24th Annual Review of the Field of National Security Law

CONFERENCE MATERIAL

DAY TWO

SPONSORED BY:

American Bar Association
Standing Committee on Law and National Security

Center for National Security Law
University of Virginia School of Law

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

Center on National Security and the Law
Georgetown Law

November 6—November 7, 2014

Capital Hilton Hotel
1001 16th Street, NW
Washington, DC
# Conference Material: Day Two

## Panel IV

**Ethical Issues Facing Lawyers Practicing National Security Law - A Discussion**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Rules of Professional Conduct - American Bar Association</td>
<td>1</td>
</tr>
<tr>
<td>&quot;The National Security Lawyer&quot; <em>(In the Common Defense)</em> - Judge James E. Baker</td>
<td>25</td>
</tr>
</tbody>
</table>

## Panel V

**The Economic & Financial Threat Domain: Making Smart Sanctions Smarter**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Civil Litigation Against Terrorism: Neglected Promise&quot; <em>(Legal Issues in the Struggle Against Terror)</em> - John Norton Moore</td>
<td>37</td>
</tr>
<tr>
<td>Enforcement Provisions Against Sponsors of Terrorism - Steven R. Perles</td>
<td>53</td>
</tr>
<tr>
<td>What Putin Is Costing Russia <em>(The Wall Street Journal)</em> - Ilan Berman</td>
<td>101</td>
</tr>
<tr>
<td>Putin's Costly Ukraine Policy <em>(The Moscow Times)</em> - Ilan Berman</td>
<td>103</td>
</tr>
<tr>
<td>Iran's Mullahs Blame Mahmoud <em>(The Wall Street Journal)</em> - Ilan Berman</td>
<td>105</td>
</tr>
<tr>
<td>The Economic and Financial Threat Domain - Roger W. Robertson, Jr.</td>
<td>107</td>
</tr>
<tr>
<td>About the Office of Foreign Assets Control (OFAC) - U.S. Department of the Treasury</td>
<td>109</td>
</tr>
</tbody>
</table>

## Panel VI

**Military Justice: Continuity or Change?**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Military Justice System and Command Accountability - Charles J. Dunlap, Jr.</td>
<td>113</td>
</tr>
<tr>
<td>&quot;Top Ten Reasons Sen. Gillibrand’s Bill is the Wrong Solution to Military Sexual Assault&quot; <em>(The Modern American Military)</em> - Charles J. Dunlap, Jr.</td>
<td>125</td>
</tr>
<tr>
<td>&quot;Military Justice&quot; <em>(The Modern American Military)</em> - Charles J. Dunlap, Jr.</td>
<td>143</td>
</tr>
<tr>
<td>Lawful Command Emphasis: Talk Offense, Not Offender; Talk Process, Not Results - Colonel James F. Garrett, Colonel Mark “Max” Maxwell, Lieutenant Colonel Matthew A. Calarco &amp; Major Franklin D. Roosevelt</td>
<td>183</td>
</tr>
<tr>
<td>Memorandum for Secretaries of the Military Departments - The Honorable Charles T. Hagel</td>
<td>205</td>
</tr>
</tbody>
</table>

## Panel VII

**Cybersecurity - Will We Ever Be Secure?**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report to the Board of Governors <em>(November 2012)</em> - American Bar Association</td>
<td>209</td>
</tr>
<tr>
<td>Resolution 118 <em>(August 2013)</em> - American Bar Association</td>
<td>217</td>
</tr>
<tr>
<td>Resolution 105A <em>(August 2012)</em> - American Bar Association</td>
<td>233</td>
</tr>
<tr>
<td>Resolution 109 <em>(August 2014)</em> - American Bar Association</td>
<td>239</td>
</tr>
<tr>
<td>Panel VII</td>
<td>Title and Author</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cybersecurity - Will We Ever Be Secure?</td>
<td>Foreign Spies Stealing US Economic Secrets in Cyberspace - Office of the National Counterintelligence Executive</td>
</tr>
<tr>
<td></td>
<td>Chapter: “Understanding Cyber and Data Security Risks and Best Practices” (The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals) - Lucy L. Thomson and Randy V. Sabett (chapter authors)</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity: Legislation, Hearings, and Executive Branch Documents - Rita Tehan</td>
</tr>
<tr>
<td></td>
<td>Executive Order 13636 - Improving Critical Infrastructure Cybersecurity - Federal Register</td>
</tr>
<tr>
<td></td>
<td>Antitrust Policy Statement on Sharing of Cybersecurity Information - Department of Justice and Federal Trade Commission</td>
</tr>
<tr>
<td></td>
<td>Framework for Improving Critical Infrastructure Cybersecurity - National Institute of Standards and Technology</td>
</tr>
</tbody>
</table>
PANEL IV:

ETHICAL ISSUES FACING LAWYERS
PRACTICING NATIONAL SECURITY LAW – A DISCUSSION

HARVEY RISHIKOF
&
THE HONORABLE JAMES BAKER
MODEL RULES OF PROFESSIONAL CONDUCT

PREAMBLE: A LAWYER'S RESPONSIBILITIES

[1] A lawyer, as a member of the legal profession, is a representative of clients, an officer of the legal system and a public citizen having special responsibility for the quality of justice.

[2] As a representative of clients, a lawyer performs various functions. As advisor, a lawyer provides a client with an informed understanding of the client’s legal rights and obligations and explains their practical implications. As advocate, a lawyer zealously asserts the client’s position under the rules of the adversary system. As negotiator, a lawyer seeks a result advantageous to the client but consistent with requirements of honest dealings with others. As an evaluator, a lawyer acts by examining a client’s legal affairs and reporting about them to the client or to others.

[3] In addition to these representational functions, a lawyer may serve as a third-party neutral, a nonrepresentational role helping the parties to resolve a dispute or other matter. Some of these Rules apply directly to lawyers who are or have served as third-party neutrals. See, e.g., Rules 1.12 and 2.4. In addition, there are Rules that apply to lawyers who are not active in the practice of law or to practicing lawyers even when they are acting in a nonprofessional capacity. For example, a lawyer who commits fraud in the conduct of a business is subject to discipline for engaging in conduct involving dishonesty, fraud, deceit or misrepresentation. See Rule 8.4.

[4] In all professional functions a lawyer should be competent, prompt and diligent. A lawyer should maintain communication with a client concerning the representation. A lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Rules of Professional Conduct or other law.

[5] A lawyer’s conduct should conform to the requirements of the law, both in professional service to clients and in the lawyer’s business and personal affairs. A lawyer should use the law’s procedures only for legitimate purposes and not to harass or intimidate others. A lawyer should demonstrate respect for the legal system and for those who serve it, including judges, other lawyers and public officials. While it is a lawyer’s duty, when necessary, to challenge the rectitude of official action, it is also a lawyer’s duty to uphold legal process.

[6] As a public citizen, a lawyer should seek improvement of the law, access to the legal system, the administration of justice and the quality of service rendered by the legal profession. As a member of a learned profession, a lawyer should cultivate knowledge of the law beyond its use for clients, employ that knowledge in reform of the law and work to strengthen legal education. In addition, a lawyer should further the public’s

---

1 Selected sections of the ABA Model Rules of Professional Conduct (MRPC). The ABA House of Delegates adopted the MRPC in 1983 and today the MRPC continue to serve as models for the ethics rules of most states.
understanding of and confidence in the rule of law and the justice system because legal institutions in a constitutional democracy depend on popular participation and support to maintain their authority. A lawyer should be mindful of deficiencies in the administration of justice and of the fact that the poor, and sometimes persons who are not poor, cannot afford adequate legal assistance. Therefore, all lawyers should devote professional time and resources and use civic influence to ensure equal access to our system of justice for all those who because of economic or social barriers cannot afford or secure adequate legal counsel. A lawyer should aid the legal profession in pursuing these objectives and should help the bar regulate itself in the public interest.

[7] Many of a lawyer's professional responsibilities are prescribed in the Rules of Professional Conduct, as well as substantive and procedural law. However, a lawyer is also guided by personal conscience and the approbation of professional peers. A lawyer should strive to attain the highest level of skill, to improve the law and the legal profession and to exemplify the legal profession's ideals of public service.

[8] A lawyer's responsibilities as a representative of clients, an officer of the legal system and a public citizen are usually harmonious. Thus, when an opposing party is well represented, a lawyer can be a zealous advocate on behalf of a client and at the same time assume that justice is being done. So also, a lawyer can be sure that preserving client confidences ordinarily serves the public interest because people are more likely to seek legal advice, and thereby heed their legal obligations, when they know their communications will be private.

[9] In the nature of law practice, however, conflicting responsibilities are encountered. Virtually all difficult ethical problems arise from conflict between a lawyer's responsibilities to clients, to the legal system and to the lawyer's own interest in remaining an ethical person while earning a satisfactory living. The Rules of Professional Conduct often prescribe terms for resolving such conflicts. Within the framework of these Rules, however, many difficult issues of professional discretion can arise. Such issues must be resolved through the exercise of sensitive professional and moral judgment guided by the basic principles underlying the Rules. These principles include the lawyer's obligation zealously to protect and pursue a client's legitimate interests, within the bounds of the law, while maintaining a professional, courteous and civil attitude toward all persons involved in the legal system.

[10] The legal profession is largely self-governing. Although other professions also have been granted powers of self-government, the legal profession is unique in this respect because of the close relationship between the profession and the processes of government and law enforcement. This connection is manifested in the fact that ultimate authority over the legal profession is vested largely in the courts.

[11] To the extent that lawyers meet the obligations of their professional calling, the occasion for government regulation is obviated. Self-regulation also helps maintain the legal profession's independence from government domination. An independent legal profession is an important force in preserving government under law, for abuse of legal
authority is more readily challenged by a profession whose members are not dependent on government for the right to practice.

[12] The legal profession's relative autonomy carries with it special responsibilities of self-government. The profession has a responsibility to assure that its regulations are conceived in the public interest and not in furtherance of parochial or self-interested concerns of the bar. Every lawyer is responsible for observance of the Rules of Professional Conduct. A lawyer should also aid in securing their observance by other lawyers. Neglect of these responsibilities compromises the independence of the profession and the public interest which it serves.

[13] Lawyers play a vital role in the preservation of society. The fulfillment of this role requires an understanding by lawyers of their relationship to our legal system. The Rules of Professional Conduct, when properly applied, serve to define that relationship.

**SCOPE:**

[14] The Rules of Professional Conduct are rules of reason. They should be interpreted with reference to the purposes of legal representation and of the law itself. Some of the Rules are imperatives, cast in the terms "shall" or "shall not." These define proper conduct for purposes of professional discipline. Others, generally cast in the term "may," are permissive and define areas under the Rules in which the lawyer has discretion to exercise professional judgment. No disciplinary action should be taken when the lawyer chooses not to act or acts within the bounds of such discretion. Other Rules define the nature of relationships between the lawyer and others. The Rules are thus partly obligatory and disciplinary and partly constitutive and descriptive in that they define a lawyer's professional role. Many of the Comments use the term "should." Comments do not add obligations to the Rules but provide guidance for practicing in compliance with the Rules.

[15] The Rules presuppose a larger legal context shaping the lawyer's role. That context includes court rules and statutes relating to matters of licensure, laws defining specific obligations of lawyers and substantive and procedural law in general. The Comments are sometimes used to alert lawyers to their responsibilities under such other law.

[16] Compliance with the Rules, as with all law in an open society, depends primarily upon understanding and voluntary compliance, secondarily upon reinforcement by peer and public opinion and finally, when necessary, upon enforcement through disciplinary proceedings. The Rules do not, however, exhaust the moral and ethical considerations that should inform a lawyer, for no worthwhile human activity can be completely defined by legal rules. The Rules simply provide a framework for the ethical practice of law.

[17] Furthermore, for purposes of determining the lawyer's authority and responsibility, principles of substantive law external to these Rules determine whether a client-lawyer relationship exists. Most of the duties flowing from the client-lawyer relationship attach only after the client has requested the lawyer to render legal services and the lawyer has agreed to do so. But there are some duties, such as that of confidentiality under Rule 1.6,
that attach when the lawyer agrees to consider whether a client-lawyer relationship shall be established. See Rule 1.18. Whether a client-lawyer relationship exists for any specific purpose can depend on the circumstances and may be a question of fact.

[18] Under various legal provisions, including constitutional, statutory and common law, the responsibilities of government lawyers may include authority concerning legal matters that ordinarily reposes in the client in private client-lawyer relationships. For example, a lawyer for a government agency may have authority on behalf of the government to decide upon settlement or whether to appeal from an adverse judgment. Such authority in various respects is generally vested in the attorney general and the state's attorney in state government, and their federal counterparts, and the same may be true of other government law officers. Also, lawyers under the supervision of these officers may be authorized to represent several government agencies in intragovernmental legal controversies in circumstances where a private lawyer could not represent multiple private clients. These Rules do not abrogate any such authority.

[19] Failure to comply with an obligation or prohibition imposed by a Rule is a basis for invoking the disciplinary process. The Rules presuppose that disciplinary assessment of a lawyer's conduct will be made on the basis of the facts and circumstances as they existed at the time of the conduct in question and in recognition of the fact that a lawyer often has to act upon uncertain or incomplete evidence of the situation. Moreover, the Rules presuppose that whether or not discipline should be imposed for a violation, and the severity of a sanction, depend on all the circumstances, such as the willfulness and seriousness of the violation, extenuating factors and whether there have been previous violations.

[20] Violation of a Rule should not itself give rise to a cause of action against a lawyer nor should it create any presumption in such a case that a legal duty has been breached. In addition, violation of a Rule does not necessarily warrant any other nondisiplinary remedy, such as disqualification of a lawyer in pending litigation. The Rules are designed to provide guidance to lawyers and to provide a structure for regulating conduct through disciplinary agencies. They are not designed to be a basis for civil liability. Furthermore, the purpose of the Rules can be subverted when they are invoked by opposing parties as procedural weapons. The fact that a Rule is a just basis for a lawyer's self-assessment, or for sanctioning a lawyer under the administration of a disciplinary authority, does not imply that an antagonist in a collateral proceeding or transaction has standing to seek enforcement of the Rule. Nevertheless, since the Rules do establish standards of conduct by lawyers, a lawyer's violation of a Rule may be evidence of breach of the applicable standard of conduct.

[21] The Comment accompanying each Rule explains and illustrates the meaning and purpose of the Rule. The Preamble and this note on Scope provide general orientation. The Comments are intended as guides to interpretation, but the text of each Rule is authoritative.
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. ²

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

² http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html
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(e) (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.\(^4\)

**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.

---

\(^4\) [http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_3_diligence.html](http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_3_diligence.html)
[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: COMMUNICATIONS
(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.5

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.

5 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_4_communications.html
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 1.13: 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.6

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

6 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_13_organization_as_client.html
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 1.16(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 3.3: CANDOR TOWARDS 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.\(^7\)

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.

\(^7\) http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_3_3_candor_toward_the_tribunal.html
[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
[4] 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
[5] 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.

[6] 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.
[7] 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].

[8] 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.

[9] 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
[10] 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.

[11] 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

---

8 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_3_4_fairness_to_opposing_party_counsel.html
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 4.1: TRUTHFULNESS IN STATEMENTS TO OTHERS**

In the course of representing a client a lawyer shall not knowingly:

(a) make a false statement of material fact or law to a third person; or

(b) fail to disclose a material fact to a third person when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6. 9

**Comment:**

Misrepresentation

[1] A lawyer is required to be truthful when dealing with others on a client's behalf, but generally has no affirmative duty to inform an opposing party of relevant facts. A misrepresentation can occur if the lawyer incorporates or affirms a statement of another person that the lawyer knows is false. Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements. For dishonest conduct that does not amount to a false statement or for misrepresentations by a lawyer other than in the course of representing a client, see Rule 8.4.

**Statements of Fact**

[2] This Rule refers to statements of fact. Whether a particular statement should be regarded as one of fact can depend on the circumstances. Under generally accepted

---

9 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_4_1_truthfulness_in_statements_to_others.html

22
conventions in negotiation, certain types of statements ordinarily are not taken as statements of material fact. Estimates of price or value placed on the subject of a transaction and a party’s intentions as to an acceptable settlement of a claim are ordinarily in this category, and so is the existence of an undisclosed principal except where nondisclosure of the principal would constitute fraud. Lawyers should be mindful of their obligations under applicable law to avoid criminal and tortious misrepresentation.

