a cruise missile that is inconsistent with INF, combined with these statements about INF, calls into question Russia’s commitment to this treaty.

WMD Security in Syria

In June 2014, Syria’s declared CW stockpile was removed for destruction by the international community. The most hazardous chemical agents were destroyed aboard the MV CAPE RAY as of August 2014. The United States and its allies continue to work closely with the Organization for the Prohibition of Chemical Weapons (OPCW) to verify the completeness and accuracy of Syria’s Chemical Weapons Convention (CWC) declaration. We judge that Syria, despite signing the treaty, has used chemicals as a means of warfare since accession to the CWC in 2013. Furthermore, the OPCW continues to investigate allegations of chlorine use in Syria.

SPACE AND COUNTERSPACE

Threats to US space systems and services will increase during 2015 and beyond as potential adversaries pursue disruptive and destructive counterspace capabilities. Chinese and Russian military leaders understand the unique information advantages afforded by space systems and services and are developing capabilities to deny access in a conflict. Chinese military writings highlight the need to interfere with, damage, and destroy reconnaissance, navigation, and communication satellites. China has satellite jamming capabilities and is pursuing antisatellite systems. In July 2014, China conducted a non-destructive antisatellite missile test. China conducted a previous destructive test of the system in 2007, which created long-lived space debris. Russia’s 2010 Military Doctrine emphasizes space defense as a vital component of its national defense. Russian leaders openly assert that the Russian armed forces
have antisatellite weapons and conduct antisatellite research. Russia has satellite jammers and is pursuing antisatellite systems.

**TRANSNATIONAL ORGANIZED CRIME**

Transnational Organized Crime (TOC) is a global, persistent threat to our communities at home and our interests abroad. Savvy, profit-driven criminal networks traffic in drugs, persons, wildlife, and weapons; corrode security and governance; undermine legitimate economic activity and the rule of law; cost economies important revenue; and undercut US development efforts.

**Drug Trafficking**

Drug trafficking will remain a major TOC threat to the United States. Mexico is the largest foreign producer of US-bound marijuana, methamphetamines, and heroin, and the conduit for the overwhelming majority of US-bound cocaine from South America. The drug trade also undermines US interests abroad, eroding stability in parts of Africa and Latin America; Afghanistan accounts for 80 percent of the world’s opium production. Weak Central American states will continue to be the primary transit area for the majority of US-bound cocaine. The Caribbean is becoming an increasingly important secondary transit area for US- and European-bound cocaine. In 2013, the world’s capacity to produce heroin reached the second highest level in nearly 20 years, increasing the likelihood that the drug will remain accessible and inexpensive in consumer markets in the United States, where heroin-related deaths have surged since 2007. New psychoactive substances (NPS), including synthetic cannabinoids and synthetic cathinones, pose an emerging and rapidly growing global public health threat. Since 2009, US law enforcement officials have encountered more than 240 synthetic compounds. Worldwide, 348 new psychoactive substances had been identified, exceeding the number of 234 illicit substances under international controls.

**Criminals Profiting from Global Instability**

Transnational criminal organizations will continue to exploit opportunities in ongoing conflicts to destabilize societies, economies, and governance. Regional unrest, population displacements, endemic corruption, and political turmoil will provide openings that criminals will exploit for profit and to improve their standing relative to other power brokers.

**Corruption**

Corruption facilitates transnational organized crime and vice versa. Both phenomena exacerbate other threats to local, regional, and international security. Corruption exists at some level in all countries; however, the symbiotic relationship between government officials and TOC networks is particularly pernicious in some countries. One example is Russia, where the nexus among organized crime, state actors, and business blurs the distinction between state policy and private gain.
Human Trafficking

Human trafficking remains both a human rights concern and a challenge to international security. Trafficking in persons has become a lucrative source of revenue—estimated to produce tens of billions of dollars annually. Human traffickers leverage corrupt officials, porous borders, and lax enforcement to ply their illicit trade. This exploitation of human lives for profit continues to occur in every country in the world—undermining the rule of law and corroding legitimate institutions of government and commerce.

Wildlife Trafficking

Illicit trade in wildlife, timber, and marine resources endangers the environment, threatens rule of law and border security in fragile regions, and destabilizes communities that depend on wildlife for biodiversity and ecotourism. Increased demand for ivory and rhino horn in Asia has triggered unprecedented increases in poaching in Africa. Criminal elements, often in collusion with corrupt government officials or security forces, are involved in poaching and movement of ivory and rhino horn across Africa. Poaching presents significant security challenges for militaries and police forces in African nations, which often are outgunned by poachers and their allies. Illegal, unreported, and unregulated fishing threatens food security and the preservation of marine resources. It often occurs concurrently with forced labor in the fishing industry.

Theft of Cultural Properties, Artifacts, and Antiquities

Although the theft and trafficking of cultural heritage and art are traditions as old as the cultures they represent, transnational organized criminals are acquiring, transporting, and selling valuable cultural property and art more swiftly, easily, and stealthily. These criminals operate on a global scale without regard for laws, borders, nationalities or the significance of the treasures they smuggle.

ECONOMICS AND NATURAL RESOURCES

The global economy continues to adjust to and recover from the global financial crisis that began in 2008; economic growth since that period is lagging behind that of the previous decade. Resumption of sustained growth has been elusive for many of the world’s largest economies, particularly in European countries and Japan. The prospect of diminished or forestalled recoveries in these developed economies as well as disappointing growth in key developing countries has contributed to a readjustment of energy and commodity markets.

Energy and Commodities

Energy prices experienced sharp declines during the second half of 2014. Diminishing global growth prospects, OPEC’s decision to maintain its output levels, rapid increases in unconventional oil production in Canada and the United States, and the partial resumption of some previously sidelined output in Libya and elsewhere helped drive down prices by more than half since July, the first substantial decline since 2008-09. Lower-priced oil and gas will give a boost to the global economy, with benefits enjoyed by importers more than outweighing the costs to exporters.
Macroeconomic Stability

Extraordinary monetary policy or "quantitative easing" has helped revive growth in the United States since the global financial crisis. However, this recovery and the prospect of higher returns in the United States will probably continue to draw investment capital from the rest of the world, where weak growth has left interest rates depressed.

Global output improved slightly in 2014 but continued to lag the growth rates seen before 2008. Since 2008, the worldwide GDP growth rate has averaged about 3.2 percent, well below its 20-year, pre-GFC average of 3.9 percent. Looking ahead, prospects for slowing economic growth in Europe and China do not bode well for the global economic environment.

Economic growth has been inconsistent among developed and developing economies alike. Outside of the largest economies—the United States, the EU, and China—economic growth largely stagnated worldwide in 2014, slowing to 2.1 percent. As a result, the difference in growth rates of developing countries and developed countries continued to narrow—to 2.6 percentage points. This gap, smallest in more than a decade, underscores the continued weakness in emerging markets, whose previously much-higher average growth rates helped drive global growth.

HUMAN SECURITY

Critical Trends Converging

Several trends are converging that will probably increase the frequency of shocks to human security in 2015. Emerging infectious diseases and deficiencies in international state preparedness to address them remain a threat, exemplified by the epidemic spread of the Ebola virus in West Africa. Extremes in weather combined with public policies that affect food and water supplies will probably exacerbate humanitarian crises. Many states and international institutions will look to the United States in 2015 for leadership to address human security issues, particularly environment and global health, as well as those caused by poor or abusive governance.

Global trends in governance are negative and portend growing instability. Poor and abusive governance threatens the security and rights of individuals and civil society in many countries throughout the world. The overall risk for mass atrocities—driven in part by increasing social mobilization, violent conflict, and a diminishing quality of governance—is growing. Incidents of religious persecution also are on the rise. Legal restrictions on NGOs and the press, particularly those that expose government shortcomings or lobby for reforms, will probably continue.

Infectious Disease Continues To Threaten Human Security Worldwide

Infectious diseases are among the foremost health security threats. A more crowded and interconnected world is increasing the opportunities for human and animal diseases to emerge and spread globally. This has been demonstrated by the emergence of Ebola in West Africa on an unprecedented scale. In
addition, military conflicts and displacement of populations with loss of basic infrastructure can lead to spread of disease. Climate change can also lead to changes in the distribution of vectors for diseases.

- The Ebola outbreak, which began in late 2013 in a remote area of Guinea, quickly spread into neighboring Liberia and Sierra Leone and then into dense urban transportation hubs, where it began spreading out of control. Gaps in disease surveillance and reporting, limited health care resources, and other factors contributed to the outpacing of the international community’s response in West Africa. Isolated Ebola cases appeared outside of the most affected countries—notably in Spain and the United States—and the disease will almost certainly continue in 2015 to threaten regional economic stability, security, and governance.

- Antimicrobial drug resistance is increasingly threatening global health security. Seventy percent of known bacteria have acquired resistance to at least one antibiotic that is used to treat infections, threatening a return to the pre-antibiotic era. Multidrug-resistant tuberculosis has emerged in China, India, Russia, and elsewhere. During the next twenty years, antimicrobial drug-resistant pathogens will probably continue to increase in number and geographic scope, worsening health outcomes, straining public health budgets, and harming US interests throughout the world.

- MERS, a novel virus from the same family as SARS, emerged in 2012 in Saudi Arabia. Isolated cases migrated to Southeast Asia, Europe, and the United States. Cases of highly pathogenic influenza are also continuing to appear in different regions of the world. HIV/AIDS and malaria, although trending downward, remain global health priorities. In 2013, 2.1 million people were newly infected with HIV and 584,000 were killed by malaria, according to the World Health Organization. Diarrheal diseases like cholera continue to take the lives of 800,000 children annually.

- The world’s population remains vulnerable to infectious diseases because anticipating which pathogen might spread from animals to humans or if a human virus will take a more virulent form is nearly impossible. For example, if a highly pathogenic avian influenza virus like H7N9 were to become easily transmissible among humans, the outcome could be far more disruptive than the great influenza pandemic of 1918. It could lead to global economic losses, the unseating of governments, and disturbance of geopolitical alliances.

**Extreme Weather Exacerbating Risks to Global Food and Water Security**

Extreme weather, climate change, and public policies that affect food and water supplies will probably create or exacerbate humanitarian crises and instability risks. Globally averaged surface temperature rose approximately 0.8 degrees Celsius (about 1.4 degrees Fahrenheit) from 1951 to 2014; 2014 was warmest on earth since recordkeeping began. This rise in temperature has probably caused an increase in the intensity and frequency of both heavy precipitation and prolonged heat waves and has changed the spread of certain diseases. This trend will probably continue. Demographic and development trends that concentrate people in cities—often along coasts—will compound and amplify the impact of extreme weather and climate change on populations. Countries whose key systems—food, water, energy, shelter, transportation, and medical—are resilient will be better able to avoid significant economic and human losses from extreme weather.
• Global food supplies will probably be adequate for 2015 but are becoming increasingly fragile in Africa, the Middle East, and South Asia. The risks of worsening food insecurity in regions of strategic importance to the United States will increase because of threats to local food availability, lower purchasing power, and counterproductive government policies. Price shocks will result if extreme weather or disease patterns significantly reduce food production in multiple areas of the world, especially in key exporting countries.

• Risks to freshwater supplies—due to shortages, poor quality, floods, and climate change—are growing. These problems hinder the ability of countries to produce food and generate energy, potentially undermining global food markets and hobbling economic growth. Combined with demographic and economic development pressures, such problems will particularly hinder the efforts of North Africa, the Middle East, and South Asia to cope with their water problems. Lack of adequate water might be a destabilizing factor in countries that lack the management mechanisms, financial resources, political will, or technical ability to solve their internal water problems.

• Some states are heavily dependent on river water controlled by upstream nations. When upstream water infrastructure development threatens downstream access to water, states might attempt to exert pressure on their neighbors to preserve their water interests. Such pressure might be applied in international forums and also includes pressing investors, nongovernmental organizations, and donor countries to support or halt water infrastructure projects. Some countries will almost certainly construct and support major water projects. Over the longer term, wealthier developing countries will also probably face increasing water-related social disruptions. Developing countries, however, are almost certainly capable of addressing water problems without risk of state failure. Terrorist organizations might also increasingly seek to control or degrade water infrastructure to gain revenue or influence populations.

Increase in Global Instability Risk

Global political instability risks will remain high in 2015 and beyond. Mass atrocities, sectarian or religious violence, and curtailed NGO activities will all continue to increase these risks. Declining economic conditions are contributing to risk of instability or internal conflict.

• Roughly half of the world’s countries not already experiencing or recovering from instability are in the “most risk” and “significant risk” categories for regime-threatening and violent instability through 2015.

• Overall international will and capability to prevent or mitigate mass atrocities will probably diminish in 2015 owing to reductions in government budgets and spending.

• In 2014, about two dozen countries increased restrictions on NGOs. Approximately another dozen also plan to do so in 2015, according to the International Center for Nonprofit Law.
REGIONAL THREATS

MIDDLE EAST AND NORTH AFRICA

Iraq

Over six months into the coalition campaign against the Islamic State of Iraq and the Levant (ISIL), the frontlines against the group in Iraq have largely stabilized; no side is able to muster the resources necessary to attain its territorial ambitions. The Iraqi Security Forces (ISF), Peshmerga, Shia militants, and a few tribal allies—bolstered by air and artillery strikes, weapons, and advice from the United States, Arab and Western allies, and Iran—have prevented ISIL from gaining large swaths of additional territory.

Sectarian conflict in mixed Shia-Sunni areas in and around Baghdad that can undermine progress against ISIL is growing. ISF and Shia militants are conducting a campaign of retribution killings and forced displacement of Sunni civilians in several areas contested by Sunni militants.

Since taking office, Prime Minister al-Abadi has taken steps to change the ethno-sectarian tone in Baghdad, including engaging Sunni tribal leaders and reaching a tentative oil agreement with the Kurdistan Regional Government. However, the ethno-sectarian nature of security operations and persistent distrust among Iraqi leaders risk undermining Abadi’s nascent political progress.

Syria

The Syrian regime made consistent gains in 2014 in parts of western Syria that it considers key, retaking ground in eastern Damascus, Homs, and Latakia; it is close to surrounding Aleppo city. The regime will require years to reassert significant control over the country.

- The bulk of the opposition in the north is fighting on three fronts—against the regime, the al-Qa’ida- affiliated Nusra Front, and ISIL. The opposition in the south has made steady gains in areas that the regime has not made a priority and where ISIL has only a limited presence.

The stability of Syria’s neighbors is at risk due to the country’s prolonged conflict, which will strain regional economies forced to absorb millions of refugees. The conflict will also encourage regional sectarianism and continue to incubate extremist groups that will use Syria as a launching pad for attacks across the Middle East.

- The Syrian conflict is also putting huge economic and resource strains on countries in the region primarily due to the nearly 4 million refugees fleeing the conflict. Most of the refugees have fled to neighboring states. More than 620,000 are in Jordan; almost 1.6 million are in Turkey; almost 1.2 million are in Lebanon; and more than 240,000 are in Iraq. These states have requested additional international support to manage the influx.
Islamic State of Iraq and the Levant

In an attempt to strengthen its self-declared caliphate, ISIL probably plans to conduct operations against regional allies, Western facilities, and personnel in the Middle East; it has already executed Western and Japanese hostages as well as a Jordanian Air Force pilot. ISIL leader Abu Bakr al-Baghdadi outlined the group's ambitious external goals, including the expansion of the caliphate into the Arabian Peninsula and North Africa and attacks against Western, regional, and Shia interests, according to a public statement in November 2014.

- In September 2014, ISIL publicly called on all Sunnis to retaliate for US-led airstrikes in Iraq and Syria, advocating the targeting of law enforcement and other government officials using any means available. Individuals from Europe and North America who have trained and fought with ISIL can return home and conduct attacks either on their own or on ISIL's behalf. The French citizen arrested in May 2014 for a shooting at a Jewish museum in Brussels had returned from fighting, probably with ISIL in Syria, and was wrapped in a flag with ISIL inscriptions when he was apprehended. We do not know whether he acted at ISIL's behest.

Iran

The Islamic Republic of Iran is an ongoing threat to US national interests because of its support to the Asad regime in Syria, promulgation of anti-Israeli policies, development of advanced military capabilities, and pursuit of its nuclear program. President Ruhani—a longstanding member of the regime establishment—will not depart from Iran's national security objectives of protecting the regime and enhancing Iranian influence abroad, even while attempting different approaches to achieve these goals. He requires Supreme Leader Khamenei's support to continue engagement with the West, moderate foreign policy, and ease social restrictions within Iran.

Iran possesses a substantial inventory of theater ballistic missiles capable of reaching as far as some areas of southeastern Europe. Tehran is developing increasingly sophisticated missiles and improving the range and accuracy of its other missile systems. Iran is also acquiring advanced naval and aerospace capabilities, including naval mines, small but capable submarines, coastal defense cruise missile batteries, attack craft, anti-ship missiles, and armed unmanned aerial vehicles.

In Iraq and Syria, Iran seeks to preserve friendly governments, protect Shia interests, defeat Sunni extremists, and marginalize US influence. The rise of ISIL has prompted Iran to devote more resources to blunting Sunni extremist advances that threaten Iran's regional allies and interests. Iran's security services have provided robust military support to Baghdad and Damascus, including arms, advisers, funding, and direct combat support. Both conflicts have allowed Iran to gain valuable on-the-ground experience in counterinsurgency operations. Iranian assistance has been instrumental in expanding the capabilities of Shia militants in Iraq. The ISIL threat has also reduced Iraqi resistance to integrating those militants, with Iranian help, into the Iraqi Security Forces, but Iran has uneven control over these groups.

Despite Iran's intentions to dampen sectarianism, build responsive partners, and deescalate tensions with Saudi Arabia, Iranian leaders—particularly within the security services—are pursuing policies with negative secondary consequences for regional stability and potentially for Iran. Iran's actions to protect and empower Shia communities are fueling growing fears and sectarian responses.
Libya

We assess that Libya will remain volatile in 2015. Political polarization and broadening militia violence have pushed Libya into a civil war. Nearly four years since the revolution that toppled Qadhafi, rival governments have emerged, leaving the country with no clear legitimate political authority or credible security forces. Militias aligned with the rival governments continue to vie for dominance in Tripoli and Benghazi.

- In Benghazi, fighting that began in May 2014 is ongoing between forces aligned with former General Khalifa Hafar’s Operation Dignity forces and Ansar al-Sharia (AAS) and allied groups. In Tripoli, the Libya Dawn militias have driven their Zintani militia rivals out of the city, but fighting continues southwest of Tripoli.

- UN efforts to facilitate a negotiated resolution between Libya’s rival governments have shown limited momentum but as of early February 2015 have not made tangible progress toward a unity government or a durable cease-fire.

Extremists and terrorists from al-Qa’ida-affiliated and allied groups are using Libya’s permissive security environment as a safe haven to plot attacks, including against Western interests in Libya and the region. ISIL also has declared the country part of its caliphate, and ISIL-aligned extremists are trying to institute sharia in parts of the country.

Yemen

The Huthis have emerged as the most powerful group in Yemen since taking Sanaa last fall and are poised to dominate the political process after President’s Hadi’s resignation and their dissolution of the government. The group, however, continues to face resistance as it expands toward the south and east. Southern Yemeni leaders have been alarmed by the Huthi’s consolidation of control in Sanaa and are poised to oppose further Huthi expansion south. Al-Qa’ida in the Arabian Peninsula (AQAP) has taken advantage of many Sunni tribes’ opposition to Huthi expansion to gain recruits to fight against the Huthis.

Chronic and severe economic and humanitarian problems, exacerbated by repeated pipeline attacks and the Huthis’ push to reinstate costly fuel subsidies, will continue to undercut government control and legitimacy. Yemen will probably continue pressuring donor nations to make good on aid pledges while negotiating with tribes outside of Sanaa’s control to keep oil exports flowing.

Huthi ascendancy in Yemen has increased Iran’s influence as well.

Lebanon

Lebanon continues to struggle with spillover from the Syrian conflict, including periodic sectarian violence; terrorist attacks; and the economic, political, and sectarian strain associated with refugees.
• Lebanon faces growing threats from terrorist groups, including the al-Nusrah Front and ISIL. Sunni extremists are trying to establish networks in Lebanon and have increased attacks against Lebanese army and Hizbullah positions along the Lebanese-Syrian border. Lebanon potentially faces a protracted conflict in northern and eastern parts of the country from extremist groups seeking to seize Lebanese territory, supplies, and hostages.

• The presence of over one million mostly Sunni Syrian refugees in Lebanon, which has a population of only 4.1 million, has significantly altered Lebanon’s sectarian demographics and is a continuing burden on the Lebanese economy. In October 2014, the cabinet further tightened entry restrictions to allow only “extreme humanitarian cases” into the country. Arrivals have declined 75 to 90 percent since August, most recently due in part to the new restrictions.