Crime or Fraud by Client
[3] Under Rule 1.2(d), a lawyer is prohibited from counseling or assisting a client in conduct that the lawyer knows is criminal or fraudulent. Paragraph (b) states a specific application of the principle set forth in Rule 1.2(d) and addresses the situation where a client’s crime or fraud takes the form of a lie or misrepresentation. Ordinarily, a lawyer can avoid assisting a client’s crime or fraud by withdrawing from the representation. Sometimes it may be necessary for the lawyer to give notice of the fact of withdrawal and to disaffirm an opinion, document, affirmation or the like. In extreme cases, substantive law may require a lawyer to disclose information relating to the representation to avoid being deemed to have assisted the client’s crime or fraud. If the lawyer can avoid assisting a client’s crime or fraud only by disclosing this information, then under paragraph (b) the lawyer is required to do so, unless the disclosure is prohibited by Rule 1.6.

RULE 5.2 RESPONSIBILITIES OF A SUBORDINATE LAWYER
(a) A lawyer is bound by the Rules of Professional Conduct notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer’s reasonable resolution of an arguable question of professional duty. 10

Comment:
[1] Although a lawyer is not relieved of responsibility for a violation by the fact that the lawyer acted at the direction of a supervisor, that fact may be relevant in determining whether a lawyer had the knowledge required to render conduct a violation of the Rules. For example, if a subordinate filed a frivolous pleading at the direction of a supervisor, the subordinate would not be guilty of a professional violation unless the subordinate knew of the document’s frivolous character.

[2] When lawyers in a supervisor-subordinate relationship encounter a matter involving professional judgment as to ethical duty, the supervisor may assume responsibility for making the judgment. Otherwise a consistent course of action or position could not be taken. If the question can reasonably be answered only one way, the duty of both lawyers

http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_2_responsibilities_of_a_subordinate_lawyer.html
is clear and they are equally responsible for fulfilling it. However, if the question is reasonably arguable, someone has to decide upon the course of action. That authority ordinarily reposes in the supervisor, and a subordinate may be guided accordingly. For example, if a question arises whether the interests of two clients conflict under Rule 1.7, the supervisor's reasonable resolution of the question should protect the subordinate professionally if the resolution is subsequently challenged.
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 apprise 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 process 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, sincere 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 certain 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 is the threat that 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 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 officer 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 intelligence, 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
nation of law and lawyers. It is men and women who write the law, interpret the law, and decide whether to uphold the law. Where national security is at stake, the human influence is manifest. "National security" necessarily involves the application of subjective values and not just security criteria. Further, as considered in Chapter 4, the law is as dependent on theory as it is on black-letter principle, and thus is dependent on human values and choice. Even where the law is clear, the facts rarely arc, for the reasons articulated in Chapter 7. The application of fact to law, of intelligence to security, involves human judgment rather than the mechanical review of facts.

Law also involves moral courage. Field Marshal Slim, who served on the Western Front during the First World War and is considered one of the best commanders during World War II, compared physical and moral courage. He described moral courage as "a more reasoning attitude, which enables [a man] coolly to stake career, happiness, his whole future, on his judgment of what he thinks either right or worthwhile." Slim said,

I have known many men who had marked physical courage, but lacked moral courage. On the other hand I have seen men who undoubtedly possessed moral courage very cautious about taking physical risks. But I have never met a man with moral courage who would not, when it was really necessary, face bodily danger. Moral courage is a higher and a rarer virtue than physical courage.¹

Most lawyers will not have Field Marshal Slim's opportunity to test the comparative proposition. But they will have their moral courage tested. They will be tested sitting at a Principals Meeting when they have to decide when, whether, and how to speak up. They will be tested when they must step outside their personalities, loud, quiet, or in between, and step into a different role in order to apply the law more meaningfully. The quiet personality will be asked to make public presentations on behalf and in defense of the law. Sometimes the strong personality must sit down for the law, for example, at an interagency meeting where bureaucratic diplomacy may be the order of the day. But minutes later, in the face of the deputy secretary or national security advisor, the lawyer must have the courage to insist on attendance at a necessary meeting. In short, national security law is as contingent on the national security lawyer as it is on the law.

A. NATIONAL SECURITY LEGAL PRACTICE

In a constitutional democracy decisions are intended to be made according to law. That means that sound national security process must incorporate 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, including lawyers, to certify requests for electronic surveillance or physical search before they are submitted to the FISA court. In other cases, the president 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 DEIS, as well as the chairman's legal advisor. Of course, in context, senior deputies 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 Council'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 criminal division are all central players on issues of intelligence and counterterrorism. 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 officials 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 mentioned 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 counselor 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.
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 AECA 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 identifica-
tion of legal issues embedded in policy options, policy decisions, and policy statements. At the NSC, for example, counsel traditionally coordinate 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.

The National Security Lawyer

In addition, lawyers serving as agency general counsel, or their equiva-
 lent, perform or oversee the performance of myriad tasks generally associ-
ated 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 legis-
lative 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, per-
sonality 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 con-
straints 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 emo-
tional 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!" 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 internal 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 distinction between understanding, testing, and bullying may be lost. Policymakers 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, knowing 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 “mission creep,” whereby one legal question becomes seventeen, requiring not one lawyer but forty-three to answer). Of course, decisionmakers may also fear that the lawyer may say no to something the policymaker wants to do. Rule of law often depends on the lawyer being in 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 memos, 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 perceived 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 targets without having an understanding of the weapons, munitions, and tactics that inform judgments about necessity and proportionality. Likewise, counsel addressing the use of force should understand the qualitative and quantitative 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) textual adjustments that defer or eliminate concerns, or (g) just the force of personality or diplomacy. Concerns about the deployment of armed forces in civil context might be addressed through resort to any one of these methodologies or by textually limiting the scope, service, or situation in which the forces might be used. Such limitations might be put in the president’s action memoranda, 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 lunches of the sort that Mr. Carlucci and Mr. Berger found effective.

Where lawyers are being used to dress policy disagreements up in determinative 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 side-track deliberations. Moreover, just as policymakers forum shop for "can do" lawyers, or perhaps compliant 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 know about the day-to-day activities of the government. One purpose of these exercises is to alert policymakers and lawyers to legal obstacles that lie ahead so that lawyers might find the means of circumnavigating before the crisis.

Preparation also entails educating the policymaker. Absent the 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 A.M. 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 explore for the first time the delicate legal policy 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 preparation also helps establish lines of communication and a common vocabulary of nuances 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. In 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 remain 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 practice 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 private 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.¹
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 less apt in identifying and defining the responsibilities of the national security lawyer. To start, in government context, there are differing views on just who (or perhaps what) is the "client." Scholars and practitioners have identified both ultimate and conceptual candidates, including the president, the agency head, 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 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 determinative by the identification of the "client." 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 to 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 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 ethics 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 "dirt 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 an Al Qaeda affiliate.

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 dispersion 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 "unlawful" 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 advisory 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 counterarguments 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, or if so, who must/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 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, 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 such 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, if 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, well as the President, 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 unseen will 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 review 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 appraisal 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 actions 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 will 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 in 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.
Panel V:

The Economic and Financial Threat Domain: Making Smart Sanctions Smarter

Moderator:
John Norton Moore
Chapter 8

Civil Litigation Against Terrorism: Neglected Promise

John Norton Moore

"For as in absolute governments the king is law, so in free countries the law ought to be king; and there ought to be no other."

Thomas Paine,
Common Sense (1776)

"It is essential to the idea of a law, that it be attended with a sanction...."

Alexander Hamilton,
The Federalist no. 11 (1787)

* John Norton Moore is the Walter L. Brown Professor of Law at the University of Virginia and Director of the Center for National Security Law. He formerly served as Counsel on International Law to the Department of State, United States Ambassador to the United Nations Conference on the Law of the Sea, Chairman of the National Security Council Task Force on the Law of the Sea and Deputy Special Representative of the President for the Law of the Sea, and the founding Chairman of the Board of Directors of the United States Institute of Peace. He is a four term Chairman of the American Bar Association Standing Committee on National Security Law and is co-counsel in the case of Acree v. Republic of Iraq, 271 F.Supp.2d 179 (D.C. Dist. Col. 2003), 370 F.3d 41 (D.C. Cir. 2004), cert. denied, 135 S.C. 1928 (2005), (see also the motion for relief under Fed. R. Civ. P. 60(b)(6) 2005), discussed in this chapter. As the Counselor on International Law to the Department of State he drafted the United States Convention against the Spread of Terrorism in the aftermath of the Munich Olympics massacre and was one of the draftsmen of the original Foreign Sovereign Immunities Act. The author would like to thank Allan Gerson and Steven R. Perel for their comments on a draft of this chapter. Both attorneys have been pioneers in the use of civil litigation against terror states.
Introduction

In an age in which "the rule of law" has become a universal slogan, as well as a core component in United States and democratic nation foreign policy, one might think that civil suits against terror states would be an established part of the war on terror. But sadly this is not the reality; in large part because the movement in international law away from the complete sovereign immunity of "the King can do no wrong" has been glacially slow, and because, in the United States "old thinking" in the Executive legal offices has all too often vigorously opposed such civil suits. Change, however, is coming and coming fast, thanks primarily to the practicing bar and to more forward thinking from the Congress.

This chapter urges that civil litigation against terrorism, including against states complicit in supporting terrorism, may be one of the most important tools available for democratic nations in the fight against terror. In doing so, it offers the model of a Protocol to the United Nations Conventions on terrorism as a next step in moving forward to energize this important tool. But first this chapter will explore the glacial movement away from "The King Can Do No Wrong," a slowly eroding principal of "sovereign immunity" which has dominated international law and the thinking of foreign offices, and in doing so it will discuss the important new "Lautenberg Amendment" signed into law in the 2008 Defense Authorization Act. The chapter will then make the case as to why civil litigation is a uniquely capable and important tool in the fight against terror; discuss why traditional arguments against use of civil litigation are flawed.

1. As one example of State Department opposition to civil judgments even against terror states, approximately 90 days after President Bush declared Iran one of the nations in the "axis of evil" the Perles Law Firm attached Iranian real estate assets in California in support of a flagship judgment in Flatow v. Islamic Republic of Iran, 999 F. Supp. 1 (D.D.C. 1998) against Iran's knowing support of terror only to have the State Department intervene to quash the attachment.

2. See also on this general subject John Norton Moore (ed.), CIVIL LITIGATION AGAINST TERRORISM (2004); A. Gerson and I. Adler, THE PRICE OF TERROR (2001); "Civil Suits Against Terrorists, Terrorist Organizations, and States That Sponsor Terrorism," in J.N. Moore and R.F. Turner, eds., NATIONAL SECURITY LAW 484–490 (2nd Ed. 2005); and the Panel on "Civil Litigation in the War on Terror," (December 1, 2006) at the American Bar Association/Center for National Security Law 2006 Annual Conference on National Security Law, Washington, D.C. (including "Introductory Comments" by the author). While this chapter will focus on civil litigation against terror states, and their leaders, there is also

The thesis of this chapter is not simply to unleash unrestrained use of the courts in the fight against terror. There are important principles at stake in ensuring that causes of action are those rooted in broad general agreement about core principles of international law, that foreign states are treated fairly in the civil justice system, and that attachment or execution will not be directed at assets entitled to diplomatic or counselor immunity, military assets, or assets of foreign central banks. Rather the thesis of this chapter is that the use of the civil justice system, as with other dimensions of the rule of law, has a crucial place in the fight against terror. Indeed, as a Nation we are shockingly behind the curve in moving forward with well-structured efforts to empower the use of the civil justice system against terror states. Astoundingly, at a time in which we are supporting international and national law holding individuals, including heads of state, criminally responsible for acts of terrorism, and in which we have long since permitted suit against our own government for terror acts, the Executive is still too frequently shielding terror states from civil liability.

We know today that real world application of the criminal justice system is largely only for a few low-level "terror mules" we have apprehended. This does little to deter the regime elites of terror states, and the state machinery itself of such states, from their support for terror. In contrast, large civil judgments...
against terror states and their leaders who have ordered these acts of terror, 
judgments then reciprocally enforced in democratic nations around the world, 
have great potential to deter state sponsored terrorism. The democracies of 
the world are financial and economic superpowers. Terror states, and their 
leaders, need to trade with them, use their banking systems, and otherwise 
financially interact with them in crucially important ways. Further, the democracies 
are the leaders in the rule of law, and in application of their civil justice 
systems. Terror, as a form of asymmetric warfare in response to the conventional 
military superiority of the democracies, may be a self-perceived comparative 
advantage of non-democratic terror states. But the use of the rule of law in 
the courts of the democracies, combined with their financial and economic 
power, is one of their comparative advantages in fighting back. Law and lawyers 
are today so pervasive in the democracies that surely turning law loose on terror 
states, rather than simply on tobacco companies and corporate targets, will 
be greeted by broad public support and understanding. A

A Summary History of Sovereign Immunity in International and United States 
Foreign Relations Law

Toward "[a] government of laws, and not of men."
A phrase popularized in the United States by
John Adams and incorporated in the
Constitution of Massachusetts

A core meaning of the rule of law is the use of law as a check on power. Not 
surprisingly, monarchs and authoritarian leaders did not embrace the rule of 
law, just as this principle is rejected by terror states today. Thus the rise of the 
nation state following the Peace of Westphalia, which in its manifestation in most

states was non-democratic, was accompanied by a strong principal of sovereign 
immunity or, popularly "the King can do no wrong."5

The traditional view, widely accepted in international law and the foreign 
policy of the United States up until the mid 20th Century, was absolute immunity 
of the state from the jurisdiction of national courts. In the United States this 
view was reflected in the classic 1812 case of The Schooner Exchange.6 No less 
voice than that of Chief Justice John Marshall spoke in that case of the "perfect 
equality and absolute independence of sovereigns." While a few states begin 
to question this as a principal of international law even prior to World 
War II, and democracies were adopting reforms permitting civil actions against 
their own states, as with the Federal Tort Claims Act in the United States, the 
absolute theory of immunity has been tenacious.

The first seismic crack in absolute immunity occurred in the United States 
in 1952 and was revealed in an obscure letter. Thus, the United States moved 
to the "restrictive theory" of sovereign immunity as set out in a letter from the 
Acting Legal Adviser of the Department of State, Jack B. Tate, written to the 
Acting Attorney General, and subsequently called "The Tate Letter." The Tate 
Letter adopted the view, as the official view of the United States, that where nations 
are acting as private parties (actions de jure gestionis rather than de jure 
imperii), as in commercial transactions, they would no longer be immune 
suit in the courts.7 Difficulty in ex parte Executive determinations of this 
standard, and later in Executive efforts at adjudication on this issue, led John R. 
Stevenson, as Legal Adviser to the Department of State, to turn this issue 
over to the courts under a statutory mandate concerning the scope and application 
of sovereign immunity and actions against foreign nations in U.S. courts. 
As Counselor on International Law to the State Department I worked on the

---

5. See generally on the history of sovereign immunity I Restatement of the Law Third 
6. The Schooner Exchange, 11 U.S. (7 Cranch) 116 (1812). While this case is usually cited 
for "absolute immunity," it has been pointed out that the Court waved its jurisdiction simply 
as a matter of "grace and comity" so that there was really nothing "absolute" about the 
granting of immunity. Moreover, some other decisions did not grant immunity for state actions 
in violation of international law. See, e.g, Jordan Paust, "Federal Jurisdiction Over 
Extraterritorial Acts of Terrorism and Nonimmunity for Foreign Violators of International 
Law Under the PISA and the Act of State Doctrine," 23 Virginia Journal of Int'l Law 
91 (1983), and "Notes and Questions" in Paust, Van Dyke & Malone, International 
7. Id. at 137.
8. Given that a mere commercial breach of contract is subject to civil liability, surely it 
makes no sense to shield intentional acts of terror from such liability.
procedural provisions in this legislative package and cleared the package, with minor changes, through the interagency process before formal Executive Branch submission to the Congress. Subsequently, this statutory mandate, turning the issue over to the courts, was enacted into law in 1976 as the Foreign Sovereign Immunities Act (FSIA). Today this law still provides the exclusive basis for suits against foreign nations in United States courts.

Contrary to popular, and sometimes evinced judicial, opinion the FSIA is not solely jurisdictional, but made a series of important substantive changes in the law, including providing a detailed structure for service of process and altering the provisions for attachment and execution against the assets of foreign states. With respect to the scope of immunity, the FSIA eliminated immunity in most commercial transactions, claims in tort for injury to persons or property in the United States, and certain claims concerning property. As FSIA, itself an initiative of the State Department reflects, for over a quarter century,

10. It was understood by all who worked on the FSIA that it would be rooted in cause of action from underlying state law, as well as any other bases for federal statutory or common law causes of action. This is reflected in decisions in countless cases in the federal courts, is set out by the United States Supreme Court in the case of First Nat'l City Bank v. Banco Para el Comercio Exterior de Cuba, 462 U.S. 611, at 622 n.11 (1983), and remains the official view of the United States, despite the surprising action of the D.C. Circuit Court of Appeals in Acre v. Republic of Iraq, 370 F.3d 41 (2004), with no briefing or hearing to dismiss the District Court decision in Acre as having no cause of action; a lower court decision in reality rooted in multiple bases for cause of action, including underlying state laws of assault, battery and intentional infliction of emotional distress, the international law relations law of the United States against torture, and at least respondent superior from the FSIA statutory provisions themselves. For the official United States view that state law provides a basis for cause of action in FSIA cases see Brief for Amicus Curiae The United States of America in Support of Plaintiffs-Appellees in Kilburn v. Socialist People's Libyan Arab Jamahiriya, No. 03-7117, at 11, 13 (May 14, 2004) (stating under the FSIA "the foreign state ordinarily may be held liable according to state or foreign laws that apply to private individuals generally," and urging that "[t]he Court ... should allow the plaintiffs her opportunity to show in the district court whether state or foreign law would provide them a cause of action. . ."). See also Cicippio-Puleo v. Islamic Republic of Iran, 353 F.3d 1024 (2004), and the discussion of this Court of Appeals decision defying the intent of the Congress subsequently in this chapter. The Congress subsequently declared in the 2008 Defense Authorization Act that the holding in Cicippio-Puleo was now the law. For a discussion questioning whether "having lost the legislative battle [against 1605(a)(7)] action, should the government now play an active role in discouraging this kind of litigation because of possible negative impacts on U.S. interests? [and asking] Does the FISA make any provision for such intervention?" see "Suing Terrorists and Their Sponsors," Chapter 23 in S. Dycus, W. Banks, P. Raven-Hansen, Counterterrorism Law (2007) at 753. See also the further question of the Cicippio-Puleo decision id. at 752.

broad range of actions against foreign states have been permissible in our courts.

Though the FSIA had greatly narrowed where "the King can do no wrong" it was narrowly interpreted by the courts as not permitting actions for civil damages against states or their instrumentalities where the tort against Americans took place abroad, even if the tort was a terror attack. In this setting, a second seismic shift occurred in limiting absolute immunity, also led by the United States. Thus, in response to the bombing of Pan Am Flight 103 "Maid of the Seas" over Scotland, and in the aftermath of the terror shock from the bombing of the Murrah Federal Building in Oklahoma City, Congress passed amendments to the FSIA adding a new section 1605(a)(7) permitting such suits against actions abroad by states on the State Department terror list at the time the act occurred. These amendments were enacted as part of the Anti-Terrorism and Effective Death Penalty Act of 1996. They were vigorously fought by the Executive.

The new § 1605(a)(7) of the FSIA ushered in substantial litigation against terror states for actions against Americans abroad, despite a pattern of strained and narrow reading of the amendments by the D.C. Circuit, showing that the D.C. Circuit Court of Appeals was sympathetic to the "old-thinking" arguments of the Executive branch and in setting after setting effectively supporting the old rule of "the King can do no wrong." The 1996 amendments themselves were very narrowly tailored. They applied only against states which were designated by the State Department as terror states at the time the act occurred. They applied only after offering the defendant state "a reasonable opportunity to arbitrate the claim in accordance with accepted international rules of arbitration." They applied to permit suit only in a narrow category of cases "for personal injury or death that was caused by an act of torture, extrajudicial killing, aircraft sabotage, hostage taking, or the provision of material support or resources for such an act." They permitted suit only if the claimant or the victim was a national of the United States. Trial in the federal system could only be by a trial judge, not a jury. And even in these circumstances were the state not to show up the Judge had to specifically find the facts and the law, precisely as would be required for suit against the United States Government.

Five months after enactment of this important tool in the fight against terror Congress passed the "Flatow Amendment" clarifying damages available in such actions, and clarifying the scope of the federal statutory cause of action against foreign states in actions brought under 1605(a)(7). In its report on the original version of the state-sponsored terrorism amendment, the House Judiciary Committee stated that the purpose of the amendment was "to allow U.S. citizens who have been subjected to the terrorist actions enumerated in the
exception "to maintain a federal cause of action for damages against the for-

government involved." 11

The latest act in this continuing struggle between the Congress and the Ex-
cutive, with the Congress determined to permit suit in United States courts
against terror states in circumstances such as those permitted under the 1996
FSIA Amendments is the enactment of the "Lautenberg Amendment" as part
of the 2008 Defense Authorization Act. 12 This comprehensive updating of
§ 1605(a)(7) clarifies some of the ambiguities introduced into the previous law
by the courts, including clarifying that the statute of limitations to this provision
applies for all actions filed before April 24, 2006 or "10 years after the date
on which the cause of action arose," 13 establishing that in addition to being
available for United States nationals, actions under this section are also available
for members of the armed forces of the United States, and certain em-
ployees or contractors of the United States Government; and ending the abuse
of terror states delaying accountability by continually subjecting the denial of
their motion for sovereign immunity to interlocutory review. It also clarifies
that the law provides a statutory federal cause of action against the state itself,
an important clarification made necessary by the extraordinary decision of
the Court of Appeals for the D.C. Circuit in Cicippio-Puleo v. Islamic Republic of
Iran, 353 F. 3d 1024 (D.C. Cir. 2004), which simply ignored that the language
in the Flatow Amendment was the same language used to create a federal statutory
cause of action against the United States itself 14 and that the Report of the

11. H.R. Rep. No. 103-702, at 2 (1994). See also further acknowledging this conclusion
Dissenting Views, at 12.

No. 110-181, §1083 (2008). Senator Frank Lautenberg, working with Senator Arlen Specter,
was the principal sponsor of this update to the FSIA anti-terror provisions as initially em-
bodied in §1605(a)(7) of the 1996 Anti-Terrorism and Effective Death Penalty Act.

13. See also Simon v. Republic of Iraq, 529 F.3d 1187 (D.C. Cir. 2008) which reaffirmed
the original liberal meaning of the statute of limitations in the 1996 Amendments to the
FSIA even without relying on the 2008 Defense Authorization Act. This decision may sig-
nal a welcome new openness toward civil litigation against terror states by the Court of
Appeals for the District of Columbia Circuit.

14. The language is "An official, employee, or agent of a foreign state designated as a state
sponsor of terrorism ... while acting within the scope of his or her office, employment, or
agency shall be liable to a United States national ... for personal injury or death caused
by acts of that official, employee, or agent ..." It is a preposterous interpretation of this lan-
guage, which at minimum would create respondeat superior liability, to hold in the context
of its enactment and the background of the language itself as creating a statutory federal
cause of action against the U.S. Government, that it only creates a cause of action against the
individual and not the terror state, of which the individual in question is by definition an "of-

15. See H.R. Rep. No. 103-702, at 2 (1994), see also to the same effect Dissenting Views,
at 12.

16. This problem in attachment or execution against the assets of agencies or instrumen-
talities of the state was known as the Baneck doctrine. For an excellent post "Lauten-
berg Amendments" review of the struggle under United States law to permit meaningful
civil actions against terror states, including this problem, see Steven R. Perles, "The Evolu-

tion of Current Trends in Anti-Terrorism Civil Litigation" (Speech delivered before the Dist-
ric of Columbia Bar Association, March 2008). See also for an important historical review of
the struggle in U.S. law to permit suits against terror states, by one of the pioneers in
this field, Allan Gerson, "Privatizing Justice: The Role of Individual Civil Claims in the
Fight Against Terrorism," (Remarks at Hebrew University Law Faculty, Jerusalem, May 15,
2007); Allan Gerson, "Accountability Versus Immunity-Civil Suits vs. States and Aiders and
Abettors of Terrorism," (Remarks before the International Bar Association, April 10–11,
2008, Barcelona, Spain). Professor Gerson emphasizes the domestic effect of the truck
bombing of "the Alfred M. Murrah federal building in Oklahoma City, killing 168 Americans,
"in the subsequent passage of the 1996 Anti-Terrorism and Effective Death Penalty Act,
which brought in the FSIA anti-terror 1605(a)(7) actions. Alan Gerson, 2007 remarks
supra at 8–9. Gerson also notes as an example of the extreme State Department "old thinking"
in defense of immunity even against terror states the following: "In the summer of
1992, as the case Smith v. Libya convened in the U.S. District Court in Washington, Judge
Stanley Sporkin presiding, the backdoors of the court room suddenly swung open as a pla-
It should be noted that because the "tolling" provision in the statute of limitations ran out on April 24, 2006, for the future only terrorist acts of terror states, committed during the period the state was on the State Department list of terror states and then filled within 10 years of the date on which the cause of action arose, will be able to be heard under this section unless they had been previously filed in the courts. This should remove much of the concern about actions brought under state fact circumstances. This was true both under the original 1605(a)(7) and under the comprehensive updating of the Act pursuant to the Lautenberg Amendment.

Not surprisingly, in response to the Lautenberg Amendment, which would effectively hold Libya, among other terror states, liable for its acts of terrorism, Libya hired high-profile American lobbyists in an effort to win exemption from the law. Further, indicating that the State Department continues its enthusiastic commitment to "old thinking" in this area, on March 18, 2008, the George W. Bush Administration sent a letter to Speaker Nancy Pelosi seeking a waiver of the entire Lautenberg Amendment with respect to Libya and other states that have been removed from the U.S. list of terror states. The letter, sent from Secretaries Condolesenza Rice, Robert Gates, Carlos M. Gutierrez, and Samuel W. Bodman, says in part:

When states, at our urging, take the necessary steps for this change in status under U.S. law, the United States has a strong interest in developing commercial and security relationships with them to provide a continuing incentive to stand with us against the threats of global terrorism. Indeed, in some cases offering them such relationships en-

...
back—the progressive elimination of "the king can do no wrong." Thus, in 2004 the United Nations General Assembly passed a resolution supporting a new draft Convention on Jurisdictional Immunities of States and Their Property. This new draft Convention would ensure sovereign immunity for state-sponsored acts of terrorism and would otherwise dramatically narrow the potential for civil suits against states. Most recently, on December 23, 2008, Germany instituted proceedings against Italy before the International Court of Justice for allegedly failing to respect Germany's sovereign immunity growing out of international humanitarian law violations by Germany in World War II. These recent developments show that progressive development of the rule of law against state-sponsored terrorism and other illegal actions by states is at serious risk unless the United States Executive Branch drops its "old thinking" and the United States assumes its rightful role as champion of the rule of law.

But there are also more positive signs in acceptance of civil litigation as an important tool against terrorism. Thus, on June 2, 2009, the Canadian Minister of Public Safety, the Honorable Peter Van Loan, announced tabling of legislation "to allow victims of terrorism to sue perpetrators of terrorism and their supporters." The new law would lift state immunity for states identified by the Government of Canada as supporters of terrorism, create a new cause of action in Canadian courts, and would facilitate effective recovery through assistance of the Ministers of Foreign Affairs and Finance. The official Canadian press release reads: "The Government of Canada is determined to take decisive steps to protect Canadians from the threat of terrorism. By tabling this legislation, the Government of Canada is sending a clear message that perpetrators of terrorism and their supporters will be held accountable for their actions.

The Potential for Civil Litigation as a Core Weapon in the War on Terror

"I call on all who love freedom to stand with us now. Together we shall achieve victory."
Gen. Dwight David Eisenhower
D-Day Broadcast June 6, 1944

Terror is a form of asymmetric warfare used against the United States and other democratic nations by nations and groups which cannot hope to match our regular military capabilities. Bombings, kidnappings, torture and attacks against the civilian and business interests of the democracies, as well as against the infrastructure of international commerce such as civil aviation, all of which are implemented so as to be concealed in their origin, are modalities employed by totalitarian and authoritarian states and groups who hope by means of violence to avoid response. Moreover, because full scale military response is both politically and economically costly, in addition to the inevitable loss of life, it takes an extremely high threshold of attack before the democracies will respond with the use of military force. Further, the built-in deniability of the terror state or group that it is implicated in the terror attack adds a high political barrier against military response, with the democratic nation population generally opposed to war and skeptical about claims largely known, even if then, to their intelligence services. Yet another limitation with respect to full scale military response is that such a response inevitably hits not only the terror state regime elite, but also many innocent civilians (and even military) not involved in the decision to wage an aggressive campaign of terrorism in support of their objectives. Increasingly we are learning that deterrence should be focused on the regime elites ordering aggression, democide and terrorism,

21. Iraq, in its brief in Republic of Iraq v. Beatty, and Republic of Iraq v. Simon (NOS. 07-1090 & 08-539) (March 2009), as a "petitionor" Petitioner before the Supreme Court, also seeks to turn the clock back to pre-FISA days in which claims concerning torture and taking of "human shields" were pursued "through State-to-State negotiations, rather than subjecting each nation to coercive lawsuits in the courts of the other." Id. at 56. Not only does this repudiate the legislative structure of the FISA and any meaningful rule of law, but it also would return to the failed accountability of the past with its fictional redress. Sadly, the "old thinking" Department of State Legal Claims Office supported Iraq in its effort to seclude the FISA.
rather than the state as a whole. Invasions, or even air strikes, are blunt instruments in this respect. Of course, if the attacks are serious enough, these military actions may sometimes be a necessary mode of response, as Israel has found in response to the continuing terror attacks directed against it.

Economic sanctions have much the same problem. They are a blunt instrument whose costs are generally externalized on the population by the regime elite responsible for the campaign of terror, they also shoot the democracies in the foot that the existing trade to be interrupted was in being precisely because it was win/win for both parties. In addition, they must be agreed by all of the principal trading partners unless they are to be hollow actions simply displacing the profitable trading of the democracies themselves as other states fill the vacuum they have left. For these reasons it is frequently difficult to put together an effective campaign of economic sanctions. Again, this is not to argue against such sanctions in extreme cases, as, for example, in the effort to prevent Iran from obtaining nuclear weapons.

Criminal sanctions may apply to regime elites responsible, as well as those implementing the acts of terror, but they too have significant limitations. First, unlike the clear criminalization of waging aggressive war and committing grave breaches of the laws of war as were declared criminal under the original Nuremberg standard, it is less clear that regime elites ordering terrorism may always be covered. More importantly, it is extremely rare to catch any of the high-level elite ordering these actions in a setting permitting criminal trials. Rather, the usual subjects of anti-terror criminal actions are the low level terror "mules" carrying out the bombings or kidnappings. Because such sanctions at least theoretically include regime elites we should seek to enhance the effectiveness of this strand in the war on terror, particularly as it applies to regime elites ordering acts of terror. But this strand at present offers only limited deterrence.

And, of course, neither military action, nor economic sanctions, nor criminal trials compensate the victims of terror, who surely also deserve our attention. One of the more remarkable elements in the persistence of the absolute theory of immunity against knowing actions of terror states has been to ignore the legal rights to compensation of those injured by these actions. It is an ordinary and usual application of the rule of law that those harmed by the intentional wrongful acts of others should receive compensation from the wrongdoers. This not only deters future wrongful acts but seeks to provide at least some justice for the innocent injured party. Their injury and resultant plight in terror cases is frequently horrific. To ignore compensation for them is itself inconsistent with the rule of law. Moreover, even if it were necessary to take their rights against those who injured them for compelling foreign policy purposes, elemental fairness, as well as the Fifth Amendment to the United States Constitution, would require the payment of compensation for the taking of the claim against the foreign state for this public purpose. Sadly, all too frequently the Executive seems to have little concern for such compensation in its zeal to support the absolute theory of immunity.

In contrast to these conventional responses to terrorism, focused civil actions directed against the purveyors of terror, including setting aside the old thinking "the King can do no wrong," and holding the state and the regime- elites accountable, offer substantial advantages which have been largely overlooked. First, they provide focus on the regime-elites and their individual assets hidden around the world, as well as on the state itself which is controlled by these totalitarian leaders. As such, they place deterrence more squarely and precisely on those responsible than all approaches but the criminal approach. And unlike the criminal approach they provide abundant opportunity to be carried out against the regime-elites and their assets. For totalitarian leaders and states typically do interact economically with the democracies. Thus, they frequently store their assets in bank accounts abroad (sometimes out of fear that they might

26. It should also be noted in this connection that change of government, within the United States or in any other nation in the world, does not alter the debts and liabilities of the nation itself. This is the official position of the United States and is settled international law. Any other position would throw financial markets into turmoil and inhibit assistance to developing countries. Moreover, with respect even to an "innocent" new government why should the new government be favored over the innocent and injured victims of state action?