Egypt

Egyptian officials have announced that legislative elections will start in March 2015 and that voting will be staggered in phases over seven weeks. Egypt faces a persistent threat of terrorist and militant violence that is directed primarily at the state security forces both in the Sinai Peninsula and mainland Egypt. Since mid-2013, Sinai-based terrorist group Ansar Bayt al-Maqdis (ABM)—affiliated since November with ISIL—has claimed responsibility for some of the most sophisticated and deadly attacks against Egyptian security forces in decades.

Tunisia

Tunisia has transitioned to a permanent democratic government. Beji Caid Essebsi was elected President in the presidential runoff election in December 2014. In January 2015, Essebsi’s political party Nidaa Tounes selected former Interior Minister Essid to become Prime Minister.

• In early February, Prime Minister Habib Essid formed a broad-based coalition government, led by Nidaa Tounes, which included Islamist party al-Nahda and several smaller parties. The new government almost certainly recognizes Tunisia’s economic and security challenges.

The permanent government will inherit one of the highest youth unemployment rates in the world, a high budget deficit, and decreasing Foreign Direct Investment and balance of payments. It will struggle to meet public expectations for swift economic progress.

EUROPE

Turkey

Turkey will remain a critical partner in a wide range of US security policy priorities, including anti-ISIL and broader counterterrorism efforts. Joint US-Turkish efforts to stem instability in Iraq and Syria share the same goals but employ different approaches, increasing tension in the bilateral relationship. Turkish President Erdogan and leaders of the ruling Justice and Development Party (AKP) are focused on the general elections, which are scheduled to be held in June 2015.
• Ankara will be more inclined to support the anti-ISIL coalition if the coalition agrees to focus efforts against Asad, including setting up an internationally guaranteed buffer zone in Syria.

• Turkey is concerned that the Kurdish Democratic Union (PYD)—a group it believes is affiliated with the Kurdistan People’s Congress (KGK/former PKK)—will gain international legitimacy.

Key Partners

The Transatlantic partnership remains vital as the United States works with European leaders to maintain a concerted response to Russia’s action in Ukraine and to other security challenges on the European continent and beyond. Europeans are working to address fiscal challenges and encourage economic growth while maintaining and strengthening financial governance.

• The Transatlantic Trade and Investment Partnership has the potential to help generate economic growth for both the United States and Europe, reinforce the transatlantic link, and address public concerns about data privacy and food and health standards.

**RUSSIA AND EURASIA**

**Russia**

The Ukrainian crisis has profoundly affected Russia’s relations with the West and will have far-reaching effects on Russia’s domestic politics, economic development, and foreign policy.

President Vladimir Putin enjoys some of his highest domestic approval ratings in all his years in office. An intense state media propaganda campaign has stoked Russians’ perception that Putin righted a historical wrong in orchestrating Russia’s seizure of Crimea and reasserted Russia’s great-power interests against a hostile West.

At the same time, the crisis in Ukraine has exacerbated preexisting domestic problems in Russia. The fall of former Ukrainian President Viktor Yanukovych’s government in February 2014 has almost certainly deepened the Kremlin’s concerns over the dangers of mass demonstrations and has intensified the Kremlin’s efforts to defuse what it sees as potential catalysts for protests in Russia.

Russia’s economy was in decline even before the crisis began. Growth stagnated in 2014 due to declining oil prices, large capital outflows, and a sharply declining ruble. In addition, economic sanctions cut off some Russian firms from Western financing. These factors have increased the real and perceived risks of doing business in Russia, raised the overall cost of international credit, and will probably drive Russia into recession in 2015.

Moscow is pushing for greater regional integration, pressing neighboring states to follow the example of Belarus and Kazakhstan and join the Moscow-led Eurasian Economic Union. The Kremlin is also cultivating its relationship with China, seeking to maintain some influence in Europe and emphasizing
multilateral forums to counter what Moscow views as US unilateralism. These trends were already present in Russian diplomacy, but the Ukrainian crisis has almost certainly lent emphasis to these policies.

Russia is taking information warfare to a new level, working to fan anti-US and anti-Western sentiment both within Russia and globally. Russian state-controlled media publish false and misleading information in an effort to discredit the West, undercut consensus on Russia, and build sympathy for Russian positions.

In Ukraine, Russia has demonstrated its willingness to covertly use military and paramilitary forces in a neighboring state—a development that raises anxieties in states along Russia’s periphery. Future Russian deployments and force posture changes will probably be designed to maximize their diplomatic and public impact in Europe. Russian military officials have announced plans to conduct more “out-of-area” air and naval deployments, to include greater activity in the Caribbean and Mediterranean Seas.

Moscow has made headway in modernizing its nuclear and conventional forces, improving its training and joint operational proficiency, modernizing its military doctrine to integrate new methods of warfare, and developing long-range, precision-strike capabilities. Despite its economic difficulties, Moscow is committed to modernizing its military.

**Ukraine, Moldova, and Belarus**

Ukraine faces a daunting array of problems after nearly a year of conflict with Russia and its proxies in eastern Ukraine. At the same time, the crisis has fostered a sense of national identity and unity. Public opinion has shifted heavily in favor of pursuing integration with the EU while views of Russia have become sharply negative. Moreover, for the first time, a narrow majority of the population supports NATO membership.

Negotiations over the status of the separatist-held territory in eastern Ukraine will almost certainly be difficult and protracted. Russia has supplied substantial quantities of heavy weapons to strengthen the separatists’ forces and covertly supports them with its own troops, both within Ukraine and from across the border. More importantly, Moscow has demonstrated that it is willing to intervene directly to prevent the separatists from being defeated on the battlefield. Further fighting is likely in 2015.

Ukraine’s dire economic situation presents no less a challenge to Kyiv than the conflict in the east. Ukraine will be highly dependent on substantial outside financial assistance for years to come.

In Moldova, the narrow victory of pro-EU parties in the latest parliamentary elections suggests that Moldova will push ahead with its European integration agenda. However, Chisinau still faces numerous challenges in seeking to overcome economic difficulties, entrenched corruption, and Moscow’s displeasure with Moldova’s rejection of closer integration with Russia. Any progress on resolving the political status of the ethnic-Russian separatist region of Transnistria is unlikely.

On 1 January 2015, Belarus became, along with Kazakhstan, a founding member of the Eurasian Economic Union (EEU), a regional integration project that Moscow eventually plans to transform into a Eurasian Union as a counterpart to the EU. President Lukashenko has tread carefully in regard to the
Ukrainian crisis, declining to recognize Russia's seizure of Crimea, but agreeing nevertheless to deepen military cooperation with Moscow.

**The Caucasus and Central Asia**

In **Georgia**, progress is unlikely on the core disputes between Tbilisi and Moscow, including Georgia's NATO aspirations and the status of the occupied territories of Abkhazia and South Ossetia. Tensions with Russia will remain high, and we assess that Moscow will press Tbilisi to abandon closer EU and NATO ties.

**Armenia** and **Azerbaijan** saw an increase in 2014 of ceasefire violations and a record number of casualties along the Line of Contact (LOC), which separates ethnic Armenian and Azerbaijani forces near the separatist region of Nagorno-Karabakh. The increased violence highlights how the close proximity of opposing military forces continues to pose a risk of miscalculation and unintended escalation. Prospects for a peaceful resolution in the foreseeable future are dim.

**Central Asian states** remain concerned about regional instability in light of a reduced Coalition presence in Afghanistan. Although they have long been alarmed about the activities of Central Asian militant groups operating in Afghanistan and Pakistan, they are increasingly worried about the threat posed by the return of the small but growing number of their nationals who have traveled to Syria to join violent Islamist extremist groups. On the whole, however, the Central Asian states will probably face more acute risks of instability in 2015 from internal issues such as unclear political succession plans, weak economies, ethnic tensions, and political repression—any of which could produce a crisis with little warning.

**EAST ASIA**

**China**

China will continue to pursue an active foreign policy—especially within the Asia Pacific—bolstered by increasing capabilities and its firm stance on East and South China Sea territorial disputes with rival claimants. The chances for sustained tensions will persist because competing claimants will probably pursue actions—including energy exploration—that others perceive as infringing on their sovereignty. China will probably seek to expand its economic role and outreach in the region, pursuing broader acceptance of its economic initiatives, including the Asia Infrastructure Investment Bank. Although China remains focused on regional issues, it will seek a greater voice on major international issues and in making new international rules.

Notwithstanding this external agenda, Chinese leaders will focus primarily on addressing domestic concerns. The Chinese Communist Party leadership under President Xi Jinping announced an ambitious agenda of legal reforms in late 2014 that built on its previous agenda of ambitious economic reforms—all aimed at improving government efficiency and accountability and strengthening the control of the Communist Party. The difficulty of implementing these reforms and bureaucratic resistance to them create the possibility of rising internal frictions as the agenda moves forward. Beijing will also remain concerned about the potential for domestic unrest or terrorist acts in Xinjiang and Tibet, which might lead
to renewed human rights abuses. Following months of pro-democracy protests in late 2014, Chinese leaders will monitor closely political developments in Hong Kong for signs of instability.

North Korea

Three years after taking the helm of North Korea, Kim Jong Un has further solidified his position as unitary leader and final decision authority through purges, executions, and leadership shuffles. Kim was absent from public view for 40 days in late 2014, leading to widespread foreign media speculation about his health and the regime’s stability. The focus on Kim’s health is a reminder that the regime’s stability might hinge on Kim’s personal status. Kim has no clearly identified successor and is inclined to prevent the emergence of a clear “number two” who could consolidate power in his absence. Kim and the regime have publicly emphasized his focus on improving the country’s troubled economy and the livelihood of the North Korean people while maintaining the tenets of a command economy. He has codified this approach via his dual-track policy of economic development and advancement of nuclear weapons. (Information on North Korea’s nuclear weapons program and intentions can be found above in the section on WMD and Proliferation.) Despite renewed efforts at diplomatic outreach, Kim continues to challenge the international community with provocative and threatening behavior in pursuit of his goals, as prominently demonstrated in the November 2014 cyber attack on Sony.

SOUTH ASIA

Afghanistan

President Ashraf Ghani and Chief Executive Officer Abdullah Abdullah secured Parliament’s approval of the Bilateral Security Agreement and NATO Status of Forces Agreement prior to the NATO Ministerial in December 2014. Despite the 12 January announcement of their cabinet nominees, Ghani and Abdullah have yet to win legislative approval for all of those nominated or resolve the final details of their shared political powers derived from their national unity government agreement. Resolving these issues will require continued international engagement and support.

International financial aid remains the most important external determinant of the Kabul government’s strength. However, the slow economic recovery from the global financial crisis has created fiscal challenges for many of Afghanistan’s primary donors, particularly in Europe and Japan. These economic hurdles at home have reduced donors’ enthusiasm and capacity to provide Afghanistan additional long-term financial aid above levels pledged through 2017 and reaffirmed in 2014 at the London Conference and NATO Wales Summit.

The Afghan National Security Forces (ANSF) prevented the Taliban from achieving a decisive military advantage in 2014. The ANSF, however, will require continued international security sector support and funding to stave off an increasingly aggressive Taliban insurgency through 2015. The ANSF, with the help of anti-Taliban powerbrokers and international funding, will probably maintain control of most major population centers. However, the forces will most likely cede control of some rural areas. Without international funding, the ANSF will probably not remain a cohesive or viable force.
The Taliban will probably remain largely cohesive under the leadership of Mullah Omar and sustain its
countrywide campaign to take territory in outlying areas and steadily reassert influence over significant
portions of the Pashtun countryside, positioning itself for greater territorial gains in 2015. Reliant on
Afghanistan’s opiate trade as a key domestic source of funding, the Taliban will be able to exploit
increasing opium poppy cultivation and potential heroin production for ready revenue. The Taliban has
publicly touted the end of the mission of the International Security and Assistance Force (ISAF) and
coalition drawdown as a sign of its inevitable victory, reinforcing its commitment to returning to power.

Pakistan

Pakistan will probably continue to implement some economic reforms and target anti-Pakistan militants
and their activities.

- Prime Minister Sharif’s promises to address economic, energy, and security issues almost certainly
fell short of high public expectations. Furthermore, his standing weakened when he reportedly asked
the Army to step in and handle opposition protests in late 2014.

- We assess that Islamabad will approve some additional economic reforms in 2015. Undertaking
future economic and energy reforms will be more challenging and will probably face greater political
and popular opposition.

- The Pakistan Government will probably focus in 2015 on diminishing the capabilities of the Tehrik-i-
Taliban (TTP), which claimed the attack on a school in December—leaving over 100 children dead.

We judge that Pakistan will aim to establish positive rapport with the new Afghan Government, but
longstanding distrust and unresolved disputes between the countries will prevent substantial progress.

- Pakistan’s provision of safe haven to Lashkar-e Tayyiba will probably continue to be a key irritant in
relations with India.

India

Prime Minister Narendra Modi’s decisive leadership style, combined with the 2014 election of an absolute
majority in the lower house of Parliament of his Bharatiya Janata Party (BJP), will enable more decisive
Indian decisionmaking on domestic and foreign policy. Although India has a long-standing position that it
maintain an independent policy, Modi will probably seek to work more closely with the United States on
security, terrorism, and economic issues.

India wants to maintain a stable peace with Pakistan but views Pakistan as a direct terrorism threat and a
regional source of instability.

India is concerned about the stability of Afghanistan and its own presence there following the drawdown
of international forces and is looking for options to blunt the influence of Pakistani-supported groups and
ensure that Afghanistan does not revert to a haven for anti-Indian militants.
Indian leaders will almost certainly pursue stronger economic ties with China that support the government’s economic agenda of closing the trade gap and attracting investment in infrastructure. New Delhi’s concern over perceived Chinese aggressiveness along the disputed border and in the Indian Ocean is probably growing in light of border incidents and the visit of a Chinese submarine to Sri Lanka in 2014.

SUB-SAHARAN AFRICA

Sub-Saharan Africa will face political and security challenges in 2015 including numerous presidential elections, ongoing insurgencies, and continuing intrastate conflict. The ongoing Ebola virus epidemic will undoubtedly challenge both Western African nations and the larger international community in trying to contain the virus’ spread and counter economic degradation in fragile West African nations. Stability in South Sudan, Nigeria, Somalia, and the Central African Republic (CAR) will almost certainly remain tenuous throughout 2015.

West Africa

The Ebola virus will persist throughout West Africa in 2015, posing a significant threat to the economic viability and consequently the stability of the region. The continued drain on resources and unprecedented need for medical personnel will strain governments and economies in Liberia, Sierra Leone, and Guinea—the three worst-affected countries. Sustained financial and material assistance from the international community, continued domestic support for the governments’ anti-Ebola efforts, and community engagement to change local misperceptions about the disease’s cause, treatment options, and burial practices will remain critical to slowing the epidemic. Economic growth in the outbreak zone has already slowed and will continue to slow during 2015, straining budgets and probably increasing dependence on international donor aid. A prolonged or severe outbreak that continues well into 2015 might prompt Guinea to delay Presidential elections, increasing the possibility of election-related violence. Military and security services in the key outbreak countries will probably successfully contain isolated unrest and local hostility toward Ebola-response personnel.

Sudan

Khartoum will almost certainly confront a range of challenges, including continued insurgencies in the periphery, public dissatisfaction over continued economic decline, and potential protests surrounding its April 2015 elections. Sudanese economic conditions since South Sudan’s independence in 2011 continue to deteriorate. Such conditions, including rising prices on staple goods, fuel opposition to the Sudanese Government.

South Sudan

Clashes between opposition forces and the Sudanese Liberation Army (SPLA) will almost certainly increase during the dry season—which lasts from November to April—undermining ongoing peace talks and putting tenuous humanitarian gains at risk. Peace talks between Juba and opposition elements will probably remain slow-going.
Nigeria

Instability in Nigeria will probably increase in 2015, given contentious elections delayed until March and April, plummeting oil revenue, and the military’s inability to check Boko Haram’s ascendancy in the northeast. The election will occasion violence, with prospects for protests in the months following the election. In addition, militants might remobilize in the Niger Delta and attack the oil industry. Boko Haram will probably continue to solidify control over its self-declared Islamic state in northeastern Nigeria and expand its terror campaign in neighboring Nigerian states, Cameroon, Niger, and Chad. Abuja’s reliance on oil exports for revenue will almost certainly ensure that Nigeria remains vulnerable to fluctuations in the global oil market in 2015. Declining oil prices will probably squeeze government revenues and drain currency reserves. Abuja’s overtaxed security forces will have a limited ability to anticipate and preempt threats.

Somalia

In Somalia, al-Shabaab is conducting asymmetric attacks against government facilities and Western targets in and around Mogadishu. The credibility and effectiveness of the young Somali Government will be further threatened by persistent political infighting; ill-equipped government institutions; and pervasive technical, political, and administrative shortfalls.

Lord’s Resistance Army

The Lord’s Resistance Army (LRA), even in its weakened state, probably has the ability to regenerate if counter-LRA operations are reduced. The LRA continues to display great agility in its geographic areas of operation and in the operational security of its activities.

Central African Republic

Despite the presence of international peacekeeping forces, the risk of continued ethno-religious clashes between Christians and Muslims throughout the country, including in the capital, remains high.

The Sahel

Governments in Africa’s Sahel region—particularly Chad, Niger, Mali, and Mauritania—will remain at risk of terrorist attacks and possible internal conflict. Al-Qa’ida in the Lands of the Islamic Maghreb (AQIM) and affiliated groups are committed to continuing their terrorist activity in the Sahel, including against Western interests. They will probably seek to increase the frequency and scale of attacks in northern Mali. Sahelien militaries will struggle to handle a wide array of security threats.
LATIN AMERICA AND THE CARIBBEAN

Cuba

Cuban President Raul Castro’s focus will almost certainly be preparing the country for the eventual end of the Castro era and maintaining tight political control. He is cautiously implementing economic and leadership reforms and released dozens of political prisoners in early January. Cuba’s principal interest in normalizing relations with the United States is probably linked to its recognition of the need to ease discontent over dismal living conditions and poor economic prospects. The slow rollout of economic reforms and a fall in nickel output cut GDP growth to 1.2 percent in 2014. Crucial components of the economic reform program—reducing the state role in the economy and opening up a few opportunities for self-employment—will probably produce numerous, short-term economic dislocations before gradually increasing productivity and jobs.

Cuba’s population of 11 million has been declining since about 2005 because of falling birthrates and emigration. Cuban migrant arrivals at the US southwest border rose from 10,400 in FY12 to 17,300 in FY14. Maritime arrivals and interdictions will probably increase in 2015 because of rumors that if the two countries normalize relations, the United States would change immigration policies that allow Cubans who reach the United States to obtain status.

Central America

Weak institutions, poor economic prospects, and the growing strength of criminal gangs will probably limit the ability of the governments of Central America’s northern tier—El Salvador, Guatemala, and Honduras—to improve rule of law, job opportunities, and citizen security, which will probably continue to fuel immigration to the United States in 2015. Fractured legislatures, political challenges, and entrenched business interests will probably slow agreement on raising some of the lowest tax collection rates in the world or adopting economic and social policies that would help reduce the high rates of poverty that spur migration to the United States. About 25 percent of El Salvador’s population has emigrated during the past two decades, mostly to the United States, because of lack of economic opportunities and widespread insecurity. El Salvador’s economy has experienced the lowest economic growth rates in the region for eight consecutive years. Guatemala’s weak fiscal position will undermine efforts to ameliorate extreme poverty, particularly in rural areas. About 1.6 million Guatemalans reside in the United States and send about $5.5 billion in remittances back home each year. Honduras, one of the hemisphere’s poorest countries, is struggling to make headway against ineffective, corrupt institutions. Honduras has the world’s highest rate of homicides per capita, despite a reported modest decline in 2014, and criminal gangs are forcibly recruiting youth and extorting businesses and individuals.

Venezuela

Like most oil-exporting nations, Venezuela is experiencing the economic consequences of policy choices and the decline in global oil prices. Oil accounts for about 95 percent of Venezuelan export earnings and 45 percent of government revenue. Caracas will face a strained fiscal environment in 2015 along with rising inflation and shortages of essential goods.
Legislative elections are slated to occur by the end of 2015; voters will be concerned about public security, the economy, and political rights. President Nicolas Maduro appointed a presidential commission to review the country’s police system and recommend reforms after the high-profile murder of a national assembly deputy and a violent law enforcement confrontation in October 2014 with a radical, armed group known as a colectivo.

Haiti

Political tensions between Haitian President Martelly and his opponents will probably flare during 2015 and might undermine preparations for overdue local and parliamentary elections as well as for the vote for a new president in November 2015. Haiti will need substantial technical and financial support from the international community to organize and hold elections. Some violent protests are probable and might become more intense or widespread if political opponents believe that electoral preparations favor Martelly’s party or allies.
Ambiguity Defines the NPT: What Does “Manufacture” Mean?

David S. Jonas

Georgetown University Law Center, George Washington University Law School

Recommended Citation


This Article is brought to you for free and open access by the Law Reviews at Digital Commons @ Loyola Marymount University and Loyola Law School. It has been accepted for inclusion in Loyola of Los Angeles International and Comparative Law Review by an authorized administrator of Digital Commons @ Loyola Marymount University and Loyola Law School. For more information, please contact digitalcommons.lmu.edu.
Ambiguity Defines the NPT: What Does "Manufacture" Mean?

DAVID S. JONAS*

I'm looking for a complication. Looking 'cause I'm tired of trying. Make my way back home when I learn to fly.¹

I. INTRODUCTION

No question about it—the Nuclear Nonproliferation Treaty (NPT)² is complicated, with a healthy dollop of vagueness added to the mix. As opposed to the Foo Fighters, who apparently yearn for complications (as if they are difficult to find), in the NPT, this band of merry men would find exceptional fulfillment, since complications abound. For what appears to be a relatively succinct treaty, the NPT becomes more complex as one studies it. Although the NPT functions as the

* Senior Executive Service, Former General Counsel, Defense Nuclear Facilities Safety Board; Former General Counsel, National Nuclear Security Administration; Adjunct Professor, Georgetown University Law Center, George Washington University Law School, and former Adjunct Professor at the U.S. Naval War College. B.A., Denison University; J.D., Wake Forest University School of Law; L.L.M., The Judge Advocate General's School, U.S. Army; L.L.M., Georgetown University Law Center; M.A., U.S. Naval War College. The author previously served in the U.S. Marine Corps, concluding his service with the Joint Chiefs of Staff as the nuclear nonproliferation planner. The views expressed herein are his own and do not necessarily reflect the official policy or position of the Defense Nuclear Facilities Safety Board, the National Nuclear Security Administration, the Department of the Navy, or the U.S. Government. The author wishes to thank Elizabeth Farnar and Lauren Chang for their superior research assistance in the preparation of this Article.

1. Foo Fighters, Learn to Fly, on There Is Nothing Left to Lose (Roswell/RCA 1999).


263
foundation of the current nuclear nonproliferation regime, it suffers from certain ambiguities that heightens its complexity and poses significant policy issues. A lack of clarity in such a vital multilateral treaty may allow states to adopt valid legal positions that bolsters and defend actions inconsistent with the spirit, if not terms, of the NPT. This article examines one of the many important terms in the NPT that suffers from such opacity; specifically, the use of the term “manufacture” in Article II has generated debate regarding the precise activities that this word encompasses. In relevant part, Article II requires that the non-nuclear weapon states (NNWS) party to the treaty not “manufacture or otherwise acquire nuclear weapons” and not “seek or receive any assistance in the manufacture” of nuclear weapons. The key term “manufacture” is undefined in the treaty.

Interpreting the term “manufacture” yields a broad spectrum of activities that are potentially proscribed under the NPT. Existing literature on the subject evinces no real consensus, but the majority view is that the term “manufacture” should be interpreted narrowly. However, competing views have also arisen as to the exact scope of this narrowing interpretation, specifically, whether the prohibition on “manufacture” should bar only the manufacture of a completed nuclear weapon or include the construction of component parts of a nuclear weapon as well. There is surely a vast gulf between those two ends of the continuum.


4. Jonas, supra note 3, at 38 (“The NPT is fundamentally sound but suffers from an unfortunate lack of clarity in certain areas.”).

5. Daniel Joyner, Iran’s Nuclear Program and the Legal Mandate of the IAEA, JURIST (Nov. 9, 2011), http://jurist.org/forum/2011/11/dan-joyner-iaea-report.php (“The term ‘manufacture’ as used in Article II has been the subject of some controversy regarding its interpretation.”).

6. Id.

7. Id.; Jonas, supra note 3, at 46.

8. NPT, supra note 2.

9. See Joyner, supra note 5; Spies, supra note 3, at 407.

10. Spies, supra note 3, at 407.

Arguments that interpret the term “manufacture” broadly, encompassing activity in the early stages of nuclear weapons design, are premised on the belief that it is best to “err on the side of caution or restraint and apply . . . restrictions to facilities and materials which pose unacceptable proliferation risks . . . .” Whether the term “manufacture” is interpreted narrowly or broadly produces significant policy consequences. For example, the interpretation determines the nuclear activities in which NNWS may lawfully engage in, including energy development as well as the extent to which the United States and its allies may rely on the NPT to discourage illegal nuclear weapons development by NNWS. The interpretation of the term would also implicate the extent to which the United States and other states may lawfully assist NNWS in nuclear related activities.

Professor Joyner, a noted scholar in this area, argues that the term “manufacture” in Article II of the NPT should be interpreted narrowly in an effort to flesh out the nature of the issue. Few existing articles address the ambiguity resulting from the use of the term “manufacture” at length; among those articles are the works of Professors Spies, Stransky, and Xinjun, discussed in section B, infra. Numerous Lexis and Westlaw searches of relevant terms such as “NPT,” “manufacture,” and “prepare” yielded only a few articles that acknowledge the absence of an explicit definition of the term “manufacture,” but fail to delve into more detailed analysis.


13. Greenberg, supra note 11, at 121.
14. Id. at 120.
15. Id.
16. Joyner, supra note 5.
17. Spies, supra note 3, at 401.
Of the relatively few articles that do take a position on the ambiguity resulting from the use of the term "manufacture," most argue that the term should be interpreted narrowly.\textsuperscript{21} Under this purported reading, the term "manufacture" would apply only to the actual construction of a nuclear weapon and not the numerous preliminary activities that may indicate a nation's future plans to develop a nuclear weapon.\textsuperscript{22} Accordingly, this article attempts to respond to the gap in the existing literature by outlining these arguments and their consequences. The article concludes with recommendations for addressing this problem in the future.

Current scholarship, minimal as it is, supports a narrow interpretation of the term "manufacture" in Article II of the NPT;\textsuperscript{23} a broad view, however, is equally supportable under the terms of the treaty itself. This narrow interpretation understands the term "manufacture" to refer to the actual construction of a nuclear weapon from its component parts,\textsuperscript{24} in contrast, a broader reading would include the preliminary stages of the nuclear weapons construction process.\textsuperscript{25} The problem with the broader view is having to decide which of the many preliminary activities may be covered. Under a broader interpretation of the term "manufacture," one could infer a nation's future intent to construct a nuclear weapon from the nation's early

\textsuperscript{21} Joyner, supra note 5.

\textsuperscript{22} Id.

\textsuperscript{23} Id. ("Thus, my interpretation above of the Article II term 'manufacture,' which focuses on \textit{actus reus} and does not focus on intent, is more persuasive from both an evidentiary and substantive perspective.") (emphasis added).

\textsuperscript{24} Id.

\textsuperscript{25} Id.
“concept, capacity building, design, research and experimentation stages.” In analyzing the proper meaning of the term “manufacture,” the following section argues that the term “manufacture” should be interpreted narrowly according to: (a) the plain meaning of the NPT; (b) the negotiating history of the NPT; (c) the U.S. ratification history of the NPT; (d) the subsequent action by states party to the NPT; and (e) the problematic counterarguments that have been advanced in support of a broader reading of the term “manufacture.”

A. Plain Meaning

To determine the meaning of the term “manufacture,” one begins by looking to the plain meaning of the term pursuant to Articles 31 and 32 of the Vienna Convention on the Law of Treaties (VCLT). In the VCLT, Article 31 requires that “[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.” We must, however, look further because the plain meaning here could be, as discussed above, a broad or narrow interpretation of the term. Article 32 of the VCLT provides for a supplementary means of interpretation, which includes the “preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of Article 31.”

In interpreting Article II, the plain meaning of the term “manufacture” certainly refers to physical construction. Joyner has argued that the term “manufacturer” in the NPT “refers to the physical construction of a nuclear explosive device, or perhaps at its broadest reading, to the physical construction of the component parts of a nuclear explosive device.” Stransky also offers a plain meaning of “manufacture” based on physical construction, stating that: “[a]
common understanding of ‘manufacture’ was a ‘process of making products by hand or machinery.’”

Thus, the plain meaning of “manufacture” in Article II suggests that the term should be read narrowly. Consequently, a narrow reading of “manufacture” fails to encompass preliminary activities related to the research and development of a nuclear weapon, even if such activities might later be used in the construction of a nuclear weapon. If the drafters of the NPT intended to reach farther back into the earlier stages of weapon development, they could have used other terminology, such as “preparing for assembly.” Stated otherwise, the term “manufacture” does not “reach far back along the knowledge acquisition and development line of a nuclear weapons program to the concept, capacity building, design, research and experimentation stages.” As discussed below, the narrowed plain meaning of the term “manufacture” significantly impacts which activities of NNWS would fall within the scope of the NPT.

B. Negotiating History

The negotiating history of the NPT supports a narrow view of the definition of manufacture. The VCLT considers the travaux préparatoire an important means of deciphering ambiguous treaty terminology. Not only do all drafts of the NPT include a prohibition on the manufacture of nuclear weapons as noted in Mohamed Shaker’s treatise, but the negotiating history of the NPT also reveals a deliberate effort to incorporate terminology reflecting the narrower view of the

34. Id. at 21 (citing BLACK’S LAW DICTIONARY, 1117 (4th ed. 1951).).
35. Joyner, supra note 5.
36. Id.
37. Id.
38. VCLT, supra note 28, art. 32 (the term “travaux préparatoire” refers to the official record of the treaty negotiations).
39. MOHAMMED I. SHAKER, THE NUCLEAR NON-PROLIFERATION TREATY: ORIGIN AND IMPLEMENTATION 1959-1979 249 (Oceana Publications Inc. 1980) (hereinafter SHAKER) (In his seminal treatise on the negotiating history of the NPT, Mohamed Shaker offers this interesting vignette about the drafting of Article II, and in particular, the term “manufacture”: “the prohibition on manufacture was envisaged in all the previous treaty drafts. The Soviet draft of 24 September 1965 also envisaged the undertaking by the States ‘not possessing nuclear weapons’ not to ‘prepare for the manufacture’ of nuclear weapons. The American draft as amended on 21 March 1966 included the preparations for the manufacture but only with respect to the prohibition on assistance. This means that non-nuclear-weapon States would have been allowed, under the American draft, to prepare for the manufacture of nuclear weapons as long as no assistance was provided from outside.”).
meaning of “manufacture.” In analyzing the negotiating history of the NPT, one can see that the drafters distinguished between the terms “manufacture” and “prepare for the manufacture” before ultimately deciding to use the narrower term “manufacture.”

“Manufacture” was the more limited term; it focused “more to the later steps of actual fabrication, construction, and assembly of the component parts of a nuclear weapon, and to the completion of the full device from those component parts.” Interestingly enough, even that sentence, with its intention to clarify the matter, is itself ambiguous. That is, it establishes several elements of manufacture: fabrication, construction, assembly, and completion. Does it mean that one has “manufactured” a weapon only after completion of all four steps, or is each separate step considered “manufacture?” “Prepare for the manufacture,” in contrast, was the more expansive term. This phrase “clearly sought to include earlier steps on the ladder of development of a nuclear weapon, including the concept, capacity building, design, research and experimentation steps.” Again, there are many intermediate steps between “capacity building” and “completion of the assembly.” Even if the NPT drafters did not intend to regulate “capacity building,” perhaps they intended to prohibit other intermediate stages.

Various drafts of the NPT included alternating uses of the terms “manufacture” and “prepare for the manufacture.” Interestingly, the Chemical Weapons Convention, a related treaty, does not regulate “military preparations” for the use of chemical weapons. A 1965 Soviet draft of the NPT included a provision mandating that NNWS could not “prepare for the manufacture” of nuclear weapons. Furthermore, a 1966 American draft suggested allowing NNWS “to prepare for the manufacture of nuclear weapons as long as no assistance

40. Joyn, supra note 5. (“[I]n the early U.S. and Soviet drafts, there was a distinction clearly drawn between the terms ‘manufacture’ and ‘prepare for the manufacture.’ . . . the fact that both terms had been considered by the drafters, and that the term ‘manufacture’ was eventually agreed upon by all NPT treaty parties, confirms the limited meaning of the term.”).

41. Joyn, supra note 5.

42. Id.

43. Id.


45. Id.; see also Stransky, supra note 12, at 30 (“The Soviets’ September 24, 1965 draft . . . prohibited NWS from providing assistance to NNWS ‘in preparations for the manufacture’ of nuclear weapons . . . ”).
was provided from outside [nations].”46 “The fact that both terms were considered by the drafters, and that the term ‘manufacture’ was the term ultimately agreed upon by all NPT treaty parties confirm the limited meaning of the term.”47 Therefore, the drafters’ eventual decision to reject the broader term, “prepare for the manufacture,” in favor of the narrower term demonstrates a definitive intent to limit the activities proscribed by Article II of the NPT.

By evaluating the negotiating history, it is apparent that the 1966 American draft “apparently initiated the use of ‘manufacture,’ as opposed to ‘prepare to manufacture . . . .’48 “This fact is rather ironic in light of the current efforts led by the United States to expand the meaning of ‘manufacture’ to include steps that would have much more persuasively been included in the term ‘prepare to manufacture,’ which was previously proposed by the Soviet Union for inclusion in the NPT and rejected by U.S. drafters.”49

Existing literature supports the view that the term “manufacture” should be interpreted narrowly, as confirmed by the negotiating history of the NPT.50 For example, Professor Spies contends that a narrow reading of the term “manufacture” should prevail.51 Specifically, Spies states that the term “suggest[s] a completed nuclear explosive device . . . as some negotiating parties had originally remarked.”52 Spies also notes of the terms “manufacture” and “prepare for the manufacture” being distinguished and compared before ultimately deciding to use the narrower term, “manufacture,” as evidenced by the drafters’ rejection of a Soviet proposal to ban the “preparation” for the manufacture of a nuclear weapon.”53 Here, however, Spies suggests that only a completed nuclear weapon, as opposed to the manufactured component parts of a nuclear weapon, satisfies the narrow interpretation of the term “manufacture.”54

46. Joyner, supra note 5 (internal quotations marks omitted).
47. Id.
48. Id.
49. Id.
50. See, e.g., Spies, supra note 3, at 407; Strasky, supra note 12, at 31; see also Statute of the International Court of Justice art. 38, para. 1(d) (referring to “the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law”).
51. Spies, supra note 3, at 407.
52. Id.
53. Id. at 409.
54. Id. at 407.
Like Professors Joyner and Spies, Professor Stransky notes that excluding the term “preparation to manufacture” followed by the rejection of the “preparation for the manufacture” language in the 1965 Soviet draft supports an argument that the NPT precludes only the actual construction of a nuclear weapon. Stransky thus states that this “ambiguity in distinguishing between ‘manufacturing’ and ‘pre-manufacturing’ activity . . . creates more flexibility in interpreting acceptable behavior” under the NPT. In further discussing the consequences of this ambiguity, Stransky also notes the arguments made by the Swedish delegation about the difficulty in distinguishing manufacturing from pre-manufacturing activity.

Although Professor Xinjun’s article on the NPT refrains from explicitly advocating for a narrow reading of the term “manufacture,” he nevertheless comments on the continued ambiguity surrounding the use of the term “manufacture” based on the NPT’s negotiating history. Xinjun acknowledges the competing interpretations of the term “manufacture’s” usage and discusses how the narrow view requires

55. Stransky, supra note 12, at 30-31 (“Despite these concerns, the final version of the NPT to which the United States and Soviet Union agreed upon omits any ‘reference at all to preparations for manufacture, either in relation to prohibited nuclear-weapon state assistance or to prohibited non-nuclear-weapon state activities.’ Based on the fact that the NPT specifically excludes the ‘preparation to manufacture’ restriction that was in two previous drafts, one can credibly argue that the NPT does not prohibit NWS from ‘assisting, encouraging, or inducing’ a NNWS in pre-manufacturing efforts.”).

56. Id.

57. Id. (“[T]he Swedish delegation focused on international assistance and the risks associated with pre-manufacturing nuclear developments. For example, Swiss Representative Myrdal stated that manufacturing nuclear weapons is comparable to a ‘long ladder with many rungs’ and that ‘the practical question is: on which of these is it reasonable and feasible to introduce international blocking?’ Representative Myrdal warned that to ‘prohibit just the final act of manufacture’ would seem to come late in these long chains of decisions.”) (citing SHAKER, supra note 39, at 250).

58. Xinjun, supra note 19, at 647 (“Yet, revisiting the Treaty on the Non-Proliferation of Nuclear Weapons travaux préparatoires of Article IV of the inalienable right reveals a strong intention of the dominant negotiating States to advocate ambiguity.”); see also Xinjun, supra note 19, at 649-51 (“The article will then investigate the NPT travaux préparatoires recorded in United Nations Documents and Official Records to see how ambiguity have been made on the wording of ‘inalienable right,’ ‘the right to participate,’ as well as the relevant wording of ‘manufacture’ in Articles I and II.” (emphasis added)). Specifically, Xinjun argues that the “inalienable right” provision of Article IV (which entitles parties to pursue the “peaceful application of nuclear energy”) reveals the drafters’ intention to leave ambiguous provisions within the NPT, although the article also references the use of the term “manufacture.”

59. Id. at 651.
“actual” manufacture of a nuclear weapon. Xinjun notes that the narrow interpretation was espoused by “some U.S. nonproliferation experts” despite their pro-nonproliferation stance, and goes on to acknowledge criticisms that such a narrow interpretation would render the treaty ineffectual. Xinjun further introduces some consequences of this ambiguity, stating that “[t]he fear from NNWS was that their ‘inalienable right’ to the peaceful uses of nuclear energy might be restricted by Article II: because Article II prohibited them from manufacturing nuclear weapons, some manufacturing activities could no longer be exercised.” In Xinjun’s assessment, although the drafters of the NPT “prima facie precluded the ban on manufacturing preparation” when they rejected the term “prepare for the manufacture” in the 1965 Soviet draft, the “final phase of ‘manufacture’ remains unclear” in the final version of the NPT. His observation is wise because, as noted earlier, the term “manufacture” could conceivably encompass activities such as uranium mining and milling.

Xinjun supplements his analysis with more support from the negotiating history of the NPT, specifically, the clarification of the term “manufacture.” Notably, the Swiss representative attempted to “clarify” the term “manufacture” “by enumerating certain ‘sensitive’ nuclear activities as not within the scope of the prohibited manufacturing.” Indeed, it appears logical to differentiate between

60. Id. at 652-53 (”F. Barnaby, the then director of the Stockholm International Peace Research Institute, pointed out that an act in preparation for manufacture, even in a case that came close to weaponry, did not necessarily mean the banned ‘manufacture’ in Article II. Sensitive nuclear activities would be safe from the treaty ban. Barnaby wrote, ‘A party to the NPT could legally manufacture the components of any number of nuclear weapons, and the non-nuclear parts of the weapons could be assembled. Only when the fissile material was placed into one of the devices would the Treaty be broken.’”).

61. Id. at 653 (“Ironically, some U.S. nonproliferation experts shared this view regardless of their pro-nonproliferation position. The early response of the U.S. towards European sensitive nuclear exports was marked as ‘spreading the bomb without quite breaking the rules,’ viewing sensitive nuclear exports as not falling in the scope of prohibition in Article I and Article II.”).

62. Id. (“Leonard S. Spector criticized that such interpretation ‘would make a mockery of their commitments to renounce nuclear weapons.’ He argued, ‘It must be made clear that the NPT commitment not to ‘manufacture’ nuclear weapons incorporates a prohibition on all related development, component fabrication, and testing.’”).

63. Id. at 658.

64. Id.

65. Id.

66. Id. (”The Swiss government worked on clarifying ‘manufacture’ by enumerating certain ‘sensitive’ nuclear activities as not in the scope of the prohibited manufacturing. In an aide-memoire to the 1967 identical draft, Switzerland requested such an interpretation to be confirmed formally: ‘the phrase ‘to manufacture or otherwise acquire nuclear weapons or other nuclear
managing dual use equipment and equipment that could only be
useful for nuclear weapons. In addition, Xinjun describes both Soviet
and U.S. efforts to ensure that NNWS could pursue activities for the
peaceful acquisition of nuclear energy without violating the NPT’s
restriction on the “manufacture” of nuclear weapons, implicitly
supporting an argument for the narrower reading of the term
“manufacture.” However, Xinjun notes that such statements “had a
strong propaganda smell” and “helped little in substantially clarifying
the issue.”

Nevertheless, an evaluation of the negotiating history of the NPT
and the existing literature describing the negotiations shows that the use
of the term “manufacture,” as opposed to the broader term “prepare for
the manufacture,” in the final draft of the NPT demonstrates the
drafters’ intention to refrain from banning pre-manufacturing activity.
It would seem that the intent of the NNWS activity is crucial. If the
intent is to build a nuclear weapon, then even mining and milling should
be prohibited under the definition of “manufacture.” Without an intent
element, such activities simply cannot be included.