27. The Fifth Amendment to the Constitution of the United States provides that "[n]or shall private property be taken for public use without just compensation." In his concurring opinion in *Dames & Moore v. Reagan*, 453 U.S. 654, 690 (1981), Justice Lewis Powell summarized the Supreme Court's view on the taking of judicially cognizable claims against foreign nations for public policy reasons as a setting in which the parties may file a "takings" claim in the Court of Federal Claims. Thus, he writes: "The Court holds that parties whose valid claims are not adjudicated or not fully paid may bring a 'taking' claim against the United States in the Court of Claims, the jurisdiction of which this Court acknowledges. The Government must pay just compensation when it furthers the Nation's foreign policy goals by using as 'bargaining chips' claims lawfully held by a relatively few persons and subject to the jurisdiction of our courts. The extraordinary powers of the President and Congress upon which our decision rests cannot, in the circumstances of this case, displace the Just Compensation Clause of the Constitution." See also the famous "French Spoliation" case, *Gray v. U.S.*, 21 Ct. Cl. 340, 392–93 (1886) ("the citizen whose property is thus sacrificed for the safety and welfare of his country ... has a right to compensation.

have to leave the country quickly or simply to hide their assets), and their state enterprises must engage in activities in other nations, making them vulnerable to large judgments. Further, fair trials provide the evidence and build the record of their complicity prior to any sanction, and the resulting judgments both deter and provide compensation for the victims of terror. Nor is there anything new or remarkable about applying the civil justice system against assault, battery and intentional infliction of emotional distress, standard torts in the legal systems of the democracies. The remarkable fact is that we have given immunity to those who carry out such acts rather than applying the quite ordinary rule of law to their actions. Importantly also, large civil judgments effectively enforced against terror states directly reduce their ability to support terror. This may be particularly true in drying up their ability to support terror abroad by pressuring their dollar, yen and euro denominated assets. Finally, normal application of the rule of law against terror states through fair trials in our courts is likely to receive broad general support from the populations of democracies, unlike the likely far greater difficulty in sustaining support for military actions and even economic sanctions. In addition, such civil judgments are likely to generate less opposition from third states, which, at least if such judgments are limited to proven settings of actions in violation of United Nations terror conventions, should have broad international support.

We also have good reason to believe that large civil judgments can make a difference in the struggle for peace and human rights. Within the United States a pattern of determined civil actions brought by the Southern Poverty Law Center largely put the Ku Klux Klan out of business as a purveyor of terror in America. We also saw how effective the seizure of a small sum of bank assets was in dealing with the rogue actions of North Korea. In the case of Iran, it was so aware of the potential for large civil judgments against it when it had earlier illegally seized United States Embassy personnel that it insisted in the Algiers Accord, which obtained their release, that it be protected against civil suits from its illegal seizure. Surely the recent decision of Judge Royce Lambo-erth holding Iran liable for more than $2.6 billion in its complicity in the 1983 Marine Barracks bombing in Beirut Lebanon which killed 241 American servicemen will be noticed by Iran. This is precisely the kind of large, but fair, judgment which can dramatically turn the tide against knowing involvement of states in the terror business.

Of particular importance in this connection, not only do the democracies have huge military superiority against the terror states, but they also have huge financial superiority. It is the banks and financial markets of America, Japan and the European Union which dominate global finance. A concerted effort at direct financial pressure, through cooperative enforcement of judgments against terror states, can have a devastating impact on the purveyors of terror. Indeed, we already have in place such cooperation against non-governmental terror groups such as Al-Qaida. Why should such cooperation not be extended to the reciprocal enforcement of large anti-terror judgments against terror states? Looking specifically at Iran as a purveyor of terror in the world today, Iran cannot in the slightest compete with democratic nation control of global financial markets and resources.

The Fallacy of Traditional Objections

"Equal and exact justice to all men, of whatever state or persuasion...."
Thomas Jefferson,
First Inaugural Address, March 4, 1801

There are a variety of traditional objections to application of the civil justice system to terror states. The principal such objections are that America or American officials would become vulnerable to lawsuits in the courts of terror states, that such trials against foreign governments would not be fair to them, that such actions would interfere with foreign relations, and that there is no agreement about terrorism; that is "one man's terrorist is another man's freedom fighter." While these objections sound plausible, in reality they are greatly exaggerated and do a disservice to the rule of law.

First, let us examine more closely the objection that America or American officials would become vulnerable to lawsuits in the courts of terror states. To begin, why is this objection not also applicable to virtually any response against terror states, including military action, economic sanctions and even crim-

nal trials? When another nation commits to a pattern of terror attacks against us we are, by no action of our own, in a deadly serious struggle with them. Unless we are to do nothing, which surely should be unacceptable, it is to be expected that the aggressor will fight using whatever tools they have decided will be most effective. But in this case they have already decided to attack us with suicide bombers, kidnappings, torture and terror. The prospect of their bringing civil actions in their courts harbors little additional concern over their actions already seeking directly to kidnap or kill us. In addition, the resulting setting is one in which Americans likely have long since pulled back from residence and business in the terror state, and thus likely we have only limited asset exposure. But in sharp contrast the terror state cannot as readily cut its financial ties with the dominant economic superpowers. Moreover, unless America is itself engaging in terror such trials will simply be sham trials and will be internationally understood as such. Surely, if we believe in the rule of law, including the civil justice system as a core component of the rule of law, the age-old reality that totalitarian nations may simply use the law to do their bidding should not cause us to abandon the rule of law. This first concern does suggest, however, that we should be careful to limit such actions to those broadly understood internationally as constituting terrorism and which will only be effectuated with due process of law.

In connection with this first objection we should remember that it is no longer new to subject foreign states to suits in domestic courts. That, after all, was the very purpose of the Foreign Sovereign Immunities Act when enacted in 1976. Further, the FSIA, carrying out that purpose, has now been copied by many nations around the world. No longer is it generally accepted as a principal of international law that “the King can do no wrong.” Thus the real question becomes why should terrorist actions, by states we know to be committed to carrying out a pattern of such actions, and which are in violation of widely accepted international conventions against torture, bombing and terror, be exempted from the rule of law? Moreover, with respect to criminal actions it is now accepted by every nation in the world, in the 1949 Geneva Conventions, that there is a universal obligation to seek out and criminally try before your national courts those who engage in “grave breaches” of the Geneva Conventions, including the torture of POWs or the intentional killing of non-combatants in settings covered by the Conventions. Again, if we accept universal criminal liability before national courts of every nation in the world for similar actions why should we not encourage civil liability in national courts in such settings?

With respect to the second objection, actions against foreign states, even terror states, should be carried out only with due process of law. Such actions do have foreign policy consequences and should be carefully cabled to provide fairness. Such fairness is in part also an answer to any effort by the terror states to respond with sham trials. Fortunately, the 1605(a)(7) actions, as supported by the Congress, have been established with scrupulous fairness for the foreign nations. That is the model we should follow, and encourage others to follow.

Principles of fairness in these cases include the following, as mandated in the current law of 1605(a)(7) actions against terror states. First, these actions are limited to those states on the State Department terror list—a dubious achievement of the terror state reflecting a serious commitment to terror. Second, these actions are limited to a small category of actions, each of which is labeled as internationally illegal by a widely adhered United Nations or other international convention, including “torture, extrajudicial killing, aircraft sabotage...[and] hostage taking.” Third, they can be brought only after an elaborate procedure for service of process designed to produce full notice of the action and its nature, and even to translate this into the language of the country in question. Fourth, they can be brought only by nationals of the United States or members of its armed forces or contractors in order to avoid the use of United States courts as a litigating repository for all acts of terror against anyone. Fifth, before any such action can be filed in Federal District Court the foreign state must first be offered “a reasonable opportunity to arbitrate the claim in accordance with accepted international rules of arbitration.” Jury trial is not available against the foreign state in Federal District Court and such trials will be held only before a federal district judge, thus avoiding the emotionalism which might be expected in such cases from a jury. And finally, “[n]o

30. See, for example, Article 129 of the 1949 Third Geneva Convention (the POW Convention) which provides in clause 2: “Each High Contracting Party shall be under the obligation to search for persons alleged to have committed, or to have ordered to be committed, such grave breaches, and shall bring such persons, regardless of their nationality, before its own courts.”
32. Section 1605(a)(7), supra note 9.
33. Section 1608, supra note 9. This language requirement is taken sufficiently seriously as to even generate debate about whether a translation into Latin in an action against the Vatican is a sufficiently good translation into Latin as to provide fair notice, when obviously Latin has not really been “spoken” in the Vatican for years and the translated English was easily understood!
34. Section 1605(a)(7), supra note 9, as modified by the new 28 U.S.C. §1605A(c) of the "Lautenberg Amendment" to the 2008 Defense Authorization Act.
35. Section 1605(a)(7)(B), supra note 9.
judgment by default shall be entered by a court of the United States or of a State against a foreign state, a political subdivision thereof, or an agency or instrumentality of a foreign state, unless the claimant establishes his claim or right to relief by evidence satisfactory to the court.\textsuperscript{36} This last provision ensures that there can be no default judgment absent a written finding as to the facts and the law by a federal district judge. It also ensures that actions in our national courts against foreign states will provide no less in fairness guarantees than those brought against the United States itself.

Foreign governments today have access to a range of top law firms throughout the United States, and, indeed, throughout the world. They have the resources to hire the best attorneys and barristers in the world. Increasingly, in these cases the foreign governments are seeking and obtaining top counsel. Certainly if the terror states have every option to fairly litigate in our courts on terms no less favorable than that accorded to our own government one should not feel that they have been treated unfairly.

The third principal objection to the use of civil judgments against terror states is that such judgments would interfere with our foreign relations. But this objection fails to notice that it was the State Department itself, in the original FSIA, which determined that it was in the interest of our foreign relations to remove the State Department from the business of passing on exceptions to immunity. Thus, FSIA has for over a quarter century permitted the judiciary to make these determinations of immunity under a statutory framework. The only question is whether we should remove immunity from the actions of foreign states who knowingly engage in efforts to kill, torture, kidnap, bomb, or otherwise engage in terror acts against Americans, rather than simply those who break contracts with Americans or run over them in Washington D.C. with an embassy vehicle. Moreover, under current law such anti-terror actions can only be brought following a determination by the Department of State placing the state in question on its list of terror states. It is not easy to get on that list. And if a state is on that list the United States quite obviously has a strong, indeed overwhelmingly strong, national interest in deterring further terror from that state. Surely a practice of the United States will strongly effectuate that national interest which makes it clear that if a state already on the State Department terror list commits any of these terror acts against Americans there will be no second guessing or possibility of pressuring the State Department to excuse the actions, but rather that the state will be held accountable in a fair trial with the potential for a large adverse judgment. Indeed, the implication of saying that these actions may interfere with our foreign policy simply means that the State Department should be free to give them a pass for their killing or torturing of Americans, even following the clear warning to the responsible state of being placed on the terror list. That does not sound like an effective way to enhance deterrence against terrorism. Nor does it sound like a way to clearly establish that some state actions, terrorism as well as torture and genocide, are not acceptable. Simply put, some actions directed against our citizens and against world peace are so serious that we should insist on full application of the rule of law. No state has a justifiable expectation that it will be held immune for such acts.\textsuperscript{37} Further, is not the very purpose of the State Department terror list to deter systematic state terror by attaching consequences to being placed on the list? Civil liability as one such consequence will strengthen the deterrent effect of the list itself. Will the United States get push-back from a vigorous policy of holding terror states accountable? Of course; the more effective the accountability the more strident the likely push-back. But will that be any less true of other actions to effectively seek to deter terror? Should we perhaps be more worried about the actions we take to deter terror which produce no or only little push-back?

It should also be noted, with respect to this “interference with foreign relations objection,” that recognized governments can always bring suit in national courts. But if civil actions in national courts are an anathema to foreign relations why do we permit states to sue in our courts? Is it not hypocritical to freely permit states to sue while the state, in turn, is immune from such suits? A spectacular example of this occurred in recent civil litigation concerning Iraq when Prime Minister Nouri Kamel al-Maliki persuaded George W. Bush to veto the 2008 Defense Authorization Act to prevent applicability of U.S. law to Iraq in long-standing cases against Iraq in U.S. courts. But after seeking to erase the cases against it in U.S. courts, in June 2008, Iraq then filed an action in the Southern District of New York against 93 corporations seeking approximately $2 billion in damages under U.S. treble damage laws.\textsuperscript{38} As with Iraq

\textsuperscript{36} Section 1608(e), supra note 9.

\textsuperscript{37} In a famous dissent in the sovereign immunity case of Hugo Prince v. Federal Republic of Germany, 26 F.3d 1166, 1179–83 (D.C. Cir. 1994), Judge Patricia Wald wrote: “the operative question, then, is whether the executive branch would have recommended immunity for perpetrators of the Holocaust. The intuitive answer is no. In the mid-1940s, Germany could not, even in its wildest dreams, have expected the executive branch of the United States... to suggest immunity for its enslavement and confinement (in three concentration camps) of an American during the Holocaust... [and] Germany could not have helped but realize that it might one day be held accountable for its heinous acts by another state.”

in this case, states would, of course, like to be able to sue without, in turn, being subject to suit. But does such an arrangement promote compliance with law? Does it provide the elemental fairness essential to the rule of law?

There is an easy answer to the final objection; despite the truth in this objection that there is not complete agreement internationally as to what is "terrorism." The easy answer is that such civil actions in the national courts of states can easily be limited to those actions broadly accepted as internationally illegal. For this purpose the core of anti-terror actions might be rooted in substantive violations of the United Nations Conventions against terrorism to which the state is a party and for which the specified act has already been internationally agreed through the applicable convention to be a crime. Other possibilities include the widely accepted Convention against Torture and the Genocide Convention.39 There is no reason that states which support acts of terror broadly accepted internationally as illegal terror, and thereby even made criminal by an overwhelming consensus of the international community, should be exempt from civil suits for their intentional acts of terror or their knowing material support for such acts.

One interesting paradox, as noted above, is that nations have broadly accepted principles of international law generating personal criminal responsibility for violating certain conflict management norms. For example, the 1949 Geneva Conventions, including the POW Convention, which are universally in force, create an obligation on every nation throughout the world to search out and try before their national courts those held accountable for grave breaches of the Conventions. Yet, as the case study below illustrates, at least the United States has been far slower to embrace civil liability for the same actions, even though the POW Convention declares that no state may "absolve" a torturing state of "any liability" for the torture of POWs, a designated "grave breach" of the Convention. And this is despite the fact that it is quite simple for nations to protect their government officials from substantial civil judgments with which they disagree, simply by adopting laws which reimburse civil damages for authorized governmental action, or which, before their own courts, simply transform certain actions against governmental officials into actions against the state itself as the United States has done.40 In sharp contrast, this obviously cannot be done for personal criminal liability, yet which we already have accepted as a basis for national action in enforcing many basic provisions of the law of war, including "grave breaches" of the 1949 Geneva Conventions.41

There is also a purely legal objection to civil litigation against terrorist actions of terror states. It is argued that such actions go beyond permissible limits of non-immunity under international law.42 Never mind that the sovereign's support for terrorism in question is in blatant violation of international law. And never mind that even heads of state have personal criminal liability for such actions. This argument still stubbornly asserts that it is illegal to sue the sovereign in domestic courts for terror actions. No doubt many foreign offices, eager to retain maximum immunity, support this view. But leadership for the rule of law must start somewhere. And thoroughly bad law, were this assertion correct, begs for change.

In any event, under the foreign relations law of the United States, national law will trump international law if the legislative intent is clear. Moreover, surely a widely adhered protocol to the United Nations anti-terror conventions, as suggested here, would be a powerful tool for change and clearly not a violation of international law. But even applying ordinary principles of international law, national judicial actions against actions widely understood as illegal terror acts constitute a classic setting for lawful non-forceful reprisal which would thus make the actions lawful whatever the immunity rule. For such actions are announced to be in response to the prior illegal terror attacks, are quintessentially proportional, submit to third party dispute settlement (even initially offering international arbitration), and end when the terror attacks end. They thus meet all of the requirements for lawful reprisal, a core enforcement mechanism in international law.43 Most importantly, if we are se-

---

39. Yet another parallel in a setting of broad international consensus would be the commission of "grave breaches" of the laws of war as specified in the 1949 Geneva Conventions. At minimum actions by terror states in torturing prisoners of war should be actionable in national courts, particularly since Article 131 of the POW Convention contemplates as one of the core deterrent mechanisms against such torture that no state party to the Convention may "absolve" a torturing state of "any liability" for the torture of POWs.