C. Ratification History

The U.S. ratification history of the NPT further illuminates the
ambiguous nature of the term “manufacture” in Article II. During
the Senate hearings on the NPT, U.S. officials were “unable to actually
proffer a definition of ‘manufacture.’” However, the testimony offered
by William Foster, Director of the U.S. Arms Control and Disarmament

Id. at 659 (“Knowing well the concerns from NNWS, the two co-authoring NWS tried
on many occasions to ease such fears. The Soviet Union . . . announced, ‘we base ourselves
on the assumption that a treaty . . . should enable [NNWS] to develop their peaceful atomic
industries and all forms of the peaceful use of nuclear energy.’ The U.S. delegate to ENDC also
emphasized that the fear for an expanded interpretation was not well founded. Foster pointed out,
‘For example, the United States, as well as some other advanced civil nuclear Powers, have made
available materials and technology for the building of nuclear reactors, the fact that these reactors
produce plutonium that can be used in weapons has not prevented us from supplying these
materials and technology under adequate safeguards.’”) (emphasis added) (citations omitted).

67. Id.
68. Id. at 659.
70. Id. at 17, 34-35.
71. Id. at 34 (citing SHAKER, supra note 39).
Agency and chief U.S. negotiator of the NPT, ostensibly supports the arguments made for a broader reading of the term "manufacture." The testimony emphasized pre-manufacturing activity rather than the narrower definition supported by the NPT's plain meaning and negotiating history. Foster submitted additional testimony in response to Senator Clifford Case's request for clarification about what constitutes a prohibited nuclear explosive device as opposed to anything else that a NNWS could research and develop. The testimony hints at an intent element, based on the response of U.S. representatives made during treaty negotiations when asked similar questions:

For example, *facts indicating that the purpose of a particular activity was the acquisition of a nuclear explosive device would tend to show non-compliance.* (Thus, the construction of an experimental or prototype nuclear explosive device would be covered by the term "manufacture" as would be the production of components, which would only have relevance to a nuclear explosive device.) Again, while the *placing of a particular activity under safeguards* would not, in and of itself, settle the question of whether that activity was in compliance with the treaty, it would of course be helpful in allaying any suspicion of non-compliance.

It may be useful to point out, for illustrative purposes, several activities which the United States would not consider per se to be violations of the prohibition on Article II. Neither uranium enrichment nor the stockpiling of fissionable materials in connection with a peaceful program would violate [A]rticle II so long as these activities were safeguarded under Article III. Also clearly permitted would be the development, under safeguards, of plutonium fueled power reactors, including research on the properties of metallic plutonium, nor would Article II interfere with the development of the use of fast breeder reactors under safeguards.

The testimony of Dr. Glenn T. Seaborg, Chairman of the Atomic Energy Commission, arguably implies a narrow interpretation of

---

73. *Id.*
74. *Id.* at 35 ("Foster's definition is concerned primarily, and most obviously, with pre-manufacturing activity.").
75. *Id.* at 34-35.
76. *Id.* (emphasis added).
“manufacture.” In addressing the inherent tension between Article V of the NPT (committing all parties to take appropriate measures to make available the benefits which may be obtained from peaceful nuclear explosions) and Article II (precluding NNWS from manufacturing or acquiring nuclear explosive devices, even for peaceful purposes), Dr. Seaborg pledged to make “freely available the information and data obtained” from the development of nuclear explosive technology for peaceful purposes “except information relating to the design or manufacture of nuclear explosive devices.” He stated further: “we will be prepared to make . . . available technical advice and assistance . . . to those nonnuclear weapon parties to the treaty which seek assistance in studying specific peaceful applications of nuclear explosions.” This statement arguably implied that sharing of nuclear explosive technology for peaceful purposes would be permitted provided that the ultimate construction of the explosive nuclear device itself was not shared. He also reserved the possibility of conducting “cooperative experiments abroad.”

D. Subsequent History

VCLT Article 31(3)(a) and (b) deal with treaty interpretation and discuss subsequent agreement and subsequent practice as the critical tools for determining the consent of parties to evolving interpretations of treaty obligations. The twin concepts of subsequent agreement and subsequent practice are premised on the idea that over time, treaty parties may informally consent to “new and different interpretations of treaty obligations.”

Existing literature also references the parties’ conduct since the NPT’s ratification as further support for a more limited interpretation of

78. Id. at 522-23.
79. Id. at 523.
80. Id.
81. Id.
82. VCLT, supra note 28, art. 31(3)(a), (b); see also Alexander M. Feldman, Evolving Treaty Obligations: A Proposal for Analyzing Subsequent Practice Derived from WTO Dispute Settlement, 41 N.Y.U. J. INT’L L. & POL. 655, 657 (2005).
83. Feldman, supra note 82, at 662; see also ANTHONY AUST, MODERN TREATY LAW AND PRACTICE 191 (2000).
the term "manufacture." According to Stransky, "[e]xamining state practice as a method of treaty interpretation has become commonplace in both the domestic and international arena." To substantiate this point, Stransky quotes Justice Brennan in United States v. Stuart: "[t]he practice of treaty signatories counts as evidence of the treaty’s proper interpretation, since their conduct generally evinces their understanding of the agreement they signed." Further, Stransky notes that Article 31 of the VCLT states that "[t]here shall be taken into account, together with the context . . . any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation."

Subsequent actions of states party to the NPT also support the narrow interpretation of the term "manufacture." The fact that the International Atomic Energy Agency (IAEA) or the U.N. Security Council has not criticized Germany and Japan, industrialized states with mastery of the nuclear fuel cycle, for their nuclear capacity demonstrates that the term was intended to be applied narrowly. Of course, not being criticized for the steps they have currently taken also does not prove that they are insulated from such criticism or would not deserve criticism if they took further steps closer to a nuclear weapons capability, even if these steps are not considered the "final assembly" of a complete device.

**E. Problems with a Broader Reading of the Term "Manufacture"**

Support for a broader application of the term "manufacture" exists, so much so that the term might extend to activity indicative of a state’s intention to manufacture a nuclear weapon in the future. A broader interpretation, however, requires one to make inappropriate inferences

---

84. Joyner, supra note 5.
85. Stransky, supra note 12, at 36.
86. Id.
87. Id. (citing VCLT, supra note 28, art. 31(3)(b)).
88. Joyner, supra note 5 ("In the practice of states since the establishment of the NPT, the cases of Japan and Germany and other advanced industrialized countries who have the knowledge and capability to construct a nuclear weapon, but that have not on that account been criticized by the IAEA or by the UN Security Council, are yet further evidence of the correctness of this interpretation of the limited definition of the term ‘manufacture’ in the Article II prohibition.").
89. Vinovskis, supra note 20, at 279-80.
90. Joyner, supra note 5 ("Some would argue that this definition of ‘manufacture’ is too limited.").
of a nation’s intent to develop a nuclear weapon. 91 Unfortunately, it is not quite clear what the term “intent” really means as applied to a state or other artificial entity. It is difficult to translate human emotions to fictional persons. This highlights yet another aspect of definitional ambiguity. “[D]omestic legal systems . . . seldom if ever provide for a determination of intent prospectively . . . .” 92 Such a determination poses a serious evidentiary challenge, as “it would be nearly impossible to ever show from evidence . . . that an accused state nevertheless intends in the future to manufacture a nuclear explosive device.” 93 Rather, it will almost always “be just as reasonable, if not more so, to infer an intent simply to develop the knowledge and capacity necessary to manufacture a nuclear weapon, without actually constructing working components or a finished device.” 94 Thus, a narrow interpretation of the term “manufacture” focusing specifically on the actus reus of constructing a nuclear weapon as opposed to intent “is more persuasive from both an evidentiary and substantive perspective.” 95 It is unfortunate that this concept is not even mentioned in the NPT text.

Not all states, however, embrace such a narrow interpretation of the term “manufacture.” 96 A state might engage in activities that would fall under a broader interpretation of “manufacture” without actually intending to develop a nuclear weapon, thereby resulting in an overbroad application of the NPT. 97

There are important policy implications in interpreting the meaning of the term “manufacture.” 98 In analyzing the final version of the NPT, the one which the United States and Soviet Union both agreed

91. Id. ("The problem with such an interpretation is that it requires an inference of a specific intent or purpose associated with activities that could be related to a nuclear weapons program. That intent must be to manufacture or otherwise acquire a nuclear explosive device.").

92. Id.
93. Id.
94. Id.
95. Id.
96. Id.
97. Spies, supra note 3, at 407-08.
98. Id. at 408-09 (“It is conceivable for a state to engage in the activities listed above without necessarily attempting to acquire nuclear weapons. For instance, the same fuel cycle facilities used in a civilian program, which all states are entitled to pursue under the NPT, can be used in a weapons program. A state may have many reasons to pursue nuclear programs, including the prestige gained from mastering an advanced technology and legitimate non-weapons military use such as naval propulsion, among many other conceivable reasons. Many state activities, such as defense and general welfare spending, can lack a strict economic justification from a critical outsider point of view, but such programs remain legitimate due to widespread domestic support and other subjective considerations.”) (citations omitted).

upon, some ambiguity arises in distinguishing between “manufacturing” and “pre-manufacturing” activity, given that the NPT specifically excludes “preparations to manufacture” restrictions that was previously included in two past drafts.99 This issue has the potential to be highly relevant if the international community ever seriously tackles the issue of nuclear disarmament. In that context, negotiators would have to consider what activities would remain permissible for former Nuclear Weapon States (NWS), specifically, which types of manufacturing activities would be allowed under a “nuclear zero” regime. In some ways, this is the mirror image of the subject of this article and would again raise the question of whether the United States should favor a broad or narrow interpretation in such a future context.100

One could argue that the exclusion of the phrase “preparations to manufacture” left open the possibility that the NPT does not prohibit NWS from “assist[ing], encourag[ing], or induc[ing]” a NNWS in pre-manufacturing efforts. Stransky argues that the ambiguity in distinguishing between “manufacturing” and “pre-manufacturing” activity is significant given the flexibility that results in interpreting acceptable behavior.102 For example, during the NPT negotiations, the Swiss representative declared that the “exploitation of uranium deposits, enrichment of uranium, extraction of plutonium from nuclear fuels, or manufacture of fuel elements or heavy water when the processes are carried out for civil purposes,” does not constitute “manufacturing” of nuclear weapons.103

Some states could claim that while such activity may constitute “pre-manufacturing” of a nuclear weapon, it is permitted under the American-Soviet’s version of the NPT given that the prohibition is on the actual “manufacture” only. The ability to interpret a state’s actions within the narrower and relatively more flexible understanding of “manufacture” as opposed to “preparations to manufacture” provides important leeway for state officials in deciding what actions, if any, are appropriate to take in response to state transgressions. Ultimately, it is clear that intent remains the one unresolved element at work here.

99. Id. at 31; Spies, supra note 3, at 409.
100. Id.
101. Id.
102. Id.
103. SHAKER, supra note 39, at 250.
II. HOW STATES SHOULD ADDRESS THIS PROBLEM

NPT Review Conferences (RevCon) are held every five years.104 If successful, the RevCon will produce an agreed text.105 This text, not a part of the NPT, would represent the political commitments from the states party to the treaty. Such text could easily include a point regarding the parties’ collective understanding of the meaning of “manufacture” and perhaps even an acknowledgement of intent’s importance in regards to a state’s pursuance of either a peaceful nuclear program or a nuclear weapon.

III. CONCLUSION

Ultimately, this issue may have real world ramifications. For example, Joynor uses his argument for a narrow interpretation of the term “manufacture” to support the assertion that there is no evidence that Iran breached the NPT, as indicated by the recent IAEA report, because—based on current U.S. knowledge—Iran has not “physically constructed a nuclear explosive device or any of its components.”106 However, beyond the immediate repercussions of this debate, the continued ambiguity arising from the use of the term “manufacture” raises questions regarding the scope of permitted uses of nuclear development and the reach of the NPT. What if intent was an anticipated aspect of the “manufacture” determination? If so, Iran’s intent is fairly obvious; it does not need nuclear power, as it is sitting on a sea of oil.

In assessing the consequences of ongoing ambiguity about the proper interpretation of “manufacture,” Spies argues that any uncertainty arising from the term “manufacture” in Article II will not independently affect a nation’s compliance with the NPT, as actions that might be included under a broader reading of “manufacture” are specifically proscribed in Article III.107 In support of this argument, Spies notes that Article III requires fissile material, which is necessary for the production of nuclear weapons, to be placed under safeguards.108

Despite the lack of a definitive interpretation of the term “manufacture,” the prevailing interpretation of Article II is that the

104. NPT, supra note 2, at 4.
105. Id.
106. Joynor, supra note 5.
108. Id. at 409.
many activities a state must undertake to eventually construct a nuclear explosive, thereby indicating non-compliance with Article II, would necessarily involve violating specific provisions in Article III.\textsuperscript{109} Spies, however, maintains that the existing ambiguity of the proper interpretation of “manufacture” continues to create problems in monitoring compliance with the NPT.\textsuperscript{110} Consequently, this poses practical and policy challenges to the NPT’s ability to function as the foundation of an effective nuclear nonproliferation regime.\textsuperscript{111}

Based on the limited volume of literature addressing this important question, the plain language of the NPT, the negotiating history of the NPT, and the subsequent state action by states party to the NPT, one can deduce that the drafters of the NPT intended for the term “manufacture” to be applied narrowly. Such a narrow construction would prohibit only the physical construction of nuclear weapons. However, this may only have been because an intent element was too difficult to capture in treaty text.

Regardless of how the debate over the term “manufacture” is ultimately resolved, this is yet another example of a situation where the meaning of an ambiguous NPT term must be deciphered by lawyers and policy experts. The correct outcome would be for the NPT states to debate the issue at upcoming Preparatory Committee meetings and RevCons and to reach an agreement on the incorporation of the intent element into the application of the term “manufacture” to any particular NNWS.

\textsuperscript{109} Id. at 407-09.
\textsuperscript{110} Id. at 407-08.
\textsuperscript{111} Id. ("Although such a narrow interpretation of ‘manufacture’ is not accepted by the states parties, the lack of definitive criteria for what constitutes ‘manufacture’ continues to be an issue in the context of compliance assessment. During the 2005 NPT Review Conference a U.S. diplomat noted, ‘[i]n an extreme case, an NPT party might have manufactured an entire mockup of the non-nuclear shell of a nuclear explosive, while continuing to observe its safeguards obligations on all nuclear material.’ The U.S. diplomat suggested a list of activities of concern which would indicate an ‘intent’ to manufacture a nuclear weapon in violation of Article II. These activities include seeking certain fuel cycle facilities of direct relevance to nuclear weapons, such as enrichment or reprocessing, with no clear economic or peaceful justification; clandestine facilities and procurements; committing safeguards violations and failing to cooperate with the IAEA to remedy them; and using denial and deception tactics to conceal nuclear-related activities.")
The Nuclear Nonproliferation Treaty at 45

Remarks
Rose Gottemoeller
Under Secretary for Arms Control and International Security
New Zealand Institute for International Affairs, Victoria University
Wellington, New Zealand
March 9, 2015

As Prepared

Thank you, Sir Douglas Kidd, for the introduction. I am happy to be visiting New Zealand for the first time. The U.S. – New Zealand relationship has never been stronger.

On the occasion of Waitangi Day last month, President Obama sent a message to the people of New Zealand praising our common heritage and shared commitment to democratic values. These provide a solid foundation on which to further strengthen our already close relationship. This year is also the 100th anniversary of the Gallipoli Campaign. It serves as a reminder of our shared sacrifice in the global struggle of World War I.

I share the President’s sentiment that we look forward to our close collaboration and ever deepening common efforts, as we face the challenges of the 21st Century in the Asia-Pacific region and across the globe.

I am honored to be here today to deliver the Annual Foreign Policy Lecture of the New Zealand Institute for International Affairs. Thank you to the Institute and to Victoria University for hosting me.

New Zealand is a powerful voice for progress on arms control and nonproliferation issues.

The United States joins you in that call for progress and today, I would like to talk with you about the cornerstone of international arms control and nonproliferation efforts: the Treaty on the Nonproliferation of Nuclear Weapons (NPT). Last Thursday marked the 45th anniversary of the entry into force of the Nonproliferation Treaty.

The “grand bargain” of the NPT set an enduring standard that is as relevant today as it was at the Treaty’s inception. That bargain comprises three reinforcing aspects wherein nuclear weapon states pursue disarmament, non-nuclear weapon states abstain from the pursuit of nuclear weapons and all countries are able to access the benefits of peaceful nuclear energy. For 45 years, the regime has thrived. When it has faced with challenges, NPT Parties have worked together to make the entire nonproliferation regime stronger. Beginning with 62 signatories, the Treaty is now nearly universal — and universally remains our ultimate goal.

The Treaty has stemmed the tide of proliferation; it has facilitated cooperation among its States Party; and it has institutionalized the norms of nonproliferation and disarmament. The three pillars of the Treaty provide its stability, its endurance. Each pillar is as important as the others. Each pillar reinforces the others, and each States Party can and must help strengthen all three.

Looking at the success of the NPT, it is easy to forget that the world once faced the unpredictable and narrowing prospect of dozens of nuclear weapons states. It is easy to forget that nuclear war was once a daily fear for people around the world. While some people in this room — like me — might remember vividly, most people on this planet don’t remember how close we came to ultimate destruction. They don’t remember that for 13 long, tense days in October 1962, Soviet missile placements in Cuba brought us to the edge of the nuclear abyss.

In some ways, that shouldn’t be too surprising. It has now been over 50 years since the Cuban Missile Crisis. Faced with the prospect of nuclear war, leaders in Washington and Moscow stepped back from the brink all those years ago and set about the task of reducing both the tension in our relationship and the threats posed by our respective nuclear arsenals. Together, these leaders created the first “Hotline” between the Kremlin and the White House, allowing for direct, immediate communications between our leaders. Within a year, the United States and the Soviet Union negotiated, signed and ratified a Limited Nuclear Test Ban Treaty (LTBT), which went into force just four months later. The LTBT outlawed nuclear explosive tests on land, in the sea, in the atmosphere, and in space. This was a tremendous step in the right direction and one that helped create the political conditions to conclude the NPT.

At the U.S. signing of the NPT in 1968, President Lyndon Johnson proclaimed that “after nearly a quarter century of danger and fear — reason and sanity have prevailed.” The NPT, he said, was “evidence that amid the tensions, the strife, the struggle, and the sorrow [those] years, men of many nations [had] not lost the way — but the will — toward peace.”

Indeed, if the LTBT was the turning point away from the unthinkable, the NPT was proof that the world was committed to creating a safer, more secure world.

Now 45 years after the Treaty’s entry into force, we find ourselves in a completely different security paradigm. The threat of nuclear war has been eclipsed by threat of nuclear terrorism — an amorphous, ever-changing threat that has no home address. As the world works to further reduce and prevent the spread of stockpiles of nuclear weapons and to provide the best nuclear security, the NPT remains an essential tool.
In late April, the 190 Parties to the Treaty will meet in New York to discuss progress on advancing the commitments laid out in this essential agreement, as well as the challenges to its viability.

For its part, the United States is fulfilling its commitments in all three pillars of the NPT.

Nonproliferation

No nation has provided as much time and as many resources to preventing the spread of nuclear weapons as the United States. We are the single largest supporter of the IAEA and we put an extremely high priority on promoting and facilitating nuclear safety and security programs around the world. We have worked to strengthen the IAEA’s safeguards system for verifying peaceful nuclear programs, and championed the Additional Protocol as the accepted standard for verifying the absence of clandestine nuclear programs. Our support for the IAEA also includes leading a global effort to secure nuclear material in order to prevent nuclear terrorism. The United States knows that nuclear security and nonproliferation efforts are never “finished.” As long as nuclear and radioactive materials exist, they require our utmost commitment to their protection, control, accounting and disposition.

The United States also has been hard at work implementing a comprehensive system of export controls for material, equipment, and technology that could be used for nuclear explosive purposes and we will continue to expand on other cooperative threat reduction activities. At the same time, we are helping to strengthen multilateral nonproliferation efforts such as the Proliferation Security Initiative and the Global Initiative to Combat Nuclear Terrorism, and encouraging their growth. On the regional level, we are also working to provide security assurances for regional nuclear weapons free zones across the world; importantly for this region, the Southeast Asia Nuclear Weapons Free Zones. And we support the proposed conference to discuss a WMD-free zone in the Middle East.

Finally, the United States is working with our P5+1 partners to seek concrete, verifiable steps to ensure that Iran’s nuclear program is exclusively peaceful. We are also working with partners in the Six-Party Talks to seek the denuclearization of North Korea and its return to the NPT and IAEA safeguards.

Disarmament

In Prague in 2009, President Obama made clear the U.S. commitment to seek the peace and security of a world without nuclear weapons. The U.S. commitment to disarmament is clear: It is unassailable. Since the entry into force of the NPT, the United States has reduced its nuclear stockpile by more than 80%. The New START Treaty just celebrated its fourth birthday, and it is being well-implemented by both the United States and Russia. Current tensions with the Russian Federation highlight the importance of the security, stability, and predictability provided by verifiable mutual limits on strategic weapons.

President Obama stated U.S. willingness to negotiate reductions in both non-strategic and strategic nuclear weapons with Russia. In June 2013, in Berlin, the President proposed a reduction of up to one-third of our deployed strategic warheads from the level established in the New START Treaty. That offer, which was a good one, is still on the table. Progress requires a willing partner and a conducive strategic environment.

To pave the way to lower numbers in the future, the United States is putting its best and brightest to work on creating new verifications and monitoring techniques. As part of this effort, the United States has created, in partnership with the Nuclear Threat Initiative, the International Partnership for Nuclear Disarmament Verification. Starting at our first meeting in a few weeks, we will work with both nuclear and non-nuclear weapons states, as well as non-governmental organizations, to discuss technical issues associated with verifying nuclear disarmament and to consider possible solutions to those problems.

Peaceful Uses

The third pillar of the treaty – the peaceful uses of nuclear energy – is perhaps less heralded, but it is no less important. This pillar aids in addressing modern challenges such as climate change, food, water and energy security, and sustainable development.

The United States is a stalwart supporter of the astonishingly varied peaceful uses of nuclear energy and technology, and we are heeding to advance projects that are making a real difference in countries throughout the world. These include projects to advance human health, combat cancer and infectious diseases such as Ebola, support water resource management, ensure food security, protect the environment, promote nuclear safety and security, develop nuclear power infrastructure, and develop uranium resources.

P5 Process

International cooperation is vital to the success of these efforts. We will continue to work with the other four nuclear-weapon states as defined by the NPT – China, France, Russia, and the United Kingdom – to advance our common goals of nuclear disarmament and nonproliferation. The P5 Process, as it has come to be known, is a multilateral discussion forum among the P5 covering a broad range of international security and stability topics, including our progress in implementing the Action Plan from the 2010 NPT Review Conference. It has been heartening to see countries like China adding to the discussion in a constructive and creative manner. The regular interaction, cooperation and trust-building activities are providing the foundation on which future P5 multilateral negotiations on nuclear disarmament will stand.

New Zealand’s Contributions to the NPT

As a strong and determined advocate for both disarmament and nonproliferation, New Zealand is a key player in the NPT review process.

On nonproliferation, New Zealand leads by example, serving as a vice-chair of the 1540 Committee, a UN effort to stem the spread of weapons of mass destruction and facilitating cooperation and collaboration at the International Atomic Energy Committee in Vienna. New Zealand has also provided over $150,000 in monetary contributions to the PUI, as well as in-kind contributions to the Ocean Acidification International Coordination Center in Monaco by coordinating such research in the Australasian region.

With its membership in the Global Initiative to Combat Nuclear Terrorism (GICNT), along with other nuclear security efforts, New Zealand is helping to curb the threat of one of the most unpredictable dangers of our time. It is a danger that should serve to move all nations to work harder and faster to reduce the likelihood of nuclear terrorism ever becoming a reality.
At last year’s Preparatory Meeting for the NPT RevCon, New Zealand called for an increased focus on the nuclear disarmament pillar of the NPT. Such focus can take many shapes. As I mentioned, the United States is particularly interested in expanding our collective work on developing the technologies that will help us verify further nuclear reductions.

Further, there are initiatives and agreements that are essential to progress in this pillar. The United States and New Zealand have both provided strong support for the Comprehensive Test Ban Treaty (CTBT) and the negotiation of a Fissile Material Cut-off Treaty (FMCT). As the United States works to complete its ratification process for the CTBT, we look to partner with Wellington on further development of the Treaty’s International Monitoring System and efforts to move towards the Treaty’s entry into force. We and the New Zealanders are equally committed to finally spurring the negotiations of an FMCT in the Conference on Disarmament.

CTBT and FMCT share a long pedigree. Both are needed to support more ambitious disarmament steps and more immediately, to end the nuclear arms build-up in Asia. These treaties remain an important part of our dialogue within the P5 and discussions with India and Pakistan.

There is no doubt that New Zealand is fulfilling its NPT commitments in both word and deed, and the United States looks forward to constructive cooperation at the RevCon in April.

Challenges Ahead

As I said, the NPT is facing challenges and the United States is aware of criticisms it will face in April. There are those that think the United States is not moving fast enough to fulfill our disarmament commitments. The record, as evidenced by a more than 80% reduction in stockpile numbers since the entry into force of the NPT, refutes that notion. In hard numbers, the United States had 20,008 nuclear weapons in our active stockpile in 1970. In 2013, the active stockpile consisted of 4,804 warheads. That is still too many and we know it. We continue to drive downwards, but occasionally we will find ourselves on a plateau. That is not a failure; that is the reality of how any process works.

The United States and the Russian Federation continue to possess over 90% of the world’s nuclear weapons, so further bilateral reductions between our nations is the next logical move. That is why, as I said, President Obama proposed a next round of strategic reduction talks between the United States and the Russian Federation.

Unfortunately, Russia’s actions in Ukraine have made it difficult to engage with Russia on the full range of issues affecting strategic stability. This is unfortunate, as there are real and meaningful steps we should be taking that can contribute to a more predictable, safer security environment.

Addressing current Russian actions is an ongoing process. For example, we will keep pushing the Russian government to return to verifiable compliance with its Intermediate-Range Nuclear Forces Treaty (INF) obligations, as the Treaty is in our mutual security interest and that of the globe. We have been clear with Russia that our preference is to resolve this issue diplomatically and not risk a return to the action/reaction dangers of the past. The United States appreciates the support of Australia as we deal with these issues.

The United States is also aware of whispers to scrap the NPT or the 2010 Action Plan in the hopes that an outright ban on nuclear weapons can be negotiated and brought into force at this time. That desire is short-sighted at best and reckless at worst, as the NPT has served to protect and promote stability for over four decades.

For the advocates of moving ahead to a ban at this moment, it is important to remember that the United States shares the goal of the peace and security of a world without nuclear weapons. We are aware that the “nuclear sword of Damocles,” as so eloquently described by President John F. Kennedy, still hangs above the head of every man, woman and child on this planet. That concept has weighed heavy on the hearts and minds of U.S. leaders since the dawn of the nuclear age. Our deep understanding of the humanitarian consequences has become and will always be inseparable from our nuclear policy.

Moreover, as we weather new and enduring pressures to the nonproliferation regime, we must be doing the hard work to make the peace and security of a world without nuclear weapons possible. As I have said before, it is not enough to have the political will to pursue this agenda; we have to have a practical way to pursue it.

Further, pushing for a nuclear weapons convention or fixed timeline for the elimination of all nuclear weapons is not an efficient way to use the time at the NPT RevCon. The nonproliferation regime faces clear and present dangers that would make a world free of nuclear weapons more elusive. Non-compliance by some NPT Parties is a good example, as is the potential abuse of the Treaty’s withdrawal clause. Inaction on these issues would make the international security environment more chaotic and arms reductions less likely.

Those who support disarmament must acknowledge that not every nation is ready or willing to pursue serious arms control and nonproliferation efforts, least of all a total ban. Together, we must push those nations to accept their global and ethical responsibilities. Together, we must put aside disagreements over process and remember that we share the same end goal. Together we must strengthen and support all three pillars of the Treaty that has brought us so far.

The Road Ahead

We face challenges to progress in this arena, no doubt. President Johnson rightly said to expect challenges and setbacks when he signed the NPT in 1968, but he "solemnly pledge[d] the resources, the resolve, and the unrelenting efforts of the people of the United States and their Government in the pursuit of the Treaty's ultimate goal.

President Obama and the United States continue to honor this pledge today. We still face challenges, of course. When he chaired the United Nations Security Council in September of 2009, President Obama said that "we harbor no illusions about the difficulty of bringing about a world without nuclear weapons."

“We know,” he said, that “there are plenty of cynics, and that there will be setbacks to prove their point. But there will also be days… that push us forward.”

I have seen those days. I have seen Ukraine, Kazakhstan and Belarus take the wise, brave and bold step to send nuclear weapons out of their countries for dismantlement or disposition. I have seen the United States and Russia reduce their respective arsenals again and again. I have also seen the United States and Russia work together to turn the equivalent of 20,000 Soviet nuclear warheads into energy that is lighting up homes and offices across America. Most importantly, I
have seen more countries give up nuclear weapons or programs than have acquired them. The Nonproliferation Treaty is the foundation that allowed for all of these things to happen.

As we head into the RevCon and beyond, we will need to work together. With New Zealand as our partner, the United States is confident that we can move forward in advancing all three pillars of the NPT.

Thank you for your attention. I look forward to your questions.
The Threat of Nuclear Terrorism

Remarks
Rose Gottemoeller, Under Secretary for Arms Control and International Security
The Citadel's Intelligence and Security Conference "Achieving a Higher Degree of National Security" Charleston, South Carolina, September 18, 2015

(As Prepared)

Good Morning. Thank you, Dr. Book, for the introduction. It is a great honor to be at a conference sponsored by The Citadel and I am grateful to have the opportunity to speak to you about a difficult topic, the threat of nuclear terrorism.

I have two Citadel alumni staffers with me today, my Senior Military Advisor Marine Colonel Phil Boggs and Neil Couch, former Air Force Lieutenant Colonel and current Deputy Director of the Strategic Stability Office in the Department of State. I am also a Bulldog, but by way of Georgetown University, so we all have that in common. Neil just flagged the fact that The Citadel was named the Number 1 Public College in the South by US News & World Report for the fifth consecutive year. Congratulations!

I am honored to be speaking at this Conference on Intelligence and Security. As I mentioned, I would like to drill down on one topic in particular: the threat of nuclear terrorism. It's a topic that strikes fear into the hearts of people around the globe, but I find that people are not aware of all that we can do to combat this threat. In fact, while nuclear terrorism is the most immediate and extreme danger facing our nation, it is also a preventable threat.

I'll explain how, but first let me outline the threat.

During the Cold War, efforts to maintain strategic stability and deterrence helped to prevent the use of nuclear weapons. Today, the threats we face do not lend themselves to the classic understandings of nuclear deterrence. As President Reagan's former Secretary of State George Shultz has said, "If...the people who are [perpetrating] suicide attacks...get a nuclear weapon, they are almost by definition not deterable."

In a multipolar and asymmetric world, the constraints that held back nuclear proliferation for so long are straining at the seams.

There are two primary pathways by which terrorist groups could acquire a nuclear weapon: by directly acquiring a nuclear weapon itself from a nuclear weapons state's arsenal, or by acquiring enough nuclear materials to construct an improvised nuclear device.

The successful detonation by a terrorist group of even a crude and improvised nuclear device in a major city could result in the deaths of thousands and have significant, if not unflattering, economic and political global consequences.

Recognizing this threat, President Obama has made preventing nuclear terrorism one of the United States' top foreign policy priorities, labeling it in his 2009 Prague speech "the single most important threat" to U.S. national security. This President and this Administration have backed up that assessment with the most concerted diplomatic effort to address nuclear security threats worldwide ever undertaken within the international community.

The fundamental task at hand is to prevent terrorists from accessing nuclear weapons or the fissile material that goes into a nuclear weapon. Without the material, which a terrorist organization cannot produce on its own, the threat is eliminated.

A cornerstone of this effort has been the Nuclear Security Summit process. The Summits are head-of-state-level events, attended by over 50 countries and international organizations. World leaders convene to discuss the risks of nuclear terrorism and commit to addressing those risks. To date, there have been three Nuclear Security Summits, the first held in Washington in 2010, the second in Seoul in 2012, and the third in The Hague in 2014. The President will host the fourth Summit in Washington early in 2016.

As an expert who has worked on these issues for my whole career, I'll admit that fissile material control and risk reduction is a little "in the weeds" for heads of state. Fortunately, that has not been a problem at all. The leaders involved in the Nuclear Security Summits have really done their homework and are finding critical and creative solutions to this global problem. They have also committed their countries to pragmatic tasks to advance nuclear security.

The Summit process is advancing the twin goals of enhancing the international nuclear security architecture, and strengthening efforts to better secure vulnerable nuclear materials. Participants make nuclear security commitments at the Summits in the form of a Work Plan, Communiques, national statements, and joint statements. Participants also share the results of their efforts at the Summits in their national progress reports. If you are interested, you can find them all on the State Department website.

These efforts are bearing fruit. The number of countries and facilities with Highly-Enriched Uranium (HEU) and Plutonium – the key materials in nuclear weapons - is decreasing and the quantities of these materials have been substantially reduced. Security practices and procedures at nuclear sites and in transit are improving and countries across the globe are better prepared to counter nuclear smuggling. In short, nuclear security measures are stronger worldwide.

While the 2016 Summit is expected to be the last in its current format, we look forward to working with Summit participants and all states on continued nuclear security efforts. International organizations such as the International Atomic Energy Agency (IAEA), the UN, the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction, the Global Initiative to Combat Nuclear Terrorism, and INTERPOL will continue to facilitate this cooperation.

When it comes to nuclear terrorism, we are safer now than we were five years ago, but more remains to be done. The United States will continue to work with international partners to ensure that dangerous nuclear materials are accounted for and secured worldwide. Unending vigilance is required if we are to ensure that terrorist groups who may seek to acquire these materials are never able to do so.
Working toward this end, the United States puts its money where its mouth is. We are the largest national contributor to the IAEA’s Nuclear Security Fund, providing more than $70 million since 2010. These funds support cost-free experts, mission and technical visits to Member States, the development of nuclear security guidance and best practices, and the Incident and Trafficking Database.

The State Department’s Counter Nuclear Smuggling Program (CNSP) is also working with key international partners to strengthen capacity to investigate nuclear smuggling networks, secure materials in illegal circulation, and prosecute the criminals who are involved. Countries such as Georgia and Moldova are to be commended for their recent arrests of criminals attempting to traffic HEU; significant progress has been made in this area. Unfortunately, continued seizures of weapon-useable nuclear materials indicate that these materials are still available on the black market.

In fact, in many countries, it is not illegal to possess or traffic dangerous radioactive or nuclear materials. In some countries where it is illegal, their existing criminal code does not allow for the adequate prosecution or sentencing of the criminals convicted of doing so. To help fill these gaps, CNSP helps countries amend their criminal code to incorporate the necessary provisions and allow for sentences that serve as both punishment and deterrent to these crimes. CNSP also conducts workshops and exercises with the police, prosecutors, and judges who handle these unique cases in order to ensure they are able to hold these criminals accountable.

A key piece of any criminal prosecution is ensuring that evidence is properly handled, analyzed, and presented in court. It’s not different for nuclear and fissile materials, but this kind of evidence presents a unique challenge to law enforcement and technical experts – the challenge being that such material is radioactive. CNSP works with countries to build their analytical capabilities to meet courtroom requirements for the law and of course, for nuclear safety. This type of analysis belongs to a field known as nuclear forensics, and the United States is at the forefront of its study.

Similar to traditional forensic science, nuclear forensics aims to link materials, people, places, and events. Forensics can be aided when we are able to identify known characteristics and features of nuclear materials or devices. The United States has even developed nuclear forensic capabilities to identify where seized nuclear or other radioactive materials or a radiological dispersal device - also known as a dirty bomb – may have originated or who may be responsible. Such capabilities incentivize countries to make sure any material they have is locked down and secure. They would never want to be associated with a terrorist nuclear incident.

Multilaterally, the United States continues to Co-Chair with Russia the Global Initiative to Combat Nuclear Terrorism (GICNT), which is a voluntary partnership of 86 countries and five official observers committed to strengthening global capacity to prevent, detect, and respond to nuclear terrorism. Despite the terrible crisis that Russia created in Ukraine, our continued working relationship with Russia on the GICNT demonstrates our mutual concern over the threat of nuclear terrorism.

Over the past two years, the GICNT has held 15 multilateral activities, including workshops, tabletop exercises, and other practical activities that help partners address difficult and emerging nuclear security challenges.

GICNT has even held a mock trial focused on introducing nuclear forensic evidence in the courtroom to prosecute terrorist acts involving the use or unauthorized possession of nuclear or other radioactive materials. It underscored the need for countries to adopt strong legal provisions criminalizing these illicit acts before an incident occurs, reinforcing and complementing the work the United States has already been doing in this area. It also highlighted the challenges of communicating scientific conclusions in judicial proceedings.

By focusing on the “human element” of nuclear security, the State Department’s Global Threat Reduction (GTR) program seeks to reduce the risk that non-state actors or proliferant states could develop an improvised nuclear device. While “guns, gates and guards" are an important aspect of nuclear security, GTR focuses on making sure that the staff at a nuclear facility are trustworthy and report suspicious activity. It is this human reliability factor that makes all the difference in nuclear security.

Developing a nuclear security culture is especially important in countries around the world that are now developing the underlying technical and human infrastructure. GTR works with nuclear technical organizations around the world to support the vetting of staff working to diminish the risk that an employee sympathetic to – or coerced by – terrorist groups, could divert nuclear materials or expertise.

There are also global legal structures that help reduce the risk of nuclear terrorism.

Back in June, the U.S. Congress enacted long-sought implementation legislation for the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), an amendment to the Convention on the Physical Protection of Nuclear Material, and the Protocols to the Suppression of Unlawful Acts Against the Safety of Maritime Navigation. It is a mouthful, I know and the news of this Congressional action was certainly not a trending topic on Twitter.

Nevertheless, with enactment of this legislation, the United States was now in a position to move forward to ratify these important treaties. I will be depositing our instrument of ratification for the ICSANT at the United Nations next week. This legislation was also significant in its bipartisan support: it is important for our national security that nuclear security remain a high-priority, non-partisan issue on Capitol Hill.

The United States knows that nuclear security efforts are never "finished." As long as nuclear and radioactive materials exist, they require our utmost commitment to their protection, control, accounting and disposition.

With that, I will close, so we have time for questions, but I want to leave you with a final point. Nuclear terrorism is an absolutely terrifying phenomenon – an unthinkable danger looming over our cities, our families, our children. We have to be aware of this danger and we have to be aware of the fact that we can prevent it from ever happening.

The nonproliferation efforts I have mentioned today are all critical to our safety, as is our continued work on arms control and disarmament. The smaller the amount of weapons and materials, the smaller the risk. It’s just that simple and when it comes to international security, simple is rare. So nuclear disarmament is a goal that is manifestly in our national interest. It is the way, once and for all, to deal with nuclear terrorism. Thank you.
Towards Zero: Resolving the Contradictions

Remarks
Rose Gottemoeller
Under Secretary for Arms Control and International Security
2015 International Day Against Nuclear Tests High-Level Panel
UNGA at Permanent Mission of the Republic of Kazakhstan
New York City, NY
September 10, 2015

Thank you so much for the introduction, Ambassador Kawar. It is an honor to be on this podium with you, and thank you to your government for hosting the Integrated Field Exercise IFE14 in December 2014. I was able to attend as an observer, and Jordan’s work to host the event was impressive. Thanks also to Kazakhstan Government and to Ambassador Kairat Abdrakhmanov for arranging this event. I am honored to be a part of this panel observing the 2015 International Day Against Nuclear Tests. I am always grateful for the opportunity to talk about this important subject.

Over 2,000 nuclear explosive tests have taken place around the world over the last 70 years, about a quarter of which were tested in the atmosphere. Over time, radioactive and cancer-causing particles such as Strontium-90 found their way into milk and other food products, eventually ending up in the bones of children. Radioactive “hotspots” popped up across the United States and around the globe.

Growing public concern about the dangers of nuclear explosive testing collided with a turning point in history – the Cuban Missile Crisis. As an initial step leading us back from the brink of nuclear war, President John F. Kennedy called for a complete ban on nuclear explosive testing in 1963.

We were able to achieve part of this objective through the Limited Test Ban Treaty (LTBT) back in 1963 – banning tests in the water, in space and in the atmosphere. This tempered the problem of Strontium-90 in baby milk. But, at that time, we did not reach agreement on banning underground nuclear explosive testing, as we lacked the technology to accurately detect such tests. We didn’t give up in the face of this challenge. Through steady work and persistence, we developed the tools we would need to negotiate first a verifiable Threshold Test-Ban Treaty (TTBT), which entered into force in 1996, and then a Comprehensive Nuclear Test-Ban Treaty (CTBT).

Once it comes into force, the CTBT will allow us to complete the work we started 52 years ago: the world will have a legally binding global ban on nuclear explosions of any kind. In the meantime, it is important to remember that we have a superstructure already in place limiting testing: two legally binding treaties, the LTBT and the TTBT, remain in force, and since 1992, we have had an international moratorium on nuclear testing that with a few exceptions, has been remarkably effective.

Although the United States was the first to sign the CTBT in 1996, the Senate in 1999 failed to give its advice and consent to ratification. At that time, two main issues concerned the Senators: our ability to maintain the nuclear stockpile without explosive nuclear testing, and our ability to verify compliance with the Treaty.

Today the situation is entirely different.

Our science-based Stockpile Stewardship Program is ensuring that we do not need to conduct nuclear explosive tests in order to ensure the safety, security and effectiveness of our reduced nuclear arsenal, the nuclear weapons we still maintain. In fact, this month marks 23 years since the United States last conducted a nuclear explosive test. Today, the Department of Energy’s Stockpile Stewardship Program – a suite of experimental, diagnostic, and supercomputing capabilities – allows us to model and simulate nuclear devices without nuclear explosive testing. In fact, we actually understand more about how nuclear weapons work now than we did during the period of nuclear explosive testing. Let me be clear, this stockpile stewardship work is important to implementing President Obama’s commitment in Prague to reduce nuclear weapons with the goal of totally eliminating them. At the same time, the President said that as long as nuclear weapons exist, the United States must maintain a safe, secure and effective nuclear arsenal. The arsenal is shrinking, but it must remain safe, secure and effective in the meantime.