41. The current disconnect within the democracies as to application of criminal standards against government officials, illustrated by actions in Belgium, German and Spanish national courts, for example, suggests that this is an area in which the United States should take the lead in working out a comprehensive treaty to more effectively resolve the full range of associated issues concerning these criminal proceedings in national courts without losing the proper core of criminal accountability for grave breaches of the laws of war. The parallel here, of course, is also to the range of issues associated with the International Criminal Court and the challenge of an effective United States policy toward that Court.

42. See, e.g., Ronald J. Bettman, "The Foreign Sovereign Immunities Act's Anti-Terrorism Exception and International Law," presented at the 22nd Sokol Colloquium on Human Rights Litigation in U.S. Court, University of Virginia School of Law (April 2, 2009).

riously to seek to enforce international law against terrorism it is a travesty to seek to invoke international law for its protection.

Please Note: The remainder of Page 220 through the first two lines of Page 228 have been intentionally omitted.
Empowering the Rule of Law in the Fight for the Fourth Freedom

"The best test of truth is the power of the thought to get itself accepted in the competition of the market"

Oliver Wendell Holmes, Jr., Abrams v. United States, 250 U.S. 616, 630 (1919)

The revolution in empowering civil litigation as a crucial tool in the fight against terror has already begun. It began in earnest with the passage by Congress of the 1996 Amendments to the Foreign Sovereign Immunities Act which permitted the bringing of 1605(a)(7) actions in United States courts. Congress has reaffirmed and strengthened its leadership in this regard in the recent "Lautenberg Amendments" to the 2008 Defense Authorization Act despite continuing opposition from the Executive and past sniping from the Court of Appeals for the District of Columbia Circuit. Whatever the continuation of short-term "old thinking" in the Executive in opposition to such civil suits, the application of the rule of law against terror states is here to stay and will likely only get stronger. As Stephen R. Perles, who has been one of the principal innovators in this area of the law, summarizes the current U.S. national law permitting suits against terror states:

There has been a dramatic evolution in anti-terrorism civil litigation since the filing of the first successful case for the state sponsorship of terrorism against US citizens in 1996. We have seen the field of anti-terrorism litigation grow from a handful of cases against states like Iran to a flood of cases against states and recently a diversification into cases against foundations and financial institutions charged with aiding and abetting acts of terrorism. On January 28, 2008 Congress modernized the Foreign Sovereign Immunities Act's ("FSIA") terrorism exception with the passage of the National Defense Authorization Act for Fiscal Year 2008....

Today, U.S. victims of international terrorism have a robust legal right against the terrorists that attack them, their state sponsors, and private individuals or organizations that knowingly support or facilitate terrorism. Despite inconsistent and conflicting signs of support or hostility from the Executive Branch and law enforcement and investigatory officials, the field of anti-terrorism litigation has stabilized and continues to evolve as our understanding of international terrorism increases.

It is strongly in the interest of the United States in the struggle against terror not only for the Executive to support the present 1605(a)(7) actions as created by the Congress, but also to encourage every other democratic nation in the world to adopt a parallel structure in their own FSIA equivalent law. Thus, the United States Executive should take the lead in encouraging these actions as a core tool in the struggle against terror. In addition to not seeking to inhibit these actions while they are in court, but rather assisting them with Executive support where appropriate, the Executive should also take the lead internationally in promoting a protocol on civil liability to the United Nations anti-terrorism conventions. Since these Conventions are now broadly in force for

48. Steven R. Perles, supra note 16 at 1.

most nations of the world it is a simple matter to support a protocol to these Conventions which would apply civil liability in national courts where the Conventions have already authorized criminal liability in national courts. Such a protocol could also put in place a mechanism for reciprocal enforcement of such civil judgments which would greatly multiply the effectiveness of this tool against terror. Since this concept of a supplemental protocol to the terrorism conventions was first suggested in 2004, the 2005 Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation with respect to weapons of mass destruction adds in its Article 5 a provision that "liability under the Convention with respect to a legal entity located in the state parties' territory or organized under its laws] may be criminal, civil, or administrative. And it also adds that "[s]uch liability is incurred without prejudice to the criminal liability of individuals having committed the offenses." As such, the concept of civil liability has now already been accepted for at least one of the United Nations terrorism conventions.51

Set forth below as an annex to this chapter is a first draft of such a convention. As a process for moving forward with this draft the Executive might convene a group of expert attorneys experienced with 1605(a)(7) actions to review the draft, clear any resulting draft through the U.S. interagency process, and then begin discussions with nations around the world with a strong interest in the fight against terror. After the Convention has been revised as necessary to generate strong democratic nation support, particularly among major financial powers, then it should be introduced jointly by a broad coalition within the United Nations for adoption at an early time.52

Annex: A Draft Protocol to the United Nations Anti-Terrorism Conventions

MULTILATERAL
Protocol to the United Nations Conventions on Terrorism to Enhance Compliance Through Application of Civil Damages

The States Parties to this Protocol,
Having in mind the purposes and principles of the Charter of the United Nations concerning the maintenance of international peace and the promotion of friendly relations and co-operation among States,
Considering that acts of terrorism in violation of the United Nations Conventions on Terrorism are a core threat to international peace and security,
Determined to enhance compliance with these Conventions,
Conscious that these Conventions affirm criminal liability for the offenses within their purview;
Conscious that the civil justice system is an important component of the rule of law and in important ways supplements criminal liability,
Conscious that damage awards can provide both deterrence against terrorism and justice for victims of terrorism, and
Convinced that there is an urgent need to enhance compliance with these Conventions against terrorism,
Have agreed as follows:

Article 1. States Parties to this Protocol undertake to provide actions for civil damages under their national law for offenses set forth as criminal within any of the United Nations Conventions on Terrorism to which they are a Party.


Article 3. The action for civil damages for criminal offenses designated as such under any of the United Nations Conventions on Terrorism, as set out in Article 2, shall be applicable against persons, organizations, states, political subdivisions of states, and agencies or instrumentalities of states, as provided in this Protocol.

Article 4. Actions against persons shall be for offenses as set out in the applicable United Nations Convention on Terrorism. Actions against organizations, states, political subdivisions of states, and agencies or instrumentalities of states shall be for intentional participation in offenses, or knowing assistance or material support to any such offense, if such participation, assistance or support is engaged in by an official, employee, or agent of such entity while acting within the scope of his or her office, employment, or agency, and results in personal injury or death.

Article 5. The obligation to provide civil actions under this Protocol applies only to settings in which the claimant or the victim is a national of the providing state.

Article 6. Any such civil action against a foreign state shall, as an alternative, first afford the foreign state a reasonable opportunity to arbitrate the claim in accordance with accepted international rules of arbitration.

Article 7. In any such action against a foreign state the foreign state shall be liable in the same manner and to the same extent as a private individual under like circumstances. The defenses of act of state and sovereign immunity shall not be available. Nor shall failure to appear serve as a defense.

Article 8. Any such action shall accord defendants due process of law and a fair trial, and in the event of a state defendant, or any designated subdivision of a state or agency or instrumentality of a state, a trial shall follow the same procedure as a trial in a civil action against the Government of the providing state itself.

Article 9. Damages in such cases shall be monetary damages only, which may include economic damages, solutainum, and pain and suffering. Such monetary damages may also include punitive damages, provided that national law of the State Party normally permits punitive damages in such circumstances and provided further that no punitive damages may be awarded in an amount greater than compensatory damages.

Article 10. The providing state may optionally provide that actions under this Protocol for acts committed subsequent to entry into force of this Protocol shall have no statute of limitation.

Article 11. States Parties to this Protocol undertake to honor in their national legal systems judgments rendered by other States Parties under actions established consistent with this Protocol provided:

- A judge of the honoring State Party reviews the foreign judgment and determines that the judgment was fair and consistent with due process of law;
- No State Party is required to honor damage awards, such as those for punitive damages, which are inconsistent with its own national law; and
- No attachment or execution shall be permitted against facilities protected by diplomatic or consular immunity, military assets, or assets held by national central banks.

Article 12. States Parties may make reservations to this Protocol for the purpose of ensuring compliance with their national law, including principles of their civil justice system and/or their Constitution.

Article 13. States Parties may, at the time of signature, ratification or accession, announce that they will follow the principles of this Protocol with respect to designated Regional Conventions on Terrorism, as between themselves and other States Parties to such Regional Conventions who undertake reciprocally to accept the obligations of this Protocol with respect to the designated Regional Conventions.

Article 14. This Protocol shall be opened for signature by all States who are Party to any of the United Nations Conventions on Terrorism, until 31 December, 2014, at United Nations Headquarters in New York.

Article 15. This Protocol is subject to ratification by any State which is Party to any of the United Nations Conventions on Terrorism. The instruments of ratification shall be deposited with the Secretary-General of the United Nations.

Article 16. This Protocol shall remain open for accession by any State Party to any of the United Nations Conventions on Terrorism. The instruments of accession shall be deposited with the Secretary-General of the United Nations.

Article 17. 1. This Protocol shall enter into force on the thirtieth day following the date of deposit of the twenty-second instrument of ratification or accession with the Secretary-General of the United Nations.

2. For each State ratifying or acceding to the Protocol after the deposit of the twenty-second instrument of ratification or accession, the Protocol shall enter into force on the thirtieth day after deposit by such State of its instrument of ratification or accession.
ENFORCEMENT PROVISIONS AGAINST SPONSORS OF TERRORISM

Steven R. Perles
sperles@perleslaw.com
Edward B. MacAllister
emacallister@perleslaw.com
Perles Law Firm, PC
1146 19th Street, NW
Suite 500
Washington, DC 20036
202-955-9055

The Foreign Sovereign Immunities Act, as amended in 2008, and the Anti-Terrorism Act provide an exploitable policy lever for the Obama administration as it seeks to deal with threats posed by state sponsors of terror such as Iran and Syria. Supporting private causes of action, which have resulted in the liquidation of Iranian assets hidden in the U.S., by victims of terror is both just and good U.S. government policy.

The dramatic and successful evolution in civil litigation against foreign sovereign sponsors of terrorism since the late 1990s supports the argument that the U.S. government should cooperate with and support victims in their efforts to sue the parties that injured them and to collect any damages awarded. Two major recent successes in the U.S. court-ordered liquidation of Iranian assets in 2013, and the recent verdict in the consolidated Arab Bank cases have confirmed this thesis, but there is further room for cooperation. Today, U.S. victims of international terrorism have robust legal rights in U.S. federal courts against state sponsors of terrorism, after a protracted battle in the

---

1 Perles Law Firm, PC, Washington, DC. An earlier version of this paper served as the foundation of the oral presentation and comments by Mr. Perles at the 2012 Sokol Colloquium on the topic of “Enforcement Provisions of the FSIA” which was published in Foreign Affairs Litigation in United States Courts, John Norton Moore, ed. (Martinus Nijhoff, 2013). Additionally, this contains an update and expansion of a paper written in 2008 by the coauthors and Major Gabriel Lajeunesse of the United States Airforce (whose input did not necessarily reflect the views of the Department of Defense or its components).


4 In the late 1990s, the first successful cases brought by U.S. citizens against state sponsors of terrorism, such as Flotow v. Islamic Republic of Iran, 999 F. Supp. 1 (D.D.C. 1999), Eisenfeld v. Islamic Republic of
courts and Congress as to the scope of those rights. Now that the benefits of such litigation have become clearer, the Executive Branch should cooperate with victims of terrorism to ensure that they are able to collect on their damage awards, which would facilitate U.S. foreign policy goals, such as halting Iranian progress in the development of a WMD program.

The existence of the rights of victims of terrorism has not meant that they have been exercised as effectively as Congress intended. In 1990, Congress passed the Anti-Terrorism Act ("ATA") to allow terror victims to bring civil suits against terrorists and their facilitators. It was enacted in response to the inability of victims of the Pan Am 103 bombing over Lockerbie to sue the Palestinian Liberation Organization because of jurisdictional limitations. However, the ATA did nothing to address the sovereign immunity of state sponsors of terrorism. Congress created a legislative regime in 1996 to allow civil litigators to pursue state sponsors of terrorism by obtaining damages for U.S. victims of terrorism in order to both deter further acts of terrorism and compensate the victims of past acts. Two factors thereafter imperiled the efforts by private civil litigators: structural problems in the statutory regime and insufficient support from the Executive Branch and law enforcement and investigatory officials.

Prior to 1996, the only precedent in U.S. federal courts from cases brought by victims of terrorism seemed to suggest to victims of international terrorism that they should not bother to bring a lawsuit against either foreign states\(^5\) or the terrorist groups\(^6\).

\(^5\) "Although Libya's alleged participation, if true, in this tragedy is outrageous and reprehensible and the human suffering involved is heartbreaking, this Court may not rightly obtain jurisdiction over Libya for the purposes of these private rights of action. Libya's alleged terrorist actions do not fall within the enumerated exceptions to the Foreign Sovereign Immunity Act and therefore Libya must be accorded sovereign..."
that had injured them. The passage of a new “state-sponsored terrorism exception” to foreign sovereign immunity in 1996 spurred the creation of statutes extending subject matter jurisdiction against foreign states that sponsored acts of terrorism against U.S. citizens, as well as non-state actors.\textsuperscript{\textsuperscript{7}} A few harmful court decisions arising out of structural deficiencies in the key statutes, however, created difficulties for the civil litigators seeking to represent U.S. citizens who had suffered death and personal injury as a result of international terrorism. A line of cases brought against the Islamic Republic of Iran, beginning with \textit{Flatow v. Islamic Republic of Iran},\textsuperscript{\textsuperscript{9}} introduced the concept of using civil litigation to win redress against sponsors of international terrorism to a wider audience of attorneys and victims. The hesitation to litigate diminished as several attorneys and firms successfully acquired sufficient information to withstand the rigors of trial in a U.S. federal court and win a judgment against a foreign state sponsor of terrorism. The subsequent difficulties the Flatows experienced in satisfying their judgment exposed the obstacles needing removal before anti-terrorism civil litigation could near its goals of deterrence and compensation.

Despite early obstacles, the field of anti-terrorism litigation has stabilized. An increasingly sophisticated knowledge of international terrorism adds fuel to the cycle of innovation by civil litigators and their successes have encouraged further support from Congress. The hesitation from the Executive Branch does lead one to ask whether these lawsuits complement U.S. foreign policy goals. But the fact that the litigation has

\footnotesize{immunity from suit.” \textit{Smith v. Socialist People’s Libyan Arab Jamahiriya}, 886 F. Supp. 306, 315 (E.D.N.Y. 1995) (rejecting the first lawsuit against Libya for the bombing of Pan Am 103).}

\footnotesize{\textsuperscript{6} “I believe, as did the district court, that, in the circumstances presented here, appellants have failed to state a cause of action sufficient to support jurisdiction under either of the statutes on which they rely.” \textit{Tel-Oren v. Libyan Arab Republic}, 726 F.2d 774, 799 (D.C. Cir. 1984).}

\footnotesize{\textsuperscript{7} 28 U.S.C. § 1605(a)(7).}

\footnotesize{\textsuperscript{8} 18 U.S.C. § 2333.}
continued to achieve notable successes, despite the hesitation of the Executive Branch, warrants recognition of its utility to actors in the U.S. government’s foreign policy apparatus.

Success in both obtaining a judgment and collecting against the foreign sovereign debtor is critical to the effort against state sponsors of terrorism. State sponsors of terrorism ignore these lawsuits unless their assets are vulnerable to the U.S. judgment holders. While legislative reform has greatly aided the ability of civil litigators to secure large judgments in court and to attach the assets of liable state sponsors of terrorism, the cooperation of the Executive Branch is necessary to maximize the impact of anti-terrorism litigation and secure justice for victims of terrorism.

And the Executive Branch cooperation extended in two recent successful outcomes further underlines the efficacy of a public-private partnership. In two different cases—$1.9 billion in Iranian Central Bank assets and a building in downtown Manhattan worth hundreds of millions of dollars—significant Iranian assets situated outside Iran were restrained and will likely be distributed to U.S. victims of Iranian terrorism to compensate them for their injuries.