The ability to monitor and verify compliance with the CTBT is also stronger than it has ever been. The International Monitoring System (IMS), the heart of the verification regime, was just a concept two decades ago. Today, it is a nearly complete, technically advanced, global network of sensors, including 35 stations in the United States, that can detect even relatively low-yield nuclear explosions.

My boss, Secretary of State John Kerry, has called the IMS one of the great accomplishments of the modern world. In addition to its verification role, the IMS has also proven its ability to contribute critical scientific data on earthquakes, tsunamis and radioactivity from nuclear reactor accidents.

The on-site inspection element of the CTBT verification regime has advanced significantly as well. Last December, I was fortunate enough to be an observer at the Integrated Field Exercise sponsored by the CTBT Organization and hosted by Jordan. Seeing first-hand the formidable technology and expertise the international community can bring together to investigate the site of a suspected nuclear explosion was nothing short of amazing.

Plain and simple, the CTBT is good for U.S. security and it is good for international security. It is a key part of leading nuclear weapons states toward a world of diminished reliance on nuclear weapons and reduced likelihood of nuclear arms races. Most critically, an in-force CTBT would constrain a regional arms race in Asia, where states are building up and modernizing nuclear forces.

All told, it is in our interest to close the door on nuclear explosive testing forever.
Despite the clear merits of the Treaty, it remains, as President Kennedy said 52 years ago, "so near and yet so far." One of our biggest challenges is that it has been a long time since the CTBT was on the front pages of U.S. newspapers. Our first task is educating the public and Congress to build support for U.S. ratification.

As you all know, cutting through the day to day issues and getting people to focus on a treaty that many people already assume we have in place is no easy task. That’s why I am currently focusing on states most closely affected by explosive nuclear testing. They obviously include Nevada and New Mexico where testing took place, but also Utah, which is downwind from the former testing site in Nevada. There are also some lesser known testing locations such as Colorado, Alaska and Mississippi. I’ll travel to each of these states to redevelop the kind of grassroots interest that we saw in advance of the LTBT. I’ll appreciate the support of the non-governmental community as we do so.

People need to know what this Treaty is and why it is important. The most important thing that supporters of the CTBT can do is to educate their friends, their families and their communities on the reasons that the Treaty is good for America.

Back in Washington, we are focused on an open dialogue, rather than a timeline, to refamiliarize Senators with the Treaty. Ratification of the CTBT will require debate, discussion, questions, briefings, trips to the National Labs and other technical facilities, hearings and more, as was the case with the New START Treaty. The Senators should have every opportunity to ask questions — many, many questions — until they are satisfied. That is how good policy is made and that is how treaties get across the finish line.

We are confident that we have a good case to make. As former Reagan-era Secretary of State George Shultz said, “Senators might have been right voting against the CTBT some years ago, but they would be right voting for it now.”

I don’t think it will be easy, but that doesn’t matter. An in-force CTBT will benefit the United States and indeed, the whole world. We will keep pushing.

With that I want to briefly touch on the title of this event, “Towards Zero: Resolving the Contradictions.” Frankly, I have to take exception with it. I think that framing is too defeatist. What contradictions? We know what we have to do and we will do it. Yes, we have an enormous amount of work ahead of us, none of which lends itself to quick fixes. That does not mean we have failed or are bound to fail. To use a U.S. expression — it means we need to pull up our socks and try harder. That is the only way. If we give way to dispute over methods, we will get nowhere. Thank you, and I look forward to our discussion.
International Law vs the Iranian Nuclear Negotiations: Setting a Dangerous Precedent
David Jonas
May 18, 2015

If any institution is representative of the international community and international law, it is the United Nations (UN). One foundational value of the UN is its ability to hold member states accountable for their actions through establishing international norms, international agreements, and the mandates of the UN Security Council. Surprisingly, no one is discussing the serious legal and political issues that the Iranian nuclear negotiations present.

The five permanent members of the UN Security Council plus Germany (P5+1) recently negotiated the parameters for a Joint Comprehensive Plan of Action (JCPOA). How it is evaluated often depends on one’s political views, as well as regional, national, and international security concerns. Yet the impact that the agreement could have on the UN itself is ignored. Prior to this JCPOA, Iran was prohibited from enriching uranium by Security Council resolutions. Under the agreement, it is free to do so, within certain limitations. Therefore, a threshold question is whether this agreement is appropriate at all. And why is the Obama Administration — generally supportive of the UN — so anxious to legalize Iran’s flouting of Security Council resolutions, which undermines UN credibility?

International law illuminates such issues. The Permanent Court of International Justice decided the SS Lotus case in 1927, pronouncing that states may generally engage in any conduct not expressly prohibited and that states must consent to any restraints on their sovereignty.

Security Council resolutions taken under Chapter VII of the UN Charter are generally viewed as binding international law. Indeed, Article 25 of the Charter notes that all member states “agree to accept and carry out the decisions of the Security Council....” Iran signed the UN Charter and has therefore agreed to be bound by its resolutions.

Resolution 1929, for example, directs that Iran “suspend all enrichment related activities ... all reprocessing ... [and] shall not begin construction on any new uranium-enrichment...facility.” Since Iran ignored this mandate, one must ask why the P5+1 are so eager to legitimize Iranian noncompliance. Indeed, the JCPOA constitutes an initial legal authorization for Iran to abrogate all existing Security Council resolutions prohibiting it from enriching uranium. Assuming that a deal is finalized, the UN Security Council would then have to follow up with a resolution blessing whatever activity is permitted by the final agreement that is inconsistent with existing resolutions.

The P5 has the greatest stake in ensuring the observance of Security Council resolutions, so why is this happening? What does it portend for the future? At a minimum, it sets a precedent most notable for its glaring disregard of existing Security Council resolutions. Why should any state now follow them? Why not just wait until the time is right and renegotiate?

Coincidentally, the P5 are also the Nuclear Weapon States party to the Non-Proliferation Treaty (NPT). The NPT does not create rights under international law, but only limits them. Iran is a Non-Nuclear Weapon State under the treaty and specifically promises not to “manufacture” nuclear weapons, yet it may lawfully come very close to assembling a nuclear weapon yet remain technically compliant with the NPT. Article IV promises Iran the peaceful uses of nuclear energy, but does not specifically allow enrichment and reprocessing, widely understood to lead to nuclear weapons acquisition. Therefore, the United States has vigorously pursued the “gold standard” in its nuclear negotiations, and has demanded
that such states, including many close allies, not engage in enrichment or reprocessing. And yet here is the United States, leading the charge, to provide Iran (of all states) a legally established right to enrichment. Something is amiss. In certain respects, this deal resembles a plea bargain in criminal law, where there is a clear violation of the law (UNSCRs), and the guilty party negotiates a reduced penalty (or in this case agrees to stop or slow down certain activities), and then returns to “normal” status (in the sense that sanctions will be lifted).

Assuming that the parties are able to negotiate a detailed agreement in the next three months (an unlikely scenario), a new Security Council resolution will be required to “bless” the new legal reality in Iran. The Security Council could always modify/rescind prior resolutions, changing the legal obligations of relevant states and eliminating any legal quandary created by the Iran negotiations. But is this any way to do business? Such conduct raises the political question of whether this particular plea bargain is a good idea, whether we can trust Iran, and whether the deal is so sweet that other states will be tempted to follow the Iranian precedent and also violate Security Council resolutions. It does not bode well for the future credibility of the UN.

David S. Jonas is a retired U.S. Marine Corps officer. He is a former General Counsel of the National Nuclear Security Administration and former nuclear nonproliferation planner for the Joint Chiefs of Staff. He teaches Nuclear Nonproliferation Law & Policy at Georgetown and George Washington University Law Schools and has also taught that subject at the U.S. Naval War College.
Five Reasons Why the Iran Nuclear Deal is Still a Really Bad Idea
David Jonas
October 14, 2015

Most Republicans in the House and Senate seem to have accepted that President Obama has won in his quest to enact the nuclear agreement between the P5+1 and Iran. Indeed, earlier efforts to block the deal on Capitol Hill have failed. Even Israeli Prime Minister Netanyahu seems resigned to the deal’s inevitability. But not everyone has given up. Several Republican presidential candidates have promised to nix the deal once they get to the White House. And indeed they should.

No other arms control or nuclear non-proliferation agreements have played out so publicly and divisively. The negotiations produced a tome — the Joint Comprehensive Plan of Action (JCPOA) — whose every word will be studied and parsed by governments, international organizations, military officers, academics, think tanks, non-governmental organizations, and others.

It is unusual for American negotiators to work so diligently, yet obtain an agreement that we would be better off without. Why, you ask? First, the deal provides international legal cover for Iran that will expedite its quest for nuclear weapons. Second, the United States will not know precisely when Iran possesses nuclear weapons unless it tests them. Third, the JCPOA should have been a treaty requiring Senate advice and consent rather than an executive agreement. Fourth, the most important commitment in the agreement is placed in such a manner that it would be irrelevant even if the agreement were legally binding. And finally, Iran freely violates treaty obligations, so will not likely observe a mere political commitment. Let’s go over each of these in more detail.

1. The agreement is legal cover for the bomb

The Obama administration asserts that the JCPOA will prevent Iran from building a nuclear weapon for 15 years. Instead, the agreement will facilitate Iran’s path to a nuclear weapon, while unwisely providing international legal cover for its entire nuclear program. The agreement breaks with decades of consistent, bipartisan nonproliferation policy. That understanding concerns an interpretation of the Nuclear Nonproliferation Treaty (NPT) in which states party to the treaty are entitled to the peaceful uses of nuclear energy, but not to enrichment and reprocessing technologies, which provide a clear route to nuclear weapons. This agreement announces to the world that it is fine to allow Iranian enrichment of uranium, even though we have not conceded that right to many allies (although we have done so indirectly with India). Iran will use this deal to keep the world focused in one direction, allowing inspections at declared facilities where nothing is happening, while pursuing its nuclear weapons goals at undeclared sites as it did, at a minimum, from 1985 to 2003. Iran knows how to play this sort of shell game.

Iran, of course, has no peaceful need for nuclear power, as it is sitting on a sea of oil — but let’s pretend that it does. Iran deems the offer of an international nuclear fuel bank — an alternative to its own nuclear program — as “nuclear apartheid” and refuses to support such a concept. But why would it refuse offers to have fuel rods shipped in and spent fuel removed from its reactors? This would not only save it the significant effort and expense of enrichment, but would also simultaneously remove all suspicion regarding intent to build nuclear weapons, because it is impossible to build them indigenously without enrichment of uranium or reprocessing of spent fuel to extract plutonium. That such a limitation is unacceptable to Iran only makes sense if Tehran is seeking a clear path to nuclear weapons acquisition. Further, only enrichment will permit Iran to build multiple nuclear weapons.
A state, as opposed to a terrorist group (although in the case of Iran, it is hard to tell the difference at times), requires more than one nuclear weapon, unless it is willing to use a very crude design. Otherwise, it requires a nuclear weapons program, allowing for several nuclear tests of a basic design, followed by manufacture of nuclear weapons based on a proven design. But we really don’t know what direction Iran will take to the bomb. By enriching uranium far in excess of the permissible 3.67 percent under the JCPOA, Iran could secretly expand its program to a point at which it has the requisite amount of highly enriched uranium to assemble a nuclear weapon in short order without nuclear testing. Estimates vary about how long this will take, but Iran already has the nuclear weapon designs. We don’t know if Iran has learned how to produce warheads able to withstand the rigors of ballistic missile flight and atmospheric re-entry, a technical achievement necessary to hold Israel or the United States at risk.

This uncertainty highlights the importance of the documents that the International Atomic Energy Agency (IAEA) seeks from Iran regarding the “possible military dimensions” of its program. Coming clean could well reveal a separate nuclear weapons bureaucracy in Iran, rather than mere development of a parallel nuclear fuel cycle. Iran has not yet produced those documents.

2. *We won’t know Iran has the bomb ‘til they do*

Thanks to the JCPOA, Iran may now go about its business in a manner that permits the maintenance of plausible deniability regarding its true intent. After all, why should anyone be concerned about Iran pursuing peaceful nuclear power? That right is guaranteed by the NPT, although Iran also insisted on enriching uranium, a right not specified in the NPT — at least according to the United States. The U.S. view on this matter is now a minority view in the international community, with most states, including Iran, believing that the NPT confers the right to enrichment.

The trouble with a surreptitious weapons program is that, like a thief in the night, it creeps up on you very slowly, not announcing itself, even once it has arrived. And Iran is studiously practiced at secrecy, evasion, and the art of denial on the international stage. We will surely fail to know if Iran elects to conduct a nuclear test, given the failure of the U.S. intelligence community to catch the nuclear tests conducted by India and Pakistan in 1998. Why are we so confident that effective monitoring of Iranian nuclear programs is possible now? Such certainly seems highly misplaced. American inspectors will not even be permitted inside Iran pursuant to the JCPOA, since citizens from states that do not have diplomatic relations with Iran are not allowed to join IAEA inspection teams in Iran.

3. *It should have been a treaty*

International agreements that enter into force for the United States after two-thirds of the Senate provides advice and consent are known as treaties. International agreements that enter into force for the United States without the advice and consent of the Senate are executive agreements. Typically, international agreements of major import are submitted to the Senate. No U.S. president has ever claimed the authority to negotiate such a highly controversial arms control or non-proliferation agreement unilaterally as an executive agreement. Usually, only minor agreements that attract little interest in the nonproliferation and arms control spheres have been concluded as executive agreements. Yet the JCPOA is of vital importance and produced major international attention and debate. It stands to re-shape the balance of power in the Middle East, and yet here we are with an executive agreement. Bruce Fein writes that the JCPOA is clearly a treaty pursuant to the U.S. Constitution and that the administration “miscalculated the JCPOA as an executive agreement to avoid the necessity of Senate approval ... (that is) beyond his political reach.” Because this is not a treaty, it is not legally binding and therefore stands as a mere political commitment.
4. The strongest language is in the least binding part of the agreement

The JCPOA's preamble reads, "Iran reaffirms that under no circumstances will Iran ever seek, develop, or acquire any nuclear weapons." After reading that, one might conclude that there is no need to delve any further into the cumbersome document, since the entire subtext of the agreement was to prevent Iranian acquisition of nuclear weapons. Given Iran's willingness to make that commitment, why not just stop there? Unfortunately, this declaration only appears in the preamble and is therefore nearly irrelevant, as any international agreements lawyer will tell you.

International agreements typically have two major components: the preamble and operative clauses. Operative text is legally binding. In non-legally binding agreements such as the JCPOA, the operative text still constitutes the content the parties are substantively agreeing to, and is therefore politically binding. By contrast, text in the preamble is not legally binding and often represents ideas or concepts that are merely aspirational or that the parties were unable to agree to. Such language commits no party to do or refrain from doing anything.

Similar language occurs in the "preface" — whatever that is. I have never heard of a preface in an international agreement. But since the preface is not an operative part of the agreement, Iran need not act on it. If a preamble has no legally or politically operative meaning, then surely a preface does not either. The bottom line here is that even non-legally binding agreements such as this are still politically binding. But in the JCPOA, the critical binding language is placed to ensure that Iran need not follow it.

5. Iran will probably not take political commitments seriously

The JCPOA is a political commitment that can be changed at any point in time. Indeed, that is why most states have a strong preference for legally binding commitments over politically binding ones. Legally binding agreements typically have withdrawal clauses and provisions for entry-into-force, duration, amendment, and the like. For example, NPT Article X permits a state party to withdraw from the treaty if "extraordinary events, related to the subject matter of this Treaty, have jeopardized the supreme interests of its country." Such clauses in arms control agreements usually require the withdrawing state to offer a rationale for its actions. Even though this is generally a subjective requirement, it nonetheless demands that a rationale be provided. Withdrawal clauses normally require 90-day notice to the other treaty parties (which, in important agreements, means notice to the world), prior to actual withdrawal.

So what the JCPOA boils down to is a statement by Iran that it won't do certain things, such as enrich uranium above 3.67 percent for 15 years, unless the ayatollahs change their minds. And then it may do so. Upon expiration of that term, Iran could have everything it needs to make a nuclear weapon if it successfully cheats using multiple undeclared facilities where the JCPOA's protections are the weakest. And what about Iran's international behavior makes anyone think they won't try to cheat and won't be able to do so at least with partial success?

And that's only if Iran purports to stick by its commitments.

Iran may very well manufacture some real or perceived grievance to withdraw from the JCPOA as well as from the NPT, claiming that the latter was signed during the Shah's regime and must therefore be abrogated. It could manufacture similar excuses to withdraw from its commitment not to violate the object and purpose of the Comprehensive Nuclear Test Ban Treaty (CTBT), which it only signed and has not ratified, thus limiting its obligations. There is abundant precedent in Iranian behavior for breaking its commitments as a state, such as secret nuclear sites, threats to the existence of a UN member state,
intercontinental ballistic missile programs, violation of its legally binding safeguards agreement, and a failure to provide information of the “possible military dimensions” of its nuclear programs.

A Really Bad Deal

Given the politically binding nature of this agreement, one might justifiably wonder why Iran presumably insisted that its promise not to seek nuclear weapons should be contained in what would normally be considered the non-binding portion of the JCPOA — the preamble. It is curious, is it not? Did Iran need this extra assurance that it could not in any way be held to observe this commitment? In fact, since Iran is a state party to the NPT, in which it made a legal commitment not to pursue nuclear weapons, one might ask what benefit the JCPOA confers at all, other than allowing IAEA inspectors back into Iran. But Iran is a big state and the IAEA has limited resources. Or are we hoping that the JCPOA will be taken more seriously than the legal commitment that Iran undertook with the NPT? Something is seriously out of kilter here.

Politically binding agreements are often still useful, and I don’t intend to demean such agreements unfairly. If politically binding agreements are reached with states that will observe them, they may be of great value. The United States typically treats its political commitments as it does its legally binding obligations — it scrupulously observes them, as most Western states do. In such cases, political commitments have clear value. But the JCPOA was not concluded with Belgium or Switzerland. Iran, which does not even follow certain legally binding commitments, such as its safeguards agreement with the IAEA, will not feel so constrained with a mere political commitment, an agreement of a lower order. A political commitment may be revoked by a simple statement from the president himself, or an executive branch official. Indeed, several GOP candidates for the White House have promised to nix the agreement and any president would have the clear authority to do so. Once a president states that America is no longer bound by the deal, the commitment is effectively terminated. An Iranian official may make a similar statement at any time and the JCPOA would become a dead letter.

How comfortable should we be with this commitment from Iran? It should give all of us pause.

David S. Jonas is a retired Marine Corps lieutenant colonel. He concluded his military service as nuclear nonproliferation planner for the Joint Chiefs of Staff. He was a member of the career Senior Executive Service and served as General Counsel of the National Nuclear Security Administration and the Defense Nuclear Facilities Safety Board. He teaches Nuclear Nonproliferation Law & Policy at Georgetown and George Washington University Law Schools and has also taught that subject at the U.S. Naval War College. He has negotiated dozens of international nuclear agreements, including the U.S.–India Civil Nuclear Agreement. He is widely published and is a frequent speaker on nuclear nonproliferation matters.
Why Iran Doesn't Trust America -- And What Can Be Done to Change That
Seyed Hossein Mousavian
Head of Foreign Relations Committee of Iran’s National Security Council (1997-2005)

During his speech before the United Nations General Assembly, U.S. President Barack Obama accused Iran of using "violent proxies to advance its interests," which he claimed served to "fuel sectarian conflict" in the region. Iranian President Hassan Rouhani shot back during his speech, decrying what he said were "baseless accusations" against Iran and calling for the United States to halt its "dangerous policies in defense of its regional allies who only cultivate the seeds of division and extremism."

Obama and Rouhani's comments highlight a broader issue underlying the troubled U.S.-Iran relationship. In the West, many commentators often portray Iran's leaders as being unreasonably suspicious about the intentions of outside powers, particularly the United States. Often dovetailing with this mentality is that Iran is irrationally and innately aggressive. While President Obama's remarks at the UNGA reflect this black-and-white thinking about Iran to a degree, other high-level U.S. officials have been far more brazen in their dishonest condemnations of Iran. For instance, the former head of the Defense Intelligence Agency, Lt. Gen. Michael Flynn, remarkably proclaimed in a March 2015 interview that "Iran and radical Islamist extremists" have opposed the United States simply because they "do not like our way of life."

This astonishingly simplistic worldview reflects not only total ignorance of the realities of Iran's political system, its foreign policy and Iranian society at large, but also eliminates room for any sort of compromise between Iran and the United States. After all, what dialogue can there be with a foe whose base belief is opposing your fundamental identity?

What dialogue can there be with a foe whose base belief is opposing your fundamental identity?

The reality of how Iran views U.S. regional policy is, of course, far more complex and is shaped by Iran's historical experience. For U.S. policymakers who seek to advance more sensible U.S. policies in the region, understanding Iran's positions is critical. Relying on delusions about Iranian policies and aims, as well as about American ones, is not only ineffective, but wholly counterproductive.

At the top of the list of the qualms Iranian leaders have with U.S. Middle East policy is America's one-sided support for Israel. While U.S. pundits frequently posit that actions by the Assad government in Syria or the Maliki government in Baghdad fueled the radicalism that led to groups like ISIS, they rarely apply this same mode of thinking to the Israeli-Palestinian conflict. Israel's treatment of Palestinians is arguably the root driver of much of the anti-U.S. extremism in the region and throughout the Muslim world, including in Iran. Iranian policymakers believe that the support the United States gives Israel is the key reason why injustices against the Palestinians have continued for so long.

U.S. interventions in the region in the past half-century have had a similar, radicalizing effect. The United States has propped up numerous authoritarian governments in the region, from the Shah of Iran and Egypt's Hosni Mubarak in the past, to numerous others today. These current allies of the United States have doubled down on repressing their own populations in the wake of the Arab Spring revolutions, effectively ensuring a new age of exclusion, extremism and terrorism.

Iranian leaders note this U.S. indifference to authoritarianism in the region and believe the overriding U.S. strategic goal in the region has primarily been about controlling natural resources, in particular oil and natural gas. Their experience with the 1953 U.S.-British instigated coup against the democratically-elected government of Prime Minister Mohammad Mossadegh -- who had nationalized the country's oil industry -- is of course instructive in this regard. The invasions and military interventions in Iraq and Libya respectively
bolstered this view, as has the ever increasing militarization of the Persian Gulf, both by the United States as well as its allies who it has buttressed with tens of billions of dollars in military aid.

Relying on delusions about Iranian policies and aims, as well as about American ones, is not only ineffective, but wholly counterproductive.

Iran's policymakers are also always quick to jump on and criticize clear signs of U.S. double standards and hypocrisy. The United States talks about supporting democracy but supports dictators; it talks about preventing nuclear proliferation but at the same time says nothing about Israel's nuclear weapons, actively prevents efforts to establish a nuclear weapons free zone in the Middle East, and has even embarked on a $1 trillion plan to modernize its own nuclear arsenal and facilities; it purports to be against the use of weapons of mass destruction but abetted Saddam Hussein in using chemical weapons against Iran during the Iran-Iraq War; and lastly, it fights terrorists but at the same time has supported them, whether directly or indirectly, in places like Syria. Iranian leaders point to all these and more when discussing why the United States cannot be trusted.

In short, like many scholars in the United States itself, Iran's decision makers believe that America's approach towards the Middle East has been gravely wrongheaded and has been for decades. Despite these Iranian grievances with many U.S. policies, however, a much enhanced U.S.-Iran relationship is imperative and only possible when both sides recognize the others' complaints and worldview and work to bridge their disputes.

U.S.-Iran cooperation is in fact the prerequisite for solving many of the crises in the Middle East. By abiding by seven principles, the United States and Iran can cooperate on the ongoing conflicts specifically in Syria, Yemen and Bahrain. These include:

1. Preserving the territorial integrity of all these countries
2. Respecting majority rule through a power-sharing system which guarantees minority rights
3. Free elections supervised by the United Nations
4. Inclusive negotiations between the P5 world powers and the R5 regional powers (Iran, Turkey, Egypt, Saudi Arabia and Iraq)
5. Fighting terrorism and its root causes collectively and with no discrimination
6. Establishing a regional cooperation system comprised of Iran, Iraq, and the Gulf Cooperation Council countries
7. Realizing a nuclear-weapons-free zone in the Middle East through implementation of the same measures agreed on between Iran, other regional states and world powers.
Six Achievable Steps for Implementing an Effective Verification Regime for a Nuclear Agreement with Iran

Nuclear Verification Capabilities Independent Task Force of the Federation of American Scientists

ABOUT THE TASK FORCE

This non-partisan Nuclear Verification Capabilities Independent Task Force was convened by the Federation of American Scientists to examine the technical and policy requirements to verify adequately a comprehensive or other sustained nuclear agreement with Iran. The Task Force published its first report in September 2014 outlining suggested requirements for monitoring and verifying a nuclear agreement with Iran. In this report, the Task Force has outlined six achievable steps for implementation of an effective verification regime for a nuclear agreement with Iran.

Christopher A. Bidwell served as chairman and rapporteur of this Task Force. Substantial contributions were made by Amb. Joseph DeThomas (Ret.), Dr. Charles D. Ferguson, John A. Leader, Harvey Rischkof, Dr. Amy Sands, and Dr. Richard Waltz. During the course of this project, the Task Force organized an all-day workshop discussion at the Washington Center for Nonproliferation Studies of the Middlebury Institute of International Studies at Monterey. We also held several roundtable discussions: one at the Middlebury Institute of International Studies at Monterey, two at Stanford University’s Hoover Institution on War, Revolution, and Peace, one at Harvard University’s Belfer Center for Science and International Affairs at the John F. Kennedy School of Government, and one at the National Defense University’s Center for the Study of Weapons of Mass Destruction. Task Force members also met individually with experts both in and out of government. All in all the Task Force members conferred with over 75 experts in the arms control, nonproliferation, verification, international law, and security fields and considered their inputs in making these recommendations. We thank each of them for their contributions. The members of the Task Force would also like to thank the John D. and Catherine T. MacArthur Foundation for its generous funding of this project.

Disclaimer: This report is a product of the Task Force as a whole and not of the Federation of American Scientists, which simply convened the Task Force. The report synthesizes the personal views of the participants and should not be seen as reflecting the views of the private and government organizations with whom the Task Force members are now or have been affiliated, or the views of the individuals and organizations with whom it consulted.
Acknowledgements

Reports such as this do not write themselves. They require a vigorous exchange of ideas and constructive debate. The synergy that flows from the melding pot of ideas is what gives such an endeavor its value. Accordingly, the Task Force solicited input from numerous sources - some of whom would prefer not to be publicly acknowledged - and would like to publicly thank the following individuals for their invaluable suggestions and contributions:


Introduction

Over the last 20 months, Iran has been in negotiations with the P5+1 regarding its nuclear program. These negotiations culminated in an agreement on July 14, 2015 that was memorialized in a 159 page text. The essence of the agreement is that Iran has offered the P5+1 constraints on its nuclear program in exchange for sanctions relief. As part of these negotiations, in paragraph iii of the Preamble and General Conditions: “Iran reaffirms that under no circumstances will Iran ever seek, develop or acquire any nuclear weapons.”

These negotiations, and the subsequent agreement, created a question for the U.S. policy community: What monitoring and verification measures and tools will the United States, its allies, and the International Atomic Energy Agency (IAEA) require in relation to a comprehensive nuclear agreement with Iran? To examine the issue, the Federation of American Scientists (FAS) formed the Verification Capabilities Independent Task Force that released a report in September 2014 titled, Verification Requirements for a Nuclear Agreement with Iran. The Task Force continues to examine these issues. Now that an agreement has been reached between the P5+1 and Iran, the Task Force has focused on the anticipation of implementation challenges and offers findings and recommendations for strengthening the implementation process both internationally and within the United States.

As is often the case with international agreements, there are ambiguities and uncertainties in whatever language is included in an agreement. The July 14, 2015 agreement is no exception. Such ambiguities have been historically clarified in the implementation process or have been ongoing sources of tension about compliance with agreements. Here, there will be both opportunities to strengthen the agreement with Iran and risks that aspects of the agreement will be ignored or walked back. Ineffective implementation would inhibit the further development of trust, erode confidence in the agreement within international and domestic communities, and put at risk the longevity of the agreement and the prospects for follow-on negotiations. Precedents will also be established that have the potential either to strengthen or to undermine the overall nonproliferation regime. Furthermore, the implementation of the agreement will likely be a source of discord between the Executive and Legislative branches within the United States Government (USG) and the subject of considerable debate on the part of nongovernmental groups attentive to nonproliferation and relations with Iran.

Hence, our Task Force has reached the judgment that effective implementation will be as important as the agreement language itself. This phase of our study focuses on the anticipation of implementation challenges and offers findings and recommendations for strengthening the implementation process both internationally and within the United States.

The particular emphasis of this study, as it was in the first phase of the Task Force’s work, is on monitoring measures and the process of reaching compliance and verification judgments within the USG and with its international partners. Knowledgeable observers disagree on the wisdom, scope, and content of a possible agreement with Iran on its nuclear program. But nearly all judge that an agreement with Iran without effective verification and monitoring measures would be counterproductive and dangerous.

We believe it is important now to consider the modalities and institutions for implementation. Such considerations are vital if the announced agreement with Iran is to be maintained over time. Even if the current agreement with Iran were to unwind, planning for implementation of monitoring measures would help inform future negotiations and be of great value in the continued monitoring of Iran’s nuclear program.
Near the beginning of major efforts to bring about significant arms control agreements between the United States and the Soviet Union in January 1961, Fred ikle posed a provocative question in what has become a classic article from Foreign Affairs. "After Detection — What?" He argued that detecting violations of an agreement is not enough and that "even if we can develop an inspection regime that makes the probability of detection very high, a nation contemplating a violation will not be deterred if it thinks it can discourage, circumvent, or absorb our reaction." The need for the United States and its allies to consider and prepare options in advance for responding to evidence of noncompliance is equally vital with Iran. Ignoring noncompliance risks the credibility of the agreements with Iran as well as the credibility of U.S. commitments in the region and the foundations of the nonproliferation regime.

Our current findings and recommendations build upon our earlier study and focus on six achievable steps for implementing a strong verification regime for a nuclear agreement with Iran:

1) Ensure that the Joint Commission Works Effectively Among the P5+1 and Iran to Facilitate Compliance and Communication

2) Organize Executive Branch Mechanisms to Create Synergy and Sustain Focus on Implementation Over the Long-Term

3) Support and Augment the IAEA in the Pursuit of its Key Monitoring Role

4) Create a Joint Executive-Congressional Working Group (JECWG) to Facilitate Coordination Across the Legislative and Executive Branches of the USG

5) Prepare a Strategy and Guidebook for Assessing and Addressing Ambiguities and Potential Noncompliance

6) Exploit New Technologies and Open Source Tools for Monitoring a Nuclear Agreement with Iran

The sixth recommendation of the Task Force deals with emerging new technologies and open source analysis tools that could be brought to bear to strengthen monitoring of a nuclear agreement with Iran. This report offers some preliminary thoughts about such technologies and tools, but our research and findings in these areas are still ongoing.

I. Ensure that the Joint Commission Works Effectively Among the P5+1 and Iran to Facilitate Compliance and Communication

Key Finding: An effective Joint Commission would be an enduring step toward facilitating effective implementation and creating channels of communication and transparency among the parties to a nuclear agreement.

Discussion: Information declarations, inspections, and the modalities of sanctions relief will produce many questions, which will require a forum for discussion of compliance, the resolution of anomalies, and the strengthening of the dialogue among the parties. Such implementation committees have been a mainstay of many prior international agreements.

Consultative bodies normally include technical experts from multiple organizations and agencies quietly working the nitty gritty details of agreements largely outside the political glare and bureaucracies of capitals. The first order of business has often been the discussion of gaps or inaccuracies in data declarations.

The Joint Comprehensive Plan of Action (JCPOA) establishes an eight-member Joint Commission, composed of the P5+1 countries, Iran, and the European Union. The High Representative of the Union for Foreign Affairs and Security Policy will serve as the Coordinator for the Joint Commission. The commission can establish working groups, and two such groups are specified in the JCPOA. The JCPOA also lists a series of tasks for the Joint Commission, which in essence gives the body the responsibility for overseeing the technical details of the agreement’s implementation and for resolving disputes concerning implementation. Commission decisions will generally be made by consensus among the eight members, with the notable exception of decisions on challenge inspections, which can be made by only a simple majority. The commission will meet at least quarterly in New York, Geneva, or Vienna, though the scope of its duties may require it to remain in near continuous session, at least during the first phases of the agreement.

Given the breadth of the Joint Commission’s mandate, its effective functioning will be vital to the success of the agreement. The nuclear agreement with Iran will be asymmetrical in key respects (the promise of sanctions relief in exchange for rollback and more transparency). Although there will be mutual interest in the successful operation of an agreement, the lack of symmetry will complicate the work of the commission. This agreement is different from most prior arms control and confidence-building measures where there is a symmetry of interests in monitoring. Prior agreements have operated under the premise that, “I am open to you because you are open to me: if you shut me out, I can respond with perfect reciprocity by shutting you out.” Neither party would wish to be shut out. With an Iranian agreement, there is no neat symmetry. The parties all want something, but they want different things. There is no simple way to establish tit for tat. For example, if Iran fails to provide requested access, what specific sanctions would get re-imposed? This need to calibrate actions and reactions in regards to monitoring and compliance is a strong argument for an empowered and active Joint Commission.

Recommendation: We recommend that the United States work tirelessly to ensure that the Joint Commission be energetic in its fulfillment of its responsibilities. An effective and active commission would:

• Signal that the Parties are serious about compliance and provide a non-public vehicle to encourage parties to comply. The Joint Commission could keep Iran close to the source of pressure that would result from noncompliance. The group that will initially examine the completeness and accuracy of data declarations also can summon the renewal of sanctions.
Conversely, Iran has in the same body a channel to register its concerns that sanctions are appropriately eased according to the agreement.

- **Resolve ambiguities and nip creeping noncompliance in the bud.** The Joint Commission could identify and resolve issues before they rise to major compliance concerns at a political level. The discussions within the consultative body, as well as the regular interactions of international inspectors with their Iranian counterparts, provide a channel to signal displeasure with any sign that the Iranians are being less than forthcoming and to warn bluntly, but quietly, of the consequences.

- **Provide a forum for broad institutional and interagency representation and advance communication among similar organizations of the parties to the agreement.** Although each state party will determine which individuals and organizations will be represented on its delegation to the Joint Commission, the prior history of such organizations has seen broad representation from various entities of a participating government. Thus, there may be opportunities for scientist to scientist, military to military, and intelligence to intelligence dialogue with Iran.

- **Establish long-term relationships and confidence-building.** The Joint Commission can continue to build expanded dialogue with Iran by demonstrating ways in which openness has its own rewards. Although it might seem that a consultative group would be largely adversarial in zero-sum, lawyerly advocacy, the experience of prior such bodies has shown that cooperation and tested trust can develop in a forum that is neither political theater nor minutely managed formal negotiations.

- **Create a venue for floating ideas for improving the agreement and advancing additional cooperative measures among the parties.** The consultative body for the Treaty on Conventional Forces in Europe, for example, demonstrated that such a body can not only discuss, discuss, and thoroughly vet improvements at a multi-lateral level, but would be capable of negotiating side agreements to facilitate implementation or even amendments to the main document (subject, of course, to approval in capitals).

### H. Organize Executive Branch Mechanisms to Create Synergy and Sustain Focus on Implementation Over the Long-Term

**Key Finding:** Implementation of an agreement with Iran will require continuity of focus, high-level of attention, and sustained engagement over decades. There are multiple potential paths for achieving these objectives organizationally within the USG. Existing lines of authority should be used, but with clear identification of lines of responsibility and the designation of two point persons – an Ambassador-level Special Coordinator at the State Department and an Iran Agreement Monitoring Manager within the Intelligence Community.

**Discussion:** In examining the many challenges facing the implementation of an Iranian nuclear agreement, the FAS Verification Task Force recognized that multiple USG organizations, and the interagency process as a whole, will be critical to the success of the agreement given the breadth of responsibilities for daily oversight of the agreement’s implementation, as well as the need to shape operational options and policy outcomes. In addition, how the interagency is organized (i.e., who is the policy “point person,” where is the leadership situated, and what staff and budget resources are allocated) will communicate the priority of this agreement within the USG bureaucracy and will be visible to other stakeholders inside and outside the United States. So, the issue now is: how to ensure effective implementation for an agreement that will span over decades, and involve multiple actors with diverse agendas and varying levels of resources, importance, and capabilities?

As has been shown in numerous other situations, effective implementation of this type of multiparty international agreement presents an enormous challenge that will require interagency planning, coordination, and synchronization of activities in a sustained way over several administrations. As in implementing any agreement, the interagency process will face several challenges in preventing operational drift, loss of high level attention, insufficient resource allocations, and bureaucratic game playing and positioning. It also has to address the reality of work overload, 24/7 media coverage, and strong personalities of key leaders.

In the case of the Iran Nuclear Agreement, there will be these additional challenges:

- Extended timeline of the agreement with parts ongoing forever and others lasting two to three decades
- The wide range of both technical and political tasks to be undertaken by the Joint Commission
- Likelihood of changes to political leadership in the United States and elsewhere
- Demand for a visible and meaningful congressional role
- Dynamic nature of the agreement given its critical junctures and compliance determinations
- Dealing with external country actors (Israel, Iran, P5+1)
- Dealing with external international organizations (IAEA, UN Security Council)

In addition to where the policy “point person” for the agreement might be located, equally important will be how the Intelligence Community organizes its support for this agreement given its primary role in providing monitoring data and assessments in support of the policy community’s verification judgments. The key to intelligence and negotiated monitoring measures working effectively is
the synergy created among them. Data declarations tell us where to look, routine inspections audit the declarations, national and international cooperative and unilateral monitoring and intelligence means detecting anomalies, and challenge inspections seek to gather more information relevant to the resolution of those anomalies. The inspections themselves serve as forcing events that may trigger activities on the part of the Iranians that might be indicative of the extent of their compliance with the agreement. The inspectors are also in a unique position to provide ground-truth situational awareness of Iranian nuclear capabilities and intent that remote access means cannot duplicate. The complex 24-day process for dealing with disputed challenge inspections under the agreement will make it incumbent on the USG to be able to synthesize intelligence and policy aspects of agreement implementation quickly.

The Task Force considered this issue with some caution. We heard during the course of our inquiry that the agreement monitoring function has atrophied from the height of arms control monitoring in the late 1970s and 1990s. This was also a finding of a 2014 Defense Science Board Task Force report. In 2001, the agreement monitoring function moved from an Intelligence Community organization—the former Arms Control Intelligence Staff—into a new organization—the Weapons Intelligence, Nonproliferation, and Arms Control Center—within the Directorate of Intelligence (DI) at CIA.

Some have noted that the operationally focused monitoring function is now within a predominantly analytical unit. Because the move of the monitoring mission into the DI has made the production of analytical products the primary function of members of the unit, there has been a perceived loss of attention to the arcane details of agreement compliance. We were told that some younger analysts, pushed to produce analytic reports for their career advancement, often do not have the time to absorb fully the best practices of prior monitoring efforts and the pertinent details of the agreements to be monitored.

We judge that the National Counterproliferation Center (NCPC) has the capacity to elevate the priority and focus of the monitoring of an Iranian nuclear agreement. Still, the NCPC role is primarily one of oversight and coordination. The necessary collection and analytical resources will reside elsewhere. It will perhaps take considerable bureaucratic acumen to ensure that the monitoring system functions synergistically and that those performing vital tasks are appropriately trained, equipped, and incentivized over the long haul.

In addition to support for monitoring and verification, the USG needs to consider quickly what it will need to contribute effectively to the new tasks that the Joint Commission has been given, notably the oversight of the clear procurement channel for Iran’s nuclear program and for approval requests by that program to undertake key nuclear activities. Past experience with other such international activities (e.g., Iraq under UNSCR 687 and interagency export control deliberations) show that: a) the USG infrastructure to deal with such issues will dwarf that available to other parties, and b) USG decision making will be far more divided and slower than that of other parties. How the USG a) harnesses its impressive capabilities to support activities of the Joint Commission, and b) ensures that an effective and efficient decision making process can support them will be key in determining whether the Joint Commission contributes to an effective agreement or simply generates additional frictions.

Recommendation: For the USG interagency process to be effective in overseeing this agreement, the following will have to occur:

- The structure of the interagency process must ensure sustained high level and high quality attention and engagement. Achieving this objective will require using existing structures as much as possible while also empowering one senior policy position as “point person.” Although it might be possible to use the legislatively created White House Coordinator for Weapons of Mass Destruction, Security and Arms Control (sometimes called the WMD Czar) position at the National Security Council for this purpose (perhaps renaming it to Iran Nuclear Agreement Coordinator for example). It would seem to make more sense to place this key leadership position in the State Department within an existing and already involved organization, such as the Undersecretary of State for Arms Control and International Security. A new position could be created within that organization—an Ambassador-level Special Coordinator—requiring Senate confirmation and to be filled with someone with gravitas and excellent relations with the President, Secretary of State, and the Congress. By placing the new position within an existing organization, it also allows the office to have the infrastructure and sufficient staff resources needed to sustain a rigorous operational and compliance oversight capability over the 20+ years of the agreement. It would also clearly designate one person who would lead any discussions with parties to the agreement as well as be a focal point for Congressional testimony and briefings.