I. EARLY PROMISES – THE BEGINNING OF ANTI-TERRORISM CIVIL LITIGATION

There was a time when U.S. victims of terrorism had no explicit civil recourse for acts of international terrorism. In 1984, the United States Circuit Court for the District of Columbia Circuit decided Tel-Oren v. Libyan Arab Republic, and victims of horrendous attacks learned that they had no suitable remedy despite identifiable defendants.\textsuperscript{9} On March 11, 1978, thirteen heavily armed members of the Palestine Liberation

Organization landed by boat in Israel and captured two buses and a few carloads of hostages.\textsuperscript{11} They tortured them, shot them, wounded them and murdered them. Before the Israeli police could stop the massacre, 22 adults and 12 children were killed, and 73 adults and 14 children were seriously wounded.\textsuperscript{12}

In a per curiam opinion with three concurring written decisions, the appellate court found that the trial court correctly dismissed the case for lack of subject matter jurisdiction.\textsuperscript{13} The appellate court agreed that there was no jurisdictional basis for the trial court to adjudicate these acts of international terrorism\textsuperscript{14} and the case was dismissed. The claimants who brought the lawsuit originally included the sovereign state supporter of the attack as a defendant, but the trial court ruled that it had no subject matter jurisdiction over the case and those claims were abandoned in the appeal.\textsuperscript{15} The result in this case laid bare the complete inability of U.S. citizens to file civil suits against the terrorists or their supporters who injured them in acts of international terrorism.

Congress resolved this problem by enacting two statutes into law: (1) the first allowed U.S. citizens injured in his or her person, property, or business by reason of an act of international terrorism\textsuperscript{16} to sue to recover damages and (2) the second one allowed U.S. citizens to peel back the sovereign immunity that protected foreign state sponsors of terrorism from lawsuits by private individuals in the United States.\textsuperscript{17}

In 1992, Congress passed \textit{18 U.S.C.} $\S$ 2333, allowing a person "injured in his or her person, property, or business by reason of an act of international terrorism" to sue to

\textsuperscript{10} \textit{Tel-Oren v. Libyan Arab Republic}, 726 F.2d 774 (D.C. Cir. 1984).
\textsuperscript{11} \textit{Id.} at 776.
\textsuperscript{12} \textit{Id.}
\textsuperscript{13} \textit{Id.}
\textsuperscript{14} \textit{Id.} at 795, 796, 798
\textsuperscript{15} \textit{Id.} at 799 n.3.
\textsuperscript{16} \textit{18 U.S.C.} $\S$ 2333

5
recover damages. 18 U.S.C. § 2333 relies upon another statute for the controlling
definition of "international terrorism"—18 U.S.C. § 2331 defines it as "activities that
involve violent acts or acts dangerous to human life that are a violation of the criminal
laws of the United States." Civil litigation against state sponsors of terrorism also
required action by Congress.

Courts in the United States possess subject matter jurisdiction over foreign
sovereigns only to the extent granted by the Foreign Sovereign Immunities Act
(“FSIA”).18 The FSIA therefore “provides the sole basis for obtaining jurisdiction over a
foreign state in the courts of this country.”19 From early on, federal common law
generally provided foreign states with absolute immunity from suit.20 With the rise of
state trading companies in the twentieth century, exceptions emerged under a theory of
“restrictive immunity,” which was formally adopted as United States policy by the
Department of State in the so-called Tate Letter of May 1952.21 Under this theory,
immunity was confined to suits involving the foreign sovereign’s public acts, and did not
extend to cases arising out of a foreign state’s strictly commercial acts.22 Administration
of the restrictive-immunity theory proved problematic. Courts deferred to State
Department recommendations on immunity questions, which forced this executive
agency to assume a judicial function that often conflicted with its primary mission of
conducting American foreign policy: foreign nations frequently pressured the State

18 28 U.S.C. § 1330 (“The district courts shall have original jurisdiction without regard to amount in
controversy of any nonjury civil action against a foreign state as defined in section 1603”).
21 Letter from Jack B. Tate, Acting Legal Advisor, Department of State to Acting Attorney General Philip
B. Perlman (May 19, 1952), reprinted in 26 Department of State Bulletin 984-85 (1952) and in Alfred
Department to recommend immunity, and political considerations sometimes led to recommendations of immunity in cases where immunity would not have been available under the restrictive theory.\textsuperscript{23} The State Department, moreover, did not participate in every case, which left the courts to make their own decisions in that class of cases. As a result, “the governing standards were neither clear nor uniformly applied.”\textsuperscript{24} In 1976, Congress responded to these problems by enacting the Foreign Sovereign Immunities Act, 28 U.S.C. §§1330, 1602-1611, which specified seven exceptions to the general rule of immunity for foreign states (including the “commercial activities exception”), and assigned the interpretation of those exceptions to the courts.\textsuperscript{25} Subsequent amendments added two additional exceptions to the general rule (including the 1996 addition of the “state sponsored terrorism exception”).\textsuperscript{26}

The FSIA provides for immunity, subject to its enumerated exceptions: “a foreign state shall be immune from the jurisdiction of the courts of the United States and of the States except as provided in sections 1605-1607 of this chapter”.\textsuperscript{27} A U.S. citizen cannot file a lawsuit against a foreign state in the United States unless the allegations contained in his or her complaint meet the requirements found within the several enumerated exceptions, listed at 28 U.S.C. § 1605-1607. Hence the result in \textit{Tel-Oren}.

\textsuperscript{22} \textit{Id.} at 487.
\textsuperscript{23} \textit{Id.}
\textsuperscript{24} \textit{Id.} at 488 (citations omitted).
\textsuperscript{25} The originally enacted exceptions to immunity of foreign states from the courts of the United States were waiver, commercial activity, expropriation, gifts in immovable property in the United States, torts occurring within the United States, 28 U.S.C. § 1605(a)(1)-(5), suits in admiralty to enforce maritime liens, 28 U.S.C. § 1605(b), and counterclaims against foreign state plaintiffs, 28 U.S.C. § 1607.
\textsuperscript{26} In 1988, Congress added an exception to immunity for actions to enforce arbitration agreements and awards, 28 U.S.C. § 1605(a)(6). In 1996, Congress added the “state-sponsored terrorism exception” to immunity for actions arising from a foreign state’s acts of torture, extrajudicial killing, hostage-taking, aircraft sabotage or material support for such an act which results in the injury or death of United States nationals. 28 U.S.C. § 1605(a)(7).
\textsuperscript{27} 28 U.S.C. § 1604.
Results such as Tel-Oren and Smith v. Socialist People’s Libyan Arab Jamahiriya, the case brought by victims of the Pan Am 103 bombing, in the Eastern District of New York in 1995, led to the formation of political coalitions that successfully advocated on the behalf of the rights of victims of terrorism. In 1996, as part of the Antiterrorism and Effective Death Penalty Act (“AEDPA”), Congress reacted by amending the FSIA to create a judicial forum for adjudicating the claims of victims of terrorist acts committed by foreign states that the U.S. State Department has designated as state sponsors of terrorism. AEDPA created the “state-sponsored terrorism exception” to the sovereign immunity that is ordinarily enjoyed by foreign states under the FSIA. 28 U.S.C. § 1605(a)(7). Under AEDPA, countries officially designated by the Department of State as terrorist states can be held liable for personal injuries or deaths if the foreign state commits a terrorist act, or provides material support and resources to an individual or entity that commits such an act. Congress next addressed the issue of remedies for plaintiffs in these cases. A provision called “Civil Liability for Acts of State-Sponsored Terrorism” was enacted on September 30, 1996 as part of the 1997 Omnibus Consolidated Appropriations Act. This provision is commonly referred to as the "Flatow Amendment." The Flatow Amendment established the measure of damages available in suits under the “state-sponsored terrorism” provision of the FSIA. After

---

29 Id.
31 The Flatow Amendment was named after the murdered daughter of lead Plaintiff Stephen Flatow whose case resulted in the decision Flatow v. Islamic Republic of Iran, 999 F. Supp. 1 (D.D.C. 1998). 20-year Alisa was riding in a bus that was attacked by a Palestine Islamic Jihad suicide bomber, who drove a van loaded with explosives and shrapnel. Id. at 7. Alisa died shortly after the bombing, from a fatal head wound. Id. at 8.
32 Id. at 12-13. This holding was overruled by the United States Circuit Court of Appeals for the District of Columbia Circuit in Cicippio-Puleo v. Islamic Republic of Iran, which found that the Flatow Amendment only provided a cause of action against officials of a foreign state under certain circumstances. 353 F.3d 1024, 1033 (D.C. Cir. 2004). This holding was overturned by Congress in 2008 by the codification of a
passage of the Flatow Amendment, victims of terrorism moved quickly to take advantage of the new tools provided by Congress to fight back against the sovereign states that injured them. Stephen Flatow filed a wrongful death complaint against the Islamic Republic of Iran ("Iran") and its officials on February 26, 1997, in the United States District Court for the District of Columbia and on March 11, 1998, the district court entered a historic default judgment against Iran in favor of the Flatows in the amount of $247,513,220.33

There have been numerous cases since Flatow that have documented the ties between Iran, Iraq, Syria, the Sudan, and Libya and individual acts of terrorism.

II. FLATOW'S PROMISE BROKEN?

Almost immediately, court decisions that were at odds with the congressional intent behind the Flatow Amendment threatened to radically undermine anti-terrorism civil litigation. The Flatow Amendment was critical to the early development of anti-terrorism civil litigation for two principle reasons: increasing the measure of damages available to victims in order to create deterrence through massive penalties for the proscribed behavior34 and providing a uniform measure of damages by creating a federal cause of action. A foreign sovereign that is supporting acts of terrorism against U.S. citizens is unlikely to pay attention to damage awards against it unless the damages are significant:

The state-sponsored terrorism exception, however, was enacted explicitly with the intent to alter the conduct of foreign states, particularly towards

---

33 999 F. Supp. at 32.
34 Id. at 12-13 ("The brief explanation of the Flatow Amendment's purpose in the House Conference Report explicitly states that it was intended to increase the measure of damages available in suits under 28 U.S.C. § 1605(a)(7).") (citing to H.R. CONF. REP. 863, 104TH CONG., 2ND SESS. 1996, reprinted at 1996 U.S.C.C.A.N. 924).
United States nationals traveling abroad. Congressman Saxton, the Chairman of the House Task Force on Counterterrorism and Unconventional Warfare, was convinced that the only way to accomplish this goal was to impose massive civil liability on foreign state sponsors of terrorism whose conduct results in the death or personal injury of United States citizens. As compensatory damages for wrongful death cannot approach a measure of damages reasonably required for a foreign state to take notice, Congressman Saxton sponsored the Flatow Amendment in order to make the availability of punitive damages indisputable.\(^3\)

Are punitive damages appropriate for these types of cases? Punitive damages are traditionally used to both punish particularly heinous conduct and to deter future wrongdoing.\(^4\) The provision of material support to terrorists who detonate high explosives wrapped with nails and ball bearings on packed buses or in crowded civilian shopping malls would seem to be an act uniquely deserving of an award of punitive damages.\(^5\)

The evidence shows that Syria supported, protected, harbored, and subsidized a terrorist group whose modus operandi was the targeting, brutalization, and murder of American and Iraqi civilians. Premeditated violence against civilian targets is not a legitimate action by any government. Civilized society cannot tolerate states whose partnership with terrorist surrogates, like Zarqawi's terrorist network, is formed for the purpose of achieving political victory through heinous acts of barbarism.\(^6\)

The second purpose behind the codification of a federal cause of action for use in actions against state sponsors of terrorism was equally important. This was to provide a uniform measure of damages for all victims of terrorism irrespective of where the act of


\(^{37}\) See \textit{Cronin v. Islamic Republic of Iran}, 238 F. Supp. 2d 222, 235 (D.D.C. 2002) ("Here, the Court has no difficulty finding that the depraved and uncivilized conduct of the Iranian Ministry of Information and Security constitutes "outrageous" conduct. The defendant organized, trained, and funded Amal, Islamic Amal, and Hizbollah so that the organizations could torture and take individuals like the plaintiff hostage. Under even the most restrictive interpretation of the term, the defendant's actions in this matter are clearly "outrageous" and warrant the imposition of punitive damages.").

terrorism took place or of the place of residence of the victim of terrorism. The alternative in place of a federal cause of action would be dependant upon the choice-of-law analysis conducted by each court, which might lead to widely varying recoveries or, worse, to an unfortunate circumstance where some families might recover but others might not in a single mass tort case due to the vagaries of the law applicable to each family.

The importance of the Flatow Amendment was underscored after the United States Circuit Court for the District of Columbia Circuit issued a ruling that effectively nullified it. 39 Cicippio-Puleo held that the "Flatow Amendment does not authorize a cause of action against foreign states" despite Flatow's holding, the overwhelming weight and uniformity of subsequent authority, 41 and the logic behind these decisions.

The Flatow Amendment is a hollow right unless the state sponsor of terrorism itself can be held liable. Allowing the parents of a murdered U.S. citizen to sue the driver of the truck that detonated a bomb that killed their child does not have any effect or impact upon the calculations of the foreign state that paid for the driver's training, the bomb that incinerated the U.S. citizen, and the funds that sustain the organization that planned and executed the horrific act itself. The policy goals of anti-state sponsored

39 Cicippio-Puleo v. Islamic Republic of Iran, 353 F.3d 1024 (D.C. Cir. 2004).
40 Id. at 1032.
terrorism litigation, as codified by Congress, are to compensate the victims of terrorism and to staunch the flow of money from foreign states to the terrorist organizations that fight proxy wars on behalf of the foreign states. This policy cannot be effectively achieved without a federal cause of action against the state itself, and the subsequent ability to collect money judgments against the terrorists, their organizations, their funders, and the U.S. State Department designated state sponsors of terrorism.

The Cicippio-Puleo ruling created a brake on litigation against state sponsors of terrorism as litigators were not only stripped of the right to seek punitive damages against foreign sovereigns, but the question of what, if any, law would supply any cause of action against a foreign sovereign became paramount. A prime example of the potential for mischief is illustrated by the decision issued in the case brought by the families of the deceased U.S. service personnel murdered in the 1983 bombing of the Marine barracks in Beirut, Lebanon. In 1982, a multi-national peacekeeping force including U.S. and French troops, with the concurrence of the United Nations, deployed to Beirut.\textsuperscript{42} The U.S. troops were from the 24\textsuperscript{th} Marine Amphibious Unit,\textsuperscript{43} which included men and women from all over the country, including non-U.S. nationals. In Peterson \textit{v.} Islamic Republic of Iran, the court found that Iran organized and planned the attack that destroyed the Marine barracks.\textsuperscript{44} The enormously complex question remained of what law to apply to determine damages for nearly one thousand plaintiffs from numerous different states. “In order to ensure that the Court determines the appropriate amount of damages available to

\textsuperscript{42} Peterson \textit{v.} Islamic Republic of Iran, 264 F. Supp. 2d 46, 49 (D.D.C. 2003) (“The rules of engagement issued to the servicemen of the 24th MAU made clear that the servicemen possessed neither combatant nor police powers. In fact, under the rules, the servicemen were ordered not to carry weapons with live rounds in their chambers, and were not authorized to chamber the rounds in their weapons unless (1) they were directly ordered to do so by a commissioned officer or (2) they found themselves in a situation requiring the immediate use of deadly force in self-defense.”).

\textsuperscript{43} \textit{Id.}

\textsuperscript{44} \textit{Id.}
each plaintiff under the law, it must first ensure that each plaintiff has a valid claim under state law.\textsuperscript{45}

Without the ability to utilize the Flatow Amendment, the plaintiffs were forced to resort to whatever other sources of law were available. It is important to remember that 28 U.S.C. § 1605(a)(7) merely prescribed the requirements that a plaintiff's lawsuit must meet before a U.S. court may assert subject matter jurisdiction over the case. 28 U.S.C. § 1606 further provides that "the foreign state shall be liable in the same manner and to the same extent as a private individual under like circumstances . . . ." Thus, once a plaintiff pierces the immunity of a foreign state under 28 U.S.C. § 1605(a)(7), and a court asserts its subject matter jurisdiction, 28 U.S.C. § 1606 defines the sources of law that apply to a foreign sovereign. This allows a plaintiff to assert any applicable cause of action against a non-immune foreign state. Under the FSIA, a foreign sovereign "shall be liable in the same manner and to the same extent as a private individual under like circumstances".\textsuperscript{46}

Once a foreign state's immunity has been lifted under Section 1605 and jurisdiction is found to be proper, Section 1606 provides that "the foreign state shall be liable in the same manner and to the same extent as a private individual under like circumstances." 28 U.S.C. § 1606. Section 1606 acts as a "pass-through" to substantive causes of action against private individuals that may exist in federal, state or international law.\textsuperscript{47}

The Peterson court therefore performed a choice-of-law analysis through an application of the choice-of-law rules of the forum.\textsuperscript{48} The court employed the District of Columbia's "modified government interest analysis" to decide that the law of the plaintiffs' domicile

\textsuperscript{44} Id. at 61.
\textsuperscript{46} 28 U.S.C. § 1606.
\textsuperscript{48} 515 F. Supp. 2d at 38.
at the time of the attack has “the greatest interest in providing redress to its citizens.”