- An Iranian Agreement Monitoring Manager should be established within the intelligence community. To achieve synergy, all of the disparate activities flowing out of the establishment of the agreement need to be orchestrated by experts familiar with the full range of monitoring resources. During the height of arms control monitoring in the late 1980s and 1990s, the Treaty Monitoring Manager within the U.S. Intelligence Community proved an effective vehicle for coordinating the work of organizations that were implementing both negotiated monitoring measures and intelligence collection activities. A similar position should be established for the monitoring of the Iranian agreement. Given the need to coordinate with many groups within the IC and given the importance of this agreement and its effective verification, the Office of the Director of National Intelligence (ODNI) would be the best home for such an Iran Agreement Monitoring Manager position, perhaps located within the NCPC, thereby linking it to an existing IC effort while also benefiting from the status and oversight power of being in the ODNI. Such a monitoring manager would need to work closely, and behind the scenes, with allies and international organizations.

- Use the existing interagency meeting system as much as possible to support the implementation of the Iran Nuclear Agreement. When considering how to operationalize the above positions on a daily, weekly basis over many years, the need to use the existing meeting structure as much as possible becomes evident. Adding another set of meetings will not encourage individuals, especially those already stressed by overloaded schedules, to engage in meaningful ongoing ways. The Special Coordinator at State and the Iranian Agreement Monitoring Manager will need to have regular meetings with their supporting staffs and interagency working groups. It will be very important to build into all of these meetings U.S. representatives from the UN and IAEA to ensure smooth collaboration and coordination of data and verification activities. It will also be critical that the Special Coordinator have an open door to the president.

- Retain the expertise developed from negotiations in policy and technical arenas. Those that were involved in the negotiations have the best sense of what was agreed to and are in the best position to shape implementation policy in the earliest stages. Furthermore those individuals should also be asked to develop a detailed guide of the agreement.

- The USG should anticipate and develop internal strategies, tactics, and a guidebook for discovering and dealing with possible noncompliance. See the discussion later in this paper of how such a guidebook could also be discussed among the P5+1 and Iran within the Joint Commissions to emphasize the importance of compliance and to encourage dialogue about compliance issues.
III. Support and Augment the IAEA in the Pursuit of its Key Monitoring Role

Key Finding: The IAEA will need additional authorities and resources to execute its projected responsibilities under an Iran/P5+1 agreement.

Discussion: Internal Burdens on the IAEA

The July 14, 2015 text memorializing the agreement asserts that the IAEA will have to be satisfied about a number of activities before the United States and other members of the P5+1 will lift nuclear and economic sanctions on Iran. Thus, the IAEA has at least a de facto role in determining if and when sanctions relief takes place. Pursuant to the statement, there are a number of specific areas that the IAEA must be satisfied with before the United States suspends nuclear and economic sanctions—some of which are new requirements for the IAEA. An additional source of concern is the fact that 12 percent of the IAEA's historic yearly Safeguards budget had already been dedicated to monitoring and verifying Iran's compliance with the NPT. On top of that, the IAEA has been spending approximately $1 million dollars per month to monitor Iran's compliance with the Joint Plan of Action. The added tasks outlined in the Iran Nuclear Agreement mean that the IAEA Safeguards personnel's ability to keep an eye on the other 163 IAEA members could be constrained, or it might face gaps in the quality or quantity of efforts in verifying the agreement. Furthermore, the additional activities that the IAEA will now be asked to perform under the agreement are not insubstantial in terms of financial and personnel resources, as well as lead time for their initiation. They include:

- Monitoring Iran's program under the increased access rights provided under the Additional Protocol to the NPT safeguards agreement.
- Performing monitoring tasks over and above the requirements of the Additional Protocol to ensure Iran cannot break out of the P5+1 agreement without early detection.
- Investigating and reaching conclusions about past Iranian activities directly related to the design and manufacture of nuclear weapons—known as activities with a “Possible Military Dimension” (PMD).
- Monitoring of centrifuge production and storage of advanced centrifuges.
- Monitoring of uranium mining and milling activities.

In addition to the above list, the IAEA will also be responsible for verifying that Iran is not engaged in reprocessing (which could be used to produce plutonium usable for weapons) and does not have any undeclared nuclear facilities. Both of these activities require the IAEA to conduct monitoring activities to prove a negative.

Discussion: External Burdens on the IAEA

Additional burdens on the IAEA will likely come from outside sources. This will place additional financial strains on the agency as well as time pressures on its decision making apparatus. These include:

- The interventions of many non-parties to the agreement (e.g., the Israelis, Iranian dissidents, NGOs, leakers in the USG, etc.) that believe they have information relevant to the sanctions decisions will be significant. Allegations of this nature have been an issue in the past with regard to Iran. Given the stakes involved, as well as Iran's past non-disclosures (Fardow and Natanz) it
is reasonable to assume that such allegations will be made post-agreement. Whether or not the allegations are valid is likely to be immaterial. The assertions will have to be investigated and that will consume IAEA resources. Additionally, there could be pressure on the IAEA to resolve these issues quickly, beyond the typical IAEA Board of Governors' quarterly reporting timelines.

• The interventions of parties to the agreement may also be significant. There may be instances where intelligence from one of the P5+1 members contradicts or challenges conclusions reached by the IAEA with regard to Iran's compliance. On the other hand, the Iranians could produce evidence that counters an IAEA or other state's claim of non-compliance. In either case, the IAEA would have to spend additional resources and leadership time on further investigation.

Recommendations: Given the new challenges the IAEA will potentially face as a result of the agreement reached between the P5+1 and Iran, the Task Force makes the following recommendations:

• The P5+1 should increase their contributions to the IAEA's budget. It is clear that the IAEA has the switch to turn sanctions on or off. Thus all P5+1 members have an interest in ensuring the IAEA can do its job. The United States in particular is the party to this agreement that is giving up the most significant leverage (i.e., indirect financial sanctions). It also has the most resources to contribute and has a strong interest in seeing allegations and counter allegations addressed. It is therefore reasonable to expect the United States and the other members of the P5+1 to contribute more in terms of money and support.

• The P5+1 should have a well-developed pre-planned protocol with timelines for addressing disputes and processing information from various governments. Failure to plan for these foreseeable events now means that a dispute resolution process could drag on for a significant period of time. This is likely to lead to dissatisfaction by the parties and could lead to a full collapse of the agreement. A rapid resolution process should be developed by the IAEA to address allegations of non-compliance. This should include direct reporting of investigations to the P5+1 and Iran.

• The USG should consider how to support the IAEA on inspector designations and visas. The Task Force noted Iran's statement in the agreement that visas would be granted to inspectors from countries with diplomatic relations with the Islamic Republic of Iran. On the one hand, this may be intended as a relaxation of its current restrictions on IAEA inspectors. On the other, it could be interpreted to exclude inspectors from the United States, UK, Egypt and Canada (the four countries without diplomatic relations with Iran). The United States should support IAEA efforts to continue to expand the number and nationality of IAEA inspectors for Iran and may wish to explore ways that Iran might be persuaded that including inspectors from the United States and other excluded countries could build confidence in the agreement and assuage concerns over Iran's intentions.

IV. Create a Joint Executive-Congressional Working Group (JECWG) to Facilitate Coordination Across the Legislative and Executive Branches of the USG

Key Finding: An effective JECWG is critical for creating sustained channels of communication and transparency between the Executive and Legislative branches of government on the issue of Iran-U.S. relations, with a particular focus on nuclear issues.

Discussion: One of the recommendations in this Task Force's initial report was the establishment of a Joint Executive-Congressional Commission (now referred to as the JECWG) to address the U.S.-Iran relationship, with a particular focus on Iran's nuclear program. Use of such a communication channel is based upon a conceptual framework that has been used in the past and was perhaps best exemplified by the establishment of the Arms Control Observer Group—created in the 1980s to build bipartisan arms control expertise in the Senate. The group was an instrumental tool for creating bipartisanship consensus, within the Executive and Legislative branches of the USG, on issues involving nuclear arms control treaties and agreements with the former Soviet Union. Similar issues are once again on the political agenda, albeit with a new country—Iran. The Task Force has reviewed several models of similarly situated commissions and groups (reviewing such things as their histories, charters, size, membership, and ultimate influence) and has concluded that the JECWG concept is a viable vehicle for addressing the following concerns:

• Providing Congress an avenue, appropriate to its constitutional role, to actively participate in verification and policy issues surrounding an agreement with Iran.

• Establishing an additional channel for Congress to ensure it has regular and sustained access to relevant information, monitoring activity, and intelligence gathered by the Executive Branch with regard to an agreement and its implementation.

• Sharpening the focus of both the Executive and Legislative branches on implementation, and verifying compliance with any agreement that is reached between Iran and the P5+1 for the full length of that agreement.

Recommendation: The structure and membership of the JECWG is an important factor in its ability to evaluate policy and create consensus. The JECWG should therefore have the following characteristics:

• The JECWG should be comprised of serving members of Congress (both houses) and senior officials from the Executive Branch. Regarding the legislative component, the benefit of having serving members, as opposed to non-congressional appointees, is that serving members can better relate to their fellow legislators and can become issue leaders among their peers on Iran and nonproliferation issues. Allowing these legislators to actively participate in appropriate aspects of the implementation of an agreement increases the prospect of shared priorities and understandings related to implementation of an agreement. The JECWG can be an effective trust builder for members of Congress as they would then have representatives close to the decision making process who understand their priorities and concerns. On the executive side, confirmed Presidential Appointees (sub-cabinet level, one each) from the Departments of State, Commerce, and Defense, as well as from the Intelligence Community (IC), should serve on the JECWG as permanent members in order to keep the JECWG's activities closely aligned with current policy and operations.

• Congressional members of the JECWG should be serving chairs of key committees (such as Foreign Affairs and Foreign Relations). Appointing serving chairs to the JECWG will seek to
temper any concerns senior legislators may have about losing jurisdiction and prerogatives. A few additional members can be appointed by Majority and Minority Leaders.

- The JECWG should be supported by a robust permanent staff of independent professionals (perhaps 10) with experience in regional affairs, nonproliferation, and economic sanctions policy. Permanent staff should have periods of service lasting no more than two years (subject to renewal) and appointments should be staggered. This approach should balance the need for institutional memory with the need to bring in fresh perspectives.

- The JECWG should have a broad charter that lasts at least 20 years. It should have an adaptive mechanism for widening its charter as new issues emerge concerning Iran and the United States. It should, at a minimum, focus on Iran’s nuclear program and the impact of sanctions. However, locking the JECWG into a fixed set of issues over a several year period could eventually lead to a diminishment of its significance and ultimately irrelevance as political winds shift over time and new issues emerge. A flexible charter allows members to address new situations that flow from an evolving dynamic relationship with Iran.

- The JECWG should conduct regular hearings, receive briefings, and issue a yearly report. A successful and active JECWG can be a tool for codifying USG attention on Iranian issues, and by extension, help contribute to problem solving on what is likely to be a continuing and dynamic national security concern. The hearing and report writing process should ensure that the USG remains seized of the issues and has a clearinghouse for information ready to address issues as they emerge. Members should be encouraged to have interactions with Iranian counterparts and participate in future negotiations.

V. Prepare a Strategy and Guidebook for Assessing and Addressing Ambiguities and Potential Noncompliance

Key Finding: To remove surprise and miscalculations, the parties should begin discussions to fashion a guidebook outlining what activities would constitute a clear material breach of the JCPOA agreement and the associated range of remedies that may be imposed for those violations.

Discussion: To remove miscalculations on all sides it would be helpful if the parties began discussions on what behavior or activity would constitute a material breach of the agreement. As we have noted, the proposed information declarations to the IAEA, the conduct of inspections, and the modalities of sanctions relief will produce many questions. Addressing these questions will require a forum for discussions regarding compliance, the resolution of anomalies, and the strengthening of the dialogue among the parties. However, beyond having discussions, there should be a mutual understanding of what would be considered a de minimis breach and what would be considered a material breach.

We acknowledge that there is a natural tension between technical experts who prefer clarity vs. policy makers who understand the advantages of ambiguity. We also recognize there is a risk that identifying the borderline between a material breach and a technical problem may give Iran a guideline for risk free cheating. However, in this case, given the stakes involved, a mutual understanding of where the hard redlines lie would be beneficial to ensuring that an agreement holds up over time. The key triggers for a material breach, which cannot be glossed or papered over, are likely to fit into four categories:

- **Nuclear Material Issues** (significant violations of the Agreement’s provisions for reducing enrichment levels; reducing uranium stockpiles; limiting heavy water production; monitoring of uranium mines and yellowcake production; monitoring for any separation of plutonium with reprocessing techniques from irradiated nuclear material)

- **Facility Issues** (significant violations of provisions for halting enrichment and reconfiguring of the Fordow facility; restructuring Natanz and removing centrifuges; redesigning Arak; providing access to centrifuge storage and production sites; and covert or undeclared facilities of concern)

- **Core Issues** (significant violations of provisions for resolving the IAEA’s Possible Military Dimension concerns; monitoring of centrifuge storage; significant interference with established monitoring procedures; establishing supply chain and procurement transparency)

- **Sanction Relief Issues** (significant delays in the implementation of sanctions relief after milestones have been met)

On top of these concerns, the P5+1 nations should insist on effective modalities for the conduct of inspections. This should include emphasis on full compliance with the timelines specified in the agreement. Any denial of access under the set time for resolution should have a clearly defined remedy. All parties must understand this so that nonperformance has clear consequences. Small repeated infractions or a culture of repeated noncompliance cannot become the norm for how the agreement is implemented. The concept of “managed access” must thus be defined and clarified by the actual practices of the inspection process and by the work of the Joint Commission. If these understandings are not set, the agreement may implode over time.

This, we acknowledge, will not be an easy task. But when there is such a mutual distrust at the outset of an agreement, some agreed upon understanding of what will not be tolerated for nonperformance will go a long way in reducing dangerous miscalculations and gaming by the parties. To affirm this
conviction as a matter of strategic deterrence for the region the United States must be clear that Iran’s acquisition of a nuclear weapon will not be tolerated. Some have argued that in accepting the agreement, the Congress should simultaneously enact an authorization for the use of force in the event of the discovery of a material breach to be used at the discretion of the president. To be sure, any such threat of U.S. action would have to conform to the procedures the P5+1 develop for identifying a material breach so that the authorization of use force does not become a unilateral U.S. threat to break the agreement and use force on the basis of the first adverse intelligence report it receives. To be effective diplomatically, it must be coordinated with appropriate sanctions and snap-back procedures.

Recommendation: We recommend that immediately the parties use the Joint Commission to begin discussions and create a guidebook on what would constitute a material breach and the range of consequences that would follow.

- The guidebook should list the top issues where there may be continued disagreement over the terms of the agreement or where noncompliance would be most significant. It is to be expected that there will be issues concerning inspections (e.g., timing, locations, scope, equipment, etc.), enrichment levels, possible military dimensions, centrifuge monitoring, research & development projects, potential diversion of nuclear materials, etc. The parties should produce a playbook anticipating these issues and addressing ways to resolve them and both the penalties and potential remedies.

- The guidebook should delineate between technical vs. policy issues and corresponding forms of resolution. In the playbook purely technical issues should be separated from policy issues so clear and unambiguous technical standards can be established.

- The guidebook should emphasize the critical importance of compliance and verification. While spelling out a long list of absolute redlines with specific remedies may be counterproductive, spelling out one or two definitive remedies for unambiguous gross violations may be helpful if it would give all parties a clear indication that there is a possibility that any deal reached could be undone given a clear material breach of the JCPOA. Examples would be the discovery of an undeclared hidden centrifuge production site, the discovery of the purchase or procurement of significant quantities of nuclear materials outside of the procurement channel as delineated by Section 6.1 of Annex III (Civil Nuclear Cooperation), or a clandestine reprocessing facility. Such an approach would give the agreement gravitas and set the stage for meaningful discussions when the accumulation of lesser violations might bring one party closer to walking away from the agreement.

VI. Explore New Technologies and Open Source Tools for Monitoring a Nuclear Agreement with Iran

Key Finding: More and more tools such as big data analytics and commercial remote sensing are available in the public domain and are typically for purchase at affordable prices or often freely available; consequently, a variety of actors including states, the IAEA, corporations, divestment groups, and non-governmental watchdogs will make increasing use of these tools to advance their agendas. The parties to the agreement need to be prepared for ways in which these tools could help or harm the effectiveness of the agreement.

Discussion: Open source tools include several technologies and analytic methods such as: commercial remote sensing (for example, with satellites, drones, and airplanes equipped with visual, infrared, other electromagnetic sensors, and acoustic sensors), data mining of social media and websites, and analysis of commercial global trade information, scientific and other academic literature, and news media outlets. Commercial satellite imagery, in particular, is getting better in terms of spatial and spectral resolution. Other platforms and their sensors are also making greater strides in effectiveness. In parallel, the ability to acquire the images and information from these sensors has tended to drop in cost. Moreover, software to search for statistical patterns in terabytes of data has become more effective and faster in just the past decade and will likely continue to improve. More corporations are entering these sectors to provide services to private businesses, government agencies, and non-governmental agencies.

But open source tools are not omniscient. For example, commercial satellites cannot look inside buildings with opaque roofs, although some collection technology and analytical techniques could help analysts make inferences about possible activities inside these structures. Big data analytics are not perfect, either. Human decision-making and behavioral patterns are complex, and even the best statistical analysis cannot reveal all the thinking and intentions of Iranian leaders and technical experts in the nuclear program.

There are important caveats with the use of any tools, whether open or classified. Most experts expect claims and counter-claims to be expressed with unprecedented velocity, especially early on in a post-agreement environment. The challenge will be separating the wheat from the chaff. False positives are to be expected in which there appears to be evidence of a breach of an agreement, but in actuality the monitored party is still in compliance. For instance, an analyst assessing a commercially acquired satellite image might believe that a structure in an image is a building housing clandestine centrifuges, but instead the building is a warehouse for non-nuclear commercial goods. In contrast, false negatives would give the impression that there is compliance when in fact a breach has occurred. Monitored parties have at times been able to hide activities from outside monitoring. For example, in the lead up to the May 1998 nuclear tests, Indian technical experts knew when to move equipment so as to escape detection by spy satellites.

In the past two decades, the IAEA has made increasing use of these tools in its mission to strengthen the effectiveness of safeguards. In the words of Kahana Chiambro, former Director of Safeguards Information Technology, “Information analysis forms the core of strengthened safeguards. All of this new information has to be collected, processed, and evaluated, and used by the Agency to draw the conclusion that there is no evidence of undeclared nuclear material or activities in that state . . . This was, and remains, a challenging enterprise.” The challenges involve lack of adequate resources for the IAEA to be able to hire a sufficient number of highly qualified analysts who are critical thinkers and puzzle solvers. This team needs to have members with facility in the languages of the states being assessed, with information technology savvy, and with the capacity to jump back and forth between the system’s level and the individual components of a system, such as the network of interconnections among the people, parts, processes, and procurements of a nuclear program.
The USG. government agencies of the other P5+1, corporations, as well as non-governmental watchdog organizations will most likely use data mining of open source information to understand the attitudes (such as views toward their government and other countries) and behaviors (such as purchasing decisions) of the Iranian public and how the implementation of the agreement is affecting them. Such data analysis could point to what could influence the Iranian public. Iranian groups both pro- and anti-government will also likely make use of these techniques to understand what can influence the course of the implementation of the agreement. Increasingly big data and information analytics is evolving and providing policy makers with new insights and approaches to analyze behavior. More research and development of tools and applications deserve more support and exploration.

**Recommendations:** We recommend that:

- Because transparency through open use of open source tools is a vital principle for increasing the likelihood of Iranian compliance with the agreement, states parties should encourage societal verification. In particular, Iranians should be encouraged to use open-source tools to monitor the implementation of the agreement and thus become collaborators to help ensure the success of the agreement.

- Member states of the IAEA should provide the Agency with more human, financial, and technical resources to expand and strengthen its open-source analytic capabilities. This will be necessary given the new roles assigned to the IAEA under the July 14, 2015 agreement text.

- The implementing parties should use big data analytics to help with assessing the efficacy of the “Procurement Working Group” (channel procurement process as spelled out in the July 14, 2015 text) to detect any unauthorized purchases or acquisitions outside this mechanism.

- The Joint Commission (Recommendation 1, above) should establish a working group that would focus on discussing concerns arising from open source findings that appear to identify an alleged breach of the agreement. This working group should bring its assessment of recommended resolutions of the potential concerns or disputes to the leading representatives of the Joint Commission. Because of the joint nature of this working group, Iran will have a stake in resolving ambiguities.

- A clearinghouse within the NGO community should be created in order to build a cadre of experts through reputation for careful impartial analysis of open source information. Already, some are leading academic centers that can form the nuclei to grow this clearinghouse.

---

2. The P5+1 is comprised of China, France, Germany, Russia, the United Kingdom, and the United States.
9. Given suspicions of the Revolutionary Guard and the Iranian security services about U.S. intentions, this is a matter that has to be handled by the USG and IAEA with considerable finesse. (Nothing would undermine the agreement quicker than to have a U.S.-citizen IAEA inspector detained by Iranian security forces.) One possible confidence building measure would be for Iran to invite P5+1 observers to accompany some inspections.