This meant that the law of the domicile of the service person at the time of the attack would provide the applicable law for the wrongful death claims and for the battery claims of the surviving service persons. For the family members with intentional infliction of emotional distress claims, 753 plaintiffs, the court would look to the domicile of the plaintiff at the time of the attack. This led the court to analyze the various laws of:

Alabama, California, Connecticut, District of Columbia, Florida, Georgia, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, and Wisconsin.

Aside from the enormous expenditure of judicial resources, this also resulted in a tragic outcome for those plaintiffs whom happened to have been situated in states that did not allow for recovery for intentional infliction of emotional distress under the factual circumstances of the case. Plaintiffs from Louisiana and Pennsylvania therefore were unable to recover for their damages. Had there been a uniform measure of damages in a federal cause of action, those plaintiffs would have not been left out.

III. FAILED ATTEMPTS TO CAPITALIZE ON 28 U.S.C. § 1605(a)(7)

The tale of the Flatows’ attempts to enforce their judgment against Iran further highlighted the obstacles that continued to hinder litigators and provided a primer for the legislators who would set out to remove those obstacles. Among other Iranian assets

---

49 Id.
50 Id. at 39–40.
51 Id. at 41.
52 Id.
53 Id. at 45.
inside the country, the Flatows targeted the former Iranian embassy and former Iranian embassy officials' residences. The Department of Justice appeared in court to defend the Iranian assets from attachment by arguing that the attachments would impermissibly conflict with the obligations of the United States under the Vienna Convention on Diplomatic Relations, a treaty to which the United States is a signatory. The Department of Justice also defended against the attachment of any funds in the U.S. Treasury owed to Iran or under dispute in litigation between the U.S. government and Iran in other tribunals by arguing that any Iranian funds sitting in U.S. accounts are protected by U.S. sovereign immunity, and the courts agreed.

The asset hunt therefore expanded to include Iranian assets remaining in the United States yet outside U.S. government control. An insuperable obstacle quickly arose: courts began to apply the common law presumption of respect for the corporate form of juridically separate government instrumentalities, enunciated in *First National City Bank v. Banco Para El Comercio Exterior de Cuba*, and known as *Bancet* doctrine. This created an impossible obstacle to the statutory scheme through which Congress had sought to deter state-sponsored terrorism against American citizens.

*First National City Bank* had enunciated an equitable, common law principle under which duly created instrumentalities of a foreign state are ordinarily entitled to a presumption of independent status. *First National City Bank* also made it clear, however,

---

that this presumption must not be used to undermine countervailing congressional policies. "In particular, the Court has consistently refused to where it is interposed to defeat legislative policies."58 Congress enacted both the "state-sponsored terrorism exception" to the FSIA and the Flatow Amendment in order to deter state-sponsored terrorism.59 The "state-sponsored terrorism" exception, however, "was enacted explicitly with the intent to alter the conduct of foreign states, particularly towards United States nationals traveling abroad."60 The Flatow Amendment, in turn, sought to achieve deterrence by increasing the damages available for plaintiffs suing foreign state sponsors of terrorism.61 Congress intended to create massive civil liability for proven state sponsors of terrorism under 28 U.S.C. § 1605(a)(7) as a way of altering their behavior.62

Furthermore, in 1996, when Congress amended 28 U.S.C. § 1605 to include the "state-sponsored terrorism exception" to foreign sovereign immunity, it also amended 28 U.S.C. § 1610 to permit attachment of assets irrespective of the assets’ involvement in the underlying incident that provided the right for attachment.63 These amendments were intended to ease the process of attachment and execution for 28 U.S.C. § 1605(a)(7) judgment creditors. Prior to the amendments, victims of state-sponsored terrorism who obtained judgments under the then-existing provisions of the FSIA could not attach or execute upon the assets owned by the foreign state, unless they could prove the asset sought for execution or attachment was involved in the underlying incident.64

58 Id. at 630 (citing Anderson v. Abbot, 321 U.S. 349, 362-63(1944)).
60 Id.
61 Id. at 12-13.
The harsh limitations this requirement placed upon successful plaintiffs' ability to satisfy their outstanding judgments were illustrated in *Letelier v. Republic of Chile*.65 In *Letelier*, the victims of a bombing and assassination, sponsored by Chile and carried out in the United States, sought to execute upon the Chilean national airline, Linea Aerea Nacional-Chile ("LAN"), to satisfy their default judgment against Chile.66 The court found that the property was not used for the commercial activity upon which the claim was based and denied execution against LAN.67 In doing so, the court made clear the reason for its ruling: "Congress did not provide for execution against a foreign state's property under the circumstances of this case. Congress provided for execution against property used in commercial activity upon which the claim is based."68 The 1996 amendment to 28 U.S.C. § 1610 was to ensure that victims of terrorism with outstanding 28 U.S.C. § 1605(a)(7) judgments did not fall into the *Letelier* trap.

The *Letelier* trap may have been avoided, but was quickly replaced by emergence of the *Bancerc* trap in the Ninth Circuit decision *Flatow v. Islamic Republic of Iran*.69 The Flatows had "obtained a writ of execution for $247,513,220.00 on property in Carlsbad, California, owned by California Land Holding Company" a wholly-owned subsidiary of Bank Saderat Iran,70 an Iranian national bank wholly owned by the state of Iran, as are all banks in Iran since the post-revolution nationalization of banks in 1979. The Ninth Circuit affirmed the decision by the federal court in the Southern District of California by finding that the *Bancerc* doctrine prevented execution against an entity established separate from the state by the state, unless the plaintiff can show that Iran exercises

---

65 748 F.2d 790, 791 (2d Cir. 1984).
66 Id. at 792.
67 Id. at 795-96.
68 Id. at 799.
extensive or “day-to-day control” over Bank Saderat Iran.\textsuperscript{71} “The court found that Flatow had not shown that BSI operates as an arm of the Iranian government or that BSI’s mission is to further the policies of the Iranian government.”\textsuperscript{72} The U.S. government entered a statement of interest and “took the position that the amendments to the FSIA did not alter the Bancee presumption because Bancee and the FSIA govern two separate questions of law: liability and jurisdiction.”\textsuperscript{73}

The mistake of the Ninth Circuit was to formulate a federal common law rule regarding the attribution of liability under the FSIA that defeated the congressional intent behind the anti-terrorism legislation. Congress decided that financial penalties should be exacted upon those foreign states that sponsor acts of terrorism against United States citizens, and Congress deliberately constructed a legislative scheme to fulfill its goal of deterrence. The Ninth Circuit mechanically construed Bancee to block the attachment of assets otherwise available to satisfy outstanding judgments resulting from litigation that Congress had specifically sought to encourage, and thus upset Congress’s carefully crafted scheme.

In applying the Bancee doctrine, the Ninth Circuit adopted a “day-to-day control” test developed by other courts under the rubric of a \textit{different} statutory provision: the FSIA’s “commercial activities exception” to sovereign immunity, 28 U.S.C. § 1605(a)(2). This was a serious mistake because the history and purposes of the two exceptions are quite different. The “day-to-day control” test is completely incongruous when applied to cases arising under the “state-sponsored terrorism exception,” found in

\textsuperscript{69} 308 F.3d 1065 (9th Cir. 2002).
\textsuperscript{70} Id. at 1067.
\textsuperscript{71} Id. at 1072-74.
\textsuperscript{72} Id. at 1072.
28 U.S.C. §1605(a)(7). The Bancec test, which is broadly consistent with analogous rules in American corporate law,\textsuperscript{74} has an obvious appeal in light of the purpose and history of the "commercial activities exception." In establishing a separate corporation to pursue specific commercial activities, a foreign government is making trade-offs similar to those that an American corporation makes when it establishes an independent subsidiary. There being no obvious reason for applying different rules of attribution in these two highly analogous situations, courts have been inclined to treat them alike.

The legislative intent behind 28 U.S.C. § 1605(a)(7), the "state-sponsored terrorism exception," however, is quite different from that underlying 28 U.S.C. § 1605(a)(2), the "commercial activities exception." The difference is illustrated, for example, by the explicit and profound difference between the corresponding provisions for attachment in aid of execution. When the claim is brought under the "state-sponsored terrorism exception," judgment creditors do not have to prove that property sought for attachment in aid of execution was involved in the underlying claim. 28 U.S.C. § 1610(a)(7). This stands in contrast to judgment creditors holding a judgment from a claim under the "commercial activities exception," who are required by statute to prove that the asset sought for attachment in aid of execution was involved in the commercial activity that their underlying claim was based on. 28 U.S.C. § 1610(a)(2).

Whatever justification there is for the "day-to-day control" test under the FSIA's "commercial activities exception," it has no justification whatsoever under the "state-

\textsuperscript{73} Id. at 1071 n.10.

\textsuperscript{74} See, e.g., Hester Int'l Corp. v. Federal Republic of Nigeria, 879 F.2d 170, 177-78 (5th Cir. 1989).
sponsored terrorism exception” that is at issue in the Flatow case. Unlike the “commercial activities exception,” the statutory provision at issue in this case cannot be regarded as a device for facilitating legitimate commercial intercourse among the community of nations. While the “commercial activities” exception represents the codification of the restrictive doctrine of immunity, the “state-sponsored terrorism exception” is not based on the restrictive theory, and instead denies immunity for the indisputably ‘sovereign’ act of waging war or conducting a violent foreign policy. The purpose of the “state-sponsored terrorism exception,” quite unlike that of the “commercial activities exception,” is to penalize foreign states for grossly unacceptable conduct against American citizens.

The U.S. government has now come to view Bank Saderat Iran as a key cog for Iranian support for terrorism. “Stuart Levey, the Treasury’s under-secretary for terrorism and financial intelligence, announced . . . [Bank Saderat Iran] had been blacklisted because ‘this bank, which has approximately 3,400 branch offices, is used by the government of Iran to transfer money to terrorist organisations.’” In any event, time would be required before the advocates for the victims of international terrorism could successfully press for the legislative reforms necessary to address the Bansee doctrine.

The Flatows’ attachment efforts can now be seen as correct in retrospect in another case: Flatow v. Alavi Foundation. In that decision, the Fourth Circuit affirmed a trial court’s quashing of writs of execution against property of the Alavi Foundation in Maryland that Flatow alleged were controlled by Iran. On November 13, 2009, the U.S.

75 We do not necessarily endorse the “day-to-day control” test for all cases arising under the “commercial activities exception.” Our point here is only that the “day-to-day control” test is clearly not appropriate under the “state-sponsored terrorism exception,” whatever its merits may be elsewhere.
government moved to seize an entire sky scraper in New York City as well as properties around the country belonging to two non-profit foundations under civil forfeiture statutes.

The forfeiture action is part of an investigation into the Alavi Foundation, which the government says has sent millions of dollars to Iran's Bank Melli. In March, the US Treasury Department called the bank a key fundraising arm for Iran's nuclear program.\textsuperscript{78}

Utilization of the public-private partnership in 1998 would have prevented years of Iranian money laundering in Maryland subsequent to the quashing of the writs in 1998.

In 2001, Congress passed the Terrorism Risk Insurance Act ("TRIA") in an attempt to clarify the ability of the victims of terrorism to seize frozen assets in the United States.\textsuperscript{79} The law however did not sufficiently address the \textit{Bancec} doctrine. The imposition of the \textit{Bancec} doctrine has no place where foreign governments seek to use the corporate form to protect their assets from victims of acts of terrorism. A legislative solution to the \textit{Bancec} problem and the problem created by the decision in Cicippio-\textit{Puleo} were desperately needed if anti-terrorism litigation was not going to die a premature death.

\section*{IV. FLATOW'S PROMISE UPHELD – NEEDED LEGISLATIVE REFORM}

For advocates representing American victims of international terrorism, 2008 was a year of significant developments. In January 2008, Congress passed the 2008 National Defense Authorization Act ("NDAA"), P.L. 110-181, § 1083,\textsuperscript{80} amending the FSIA to

\begin{footnotesize}
\begin{itemize}
\item [\textsuperscript{77}] \textit{Flatow v. Alavi Found.}, 2000 U.S. App. LEXIS 17753 (4th Cir. July 24, 2000).
\item [\textsuperscript{78}] \textit{Alavi Foundation: Complaint comes at delicate time for US, Iran}, Michael B. Farrell http://www.csmonitor.com/2009/1113/p02s17-usip.html
\item [\textsuperscript{80}] Congress passed the law after providing for Presidential waiver authority to the application of the law to the Government of Iraq following a veto over concerns of how the legislation would affect the fledgling democracy in Iraq.
\end{itemize}
\end{footnotesize}
provide an explicit, private right of action against state sponsors of terrorism.\footnote{P.L. 110-181, § 1083(a)(1), modifying Chapter 97 of Title 28, U.S.C. § 1605A. In 1996, Congress amended the FSIA, 28 U.S.C. §§ 1602 et seq., to allow civil suits by U.S. victims of acts state-sponsored terrorism such as torture, extrajudicial killing, aircraft sabotage, and hostage taking under 28 U.S.C. § 1605(a)(7), which has now been replaced by 28 U.S.C. § 1605A. Congress subsequently created a cause of action via a further amendment against “an official, employee, or agent of a foreign state designated as a state sponsor of terrorism”, which was known as the Flatow Amendment. “Civil Liability for Acts of State-Sponsored Terrorism,” P.L. 104-208, Title I, §101(c) [Title V, § 589] (September 30, 1996), 110 Stat. 3009-172, codified at 28 U.S.C. § 1605 note.} The legislation was designed to address a 2004 opinion issued by the United States Circuit Court of Appeals for the District of Columbia Circuit that held the FSIA provided a cause of action against individual agents in their personal capacity only, rather than against the foreign state itself—forcing claimants to seek remedies under domestic state law, if available.\footnote{Ciccippio-Puleo v. Islamic Republic of Iran, 353 F.3d 1024 (D.C. Cir. 2004).} The 2008 amendment to the FSIA created a federal cause of action that allowed for the recovery of monetary damages to include economic damages, solatium, pain and suffering, and punitive damages; “in any such action, a foreign state shall be vicariously liable for the acts of its officials, employees, or agents.”\footnote{28 U.S.C. § 1605A(c).}

An early application of the amended law was seen on September 26, 2008, when Judge Rosemary M. Collyer, of the U.S. District Court for the District of Columbia, handed down a judgment for over $400 million to the survivors of Jack Armstrong and Jack Hensley, two American contractors who were brutally murdered by Al Qaeda in Iraq (“AQI”) in \textit{Gates v. Syrian Arab Republic}.\footnote{Gates v. Syrian Arab Republic, 580 F. Supp. 2d 53 (D.D.C. 2008).} The judgment was rendered against the Arab Republic of Syria—held liable for the murders via the federal cause of action under the amended FSIA for Syria’s material support to Zarqawi and AQI.\footnote{Id. at 75.} The use of the federal cause of action avoided any problem posed by using different state laws to prescribe the rules for the causes of action or damages in the case. Additionally, the new
federal cause of action allowed the court to award punitive damages for the unusually
heinous nature of the murders at issue.\textsuperscript{86}

The amended FSIA also contains a critical new provision that a judgment may be
enforced against any property “titled in the name of any defendant, or titled in the name
of any entity controlled by any defendant” expanding the scope of liability to state-owned
enterprises.\textsuperscript{87} This remedy of the \textit{Bancee} trap, in cases involving judgments against state
sponsors of terrorism, will make FSIA judgments significantly more threatening to state
sponsors than in prior experience, particularly if the judgments can be registered and
enforced in foreign jurisdictions.

State sponsors of terrorism had been able to use the \textit{Bancee} doctrine to shield
their investments in the United States from U.S. citizens who hold judgments against
them. Congress enacted both the “state-sponsored terrorism exception” to the FSIA and
the Flatow Amendment in order to deter state-sponsored terrorism by financially
penalizing the state sponsors of terrorism. Although dozens of U.S. citizens hold
judgments resulting from litigation brought under these enactments against the
government of Iran for hundreds of millions of dollars, it can avoid collection claims
from victims of terror if it actively invests money in the United States through shell

\textsuperscript{86} \textit{Id.} at 73 (“The medical evidence corroborates the video: each man was alive when his captors began to
saw upon his neck with a sharp-bladed, but relatively short tool. Williams T-2-58; Welch T-2-25. Both
were physically restrained during the ordeal, with handcuffs holding their hands behind their backs, and
ropes binding their ankles. Williams T-2-49-50 & 58; Welch T-2-24 & 32. As the expert testimony made
clear, the ability to sense pain depends upon the brain receiving input from the spinal cord. It was not easy
to sever fully the spinal cords of Mr. Armstrong or Mr. Hensley because of the methods and tools used by
their murderers, as evidenced by the markings on their spinal vertebrae. Williams T-2-60 ("it required
considerable effort and movement and length of time to cut through both the soft tissue and bone"); Welch
T-2-29 ("the blade hit the spinal column in . . . 11 different places"). The cutting began on the right side of
each man's neck and continued, around the back of the neck without severing the spinal cord, until it
reached the left carotid artery; only then did Mr. Armstrong and Mr. Hensley bleed to death and lose
sensation of pain. See Williams T-2-54 ("So consciousness with just one carotid artery [] compromised
would remain for a while."). It was, quite obviously and scientifically, "a very cruel and inhumane method
of causing death." \textit{Id.} at 63."\textsuperscript{87}}
corporations, foreign subsidiaries and other properly layered entities. The Bancerc doctrine allowed these foreign states to invest and litigate in the United States, before the eyes of their victims, even those victims with valid final outstanding judgments against those foreign states. U.S. citizens who have lost loved ones to senseless acts of violence cannot comprehend why the United States would allow Iranian business investment in the United States to be shielded from attachment when Iran has killed and injured hundreds of United States citizens since 1980.

While premised upon international trade concerns, the Bancerc doctrine frustrated Congress’s effort to deter state sponsors of terrorism. Instead, the victims of terrorism are deterred from bringing suits of the type that Congress deliberately sought to encourage. While the Bancerc doctrine is perfectly sensible in the realm of commercial activity and should be invoked to protect legitimate commercial undertakings by foreign governments, trade between the United States and state sponsors of terrorism should not take priority over compensating the victims of terrorism and penalizing the sponsors of terrorism.

V. EXECUTIVE BRANCH COOPERATION FURTHERS U.S. FOREIGN POLICY GOALS

In addition to the expanded relief afforded by the amended FSIA, 2008 saw unprecedented support from the political branches of government in holding Libya accountable for its past support of terrorism. In January 2008, the U.S. District Court for the District of Columbia ruled on behalf of a group of American families under the FSIA, awarding a $6 billion judgment against Libya in connection with the 1989 bombing of

87 28 U.S.C. § 1605(g)(1).
Libya, anxious to reestablish relations with the United States, was unable to make much progress as State Department officials and members of Congress blocked rapprochement until the claims were satisfied. In August, the governments of Libya and the U.S. reached an agreement where Libya agreed to pay the U.S. $1.5 billion in settlement of all outstanding claims. Though many victims were dissatisfied with this result and felt that the U.S. government made a politically expedient settlement at the expense of fair compensation of all victims and survivors of Libyan terrorism, the level of U.S. government participation in the vindication of private causes of action was unique. While it may have been preferable to see more done on behalf of victims, U.S. government support for the Libyan cases was vital to their eventual settlement.

In the past, the Executive Branch has typically taken a dim view of private actions against state sponsors of terrorism under the FSIA; viewing them as interfering with the President’s foreign affairs powers: “undermin[ing] the President’s ability to combat international terrorism and other threats to national security by permitting the wholesale attachment of blocked property, thereby depleting the pool of blocked assets and depriving the U.S. of a source of leverage…” President Clinton’s infamous reversal of policy—on the one hand supporting the creation of the Flatow Amendment, which was

---

89 For background see Families Who Sued Libya See Their Victory Voided U.S. Pact Nullifies $6 Billion Award in ‘89 Bombing Over Africa By Kimberly Kindy Washington Post Staff, Tuesday, December 23, 2008.
initially construed as a cause of action against state supporters of terrorism until the 2004 opinion issued by the United States Circuit Court of Appeals for the District of Columbia Circuit, while later sending the Department of Justice to file briefs on behalf of Iran to protect Iranian assets located in the United States against the efforts of the Flatow family to satisfy their judgment against Iran in U.S. court—provides another example of the kind of political football that can often occur.\footnote{For background see Clinton Shields Iran from U.S. Justice Blocks Restitution to Families of Victims Murdered By State-Sponsored Terrorists, Western Journalism Center, 28 Sep 2000 available online at...}

The resolution of the Libya cases in 2008-10 for its past acts of state sponsorship of terrorism provides an illustration of how advocates for victims of state sponsorship of terrorism can provide ammunition to the State Department in its advancement of U.S. policy and how the two can work together to achieve their goals. The primary cases that drove the agreement with Libya forward were the Lockerbie Pan Am 103 bombing, the LaBelle discotheque bombing case and the UTA Flight 177 bombing. It had been U.S. government policy to bring Libya into the community of law-abiding nations on the condition that its government take the requisite steps towards responsible governance—by giving up their WMD program, ending support to groups of terrorists, accepting liability for past terrorist actions, and increasing diplomatic and commercial ties between our countries. As isolated as Libya was, however, the U.S. Executive Branch had few levers with which to influence their behavior and to finalize the resolution of the cases against Libya.

Despite this lack of leverage, a unique United States private-public partnership succeeded in negotiating the transfer of $1.5 billion in Libyan funds to compensate past victims of Libyan acts of state-sponsored terrorism. The partnership was comprised of
Jim Kreindler and the Perles Law Firm, PC as the legal counsel for two of the largest groups of victims, and Jonathan Schwartz of the State Department, Deputy Legal Advisor for Near Eastern Affairs. This partnership should serve as a model for future reconciliation with other countries currently outside the community of law abiding nations. Such a partnership does not happen often because of the absence of an institutional voice for victims of terrorism at the State Department. One potential solution is to statutorily create an office for terror victims’ assistance, ("LTVA"), based upon LCID—which would deal with providing assistance for U.S. victims of terrorism as LCID provides assistance to U.S. companies with foreign investment disputes.

What is referred to as the “Libya model” worked well because Mr. Schwartz, Mr. Kreindler and Perles Law worked toward the ultimate goal of victim compensation, even in difficult times when the partnership was strained by inherently divergent interests. The creation of the LTVA office would lay the groundwork for the future replication of the successful results of the Libya model. The Libya model worked in this case because Mr. Schwartz took the unusual step of effectively serving as a quasi-institutional voice for victims of Libyan terrorism at the State Department. Irrespective of the establishment of an office such as LTVA, the public-private partnership should be repeated for the benefits of the victims of terrorism and to further U.S. foreign policy interests.

One of the byproducts of the Libya-United States settlement over all past acts of terrorism is the Executive Branch espousing the claims of all plaintiffs in U.S. courts who had filed suit against Libya, thereby putting an end to their litigation efforts in return for varying levels of compensation, which included a possible result of zero compensation for some plaintiffs. It cannot be doubted that the President has the authority to settle

claims or take the lead in foreign affairs. Precedents for the President’s power to enter into agreements with foreign nations to settle monetary claims by U.S. citizens are seen in cases such as *Dames & Moore v. Regan*\(^{94}\) or *United States v. Pink*\(^{95}\). Nonetheless the Executive Branch’s constitutional prerogative over these private causes of action does not automatically mean that it is good policy to exercise the power and trump the private claim. In addition to the moral rationale—doing our very best to make victims of horrific acts of terrorism whole—there is a significant public policy reason for supporting these actions. If state sponsors of terrorism come to realize that there is a cost for their malicious activities, they may reevaluate their policies. Even if private causes of action do not cause an immediate shift in state policy, these lawsuits provide another avenue for attacking the malign influence of state sponsors of terrorism such as Syria and Iran. As recently described by journalist Robin Wright, the U.S. Treasury Department has found that private industry itself provides a significant financial tool against terror.\(^{96}\) If industry is convinced that doing business with a state sponsor poses greater risk than benefit, they will simply stop doing business.

The amended FSIA provides leverage in this arena by providing an expansion of means to recover from foreign state-owned assets and enterprises. The threat of a judgment creditor attaching such properties would make industry wary of doing business with state sponsors of terror, particularly in countries which provide for full faith and credit to foreign civil judgments. While the Libyan desire for rapprochement provided a

\(^{94}\) *Dames & Moore v. Regan*, 453 U.S. 654, 687 (1980) (stating in upholding the Iran-U.S. Settlement that the “fact that the President has provided such [an alternative] forum here means that the claimants are receiving something in return for the suspension of their claims, namely, access to an international tribunal before which they may well recover something on their claims.”).

\(^{95}\) *United States v. Pink*, 315 U.S. 203 (1942) (where the United States was acting pursuant to an Executive Agreement with the former Soviet Union that required it to collect the remaining assets from the New York branch of a Russian insurance company that were allegedly owed to foreign creditors).
unique point of leverage, U.S. officials can still do much to aid in cases with unrepentant state sponsors of terror by simply taking a non-obstructive posture towards civil actions, and allowing private judgment creditors to pressure the state sponsors of terrorism. Further, the U.S. government could help by identifying state-owned assets in the United States and, in conjunction with U.S. allies abroad. These properties are often hidden in a web of front companies that victims would have difficulty identifying.97

Should the Executive Branch follow the Libya model, thereby reversing its trend of resisting the successful resolution of private actions against state sponsors of terrorism, and choose to use these private suits as levers against state sponsors, the FSIA could have an impact in not only compensating victims, but causing state sponsors of terror to recalculate the costs of their behaviors. The Obama administration should seriously consider the value of this potential tool in the continued struggle against violent extremists and the states that support them.

The Obama Administration should consider another example of the benefits that flow from cooperation with advocates for victims of state-sponsored terrorism. As a result of efforts by private claimants, the state sponsor of the Khobar Towers bombing was publicly exposed by trial lawyers after the Saudi government prevented the FBI from investigating the attack. As Louis Freeh detailed in a Wall Street Journal op-ed in July 2006, the United States government decided not to pursue the investigation into the Iranian angle due to prevailing geopolitical considerations. President Clinton was supporting the rise of then Iranian President Khatami, the Iranian reformist in hopes (in

---

97 For example, a high rise in New York City was recently seized by US authorities—owned on paper by the Assa Corporation but which acted on behalf of the Treasury designated terror facilitator, Iran's Bank
retrospect, unfounded) that Khatami could usher in a new era of U.S.-Iranian relations. The Executive Branch is constitutionally privileged to sacrifice private interests in the pursuit of foreign policy and national security objectives of the U.S. Luckily for the Khobar Towers victims and the U.S. government, the FSIA allows for lawsuits against those designated as state sponsors of terrorism. Here, a law firm took the case and pursued it—resulting in a judgment against Iran. This allowed for the public exposure of that regime’s guilt, something the Clinton administration could not investigate or pursue at the time. Nonetheless, because of the FSIA incentives, victims of that horrendous attack and their counsel were able to investigate the attack and expose its perpetrators before the world. The exposure by private litigants allowed the U.S. government to disclaim responsibility in its dialogue with the Iranian government as President Clinton pursued rapprochement.

Many cases have publicized the state sponsors of infamous attacks where the U.S. government was unwilling or unable to devote resources to the investigation, or where geopolitical considerations constrained their overt involvement. One example is seen in a case successfully brought in the District Court for the District of Columbia against Iran for its complicity in the 1983 Marine barracks bombing in Beirut, Lebanon that caused the death of over 240 servicemen, captioned Peterson v. Islamic Republic of Iran. Judge Royce Lamberth authored a May 30, 2003 opinion that adjudged Iran liable based upon the clear and convincing evidence linking Iran to the 1983 attack.98 Subsequently, Judge Lamberth entered a judgment against Iran in excess of $2.6 billion.99

---


This important case exposed Iran’s involvement in the 1983 Beirut attack. While those in intelligence circles were aware of Iran’s complicity, that fact did not reach wider public circulation until the court awarded this judgment. The news was carried on CNN.com and went around the world. The attack happened so long ago that it was almost forgotten, but this is an important terrorist attack to remember for another reason. The Marine barracks bombing inspired Bin Laden to bomb the two U.S. embassies in Africa in 1998. American soldiers are “paper tigers,” Osama bin Laden told ABC News in 1998.\textsuperscript{100} “[T]he Marines fled after two explosions.”\textsuperscript{101} Our withdrawal from Lebanon led Bin Laden to believe that he could blast the United States out of Africa to protect his then home base in the Sudan. And while Bin Laden himself withdrew from the Sudan in the late 1990s, Al Qaeda activity in the horn of Africa remains a top U.S. foreign policy concern.

VI. MISSED OPPORTUNITIES?

In view of these promising developments in anti-terrorism civil litigation, the Executive Branch should increase its cooperation with victims’ enforcement efforts. On September 7, 2007 the plaintiffs in \textit{Peterson v. Iran},\textsuperscript{102} recovered a $2.7 billion judgment against Iran arising out of the Marine Barracks bombing of October 23, 1983. Post-judgment remedies permit the \textit{Peterson} plaintiffs, the judgment creditor, to seize assets of Iran, the judgment debtor, that are in the hands of any third parties. This process is traditionally called a garnishment, in which a third party is obligated to turn over to a U.S. Marshal money or "property" due to the judgment debtor. Various subsets of the

\begin{footnotesize}
\textsuperscript{100} \url{http://www.nytimes.com/1998/08/23/weekinreview/the-world-osama-bin-laden-in-his-own-words.html}
\textsuperscript{101} \textit{Id}. (“We have seen in the last decade the decline of the American Government and the weakness of the American soldier who is ready to wage cold wars and unprepared to fight long wars. This was proven in Beirut when the Marines fled after two explosions.”).
\end{footnotesize}
legal process compel the surrender of the debtor’s property in the third party’s hands, including the service of a writ of execution, a full blown creditor’s suit to enforce the judgment, subpoena of records belonging to third parties to trace the assets of the judgment debtor, and an order compelling a physical appearance before a judge to testify and produce documents. While the Peterson plaintiffs’ judgment originated in the United States District Court for the District of Columbia, this judgment can be registered in any judicial district in the United States.

The Peterson plaintiffs promptly registered their judgments in various other judicial districts in an effort to seize Iranian assets throughout the country. These districts included the Northern District of California and the Northern District of Illinois. In both proceedings, the issue of the extent to which the foreign sovereign itself must be made to submit to discovery by the Peterson plaintiffs for the purpose of enforcing the underlying judgment has been raised. Discovery into the holdings of various third parties holding or transferring Iranian assets would necessarily provide information on one of the most important topics in U.S. national security circles today. Appeals have been entered in both proceedings and in both circuit courts. The U.S. government has filed a statement of interest siding with Iran as a party to the proceeding in the Northern District of Illinois. Additionally, the U.S. government filed a statement of interest siding with the third party in possession of Iranian assets in the Northern District

---

103 The Peterson plaintiffs sought to enforce their judgment against Iran against various third parties holding Iranian assets in the Northern District of California by registering their judgment in that District on March 11, 2008. Peterson v. Islamic Republic of Iran, 08-mc-80030 (JSW), Registration of Foreign Judgment in the amount of $2,656,944,877.00 in favor of plaintiff and against defendant (N.D. Cal. Filed March 11, 2008).
104 The Peterson plaintiffs sought to enforce their judgment against Iran in the Northern District of Illinois by a motion for intervention. Rubin v. Islamic Republic. 03-cv-09370 (BMM), Motion to Intervene by
of California. Despite the gravity of permitting a private party to proceed with broad-based non-jurisdictional discovery, neither FSIA on its face or TRIA prohibits such an endeavor nor has any court banned such practices.

What is well known is that Iran has been using national banks to fund its WMD program through an overseas network of shell companies. In 2006 and 2007 the U.S. Treasury began blacklisting various Iranian state-owned banks and international companies in an attempt to announce these entities’ ties to international terrorism and more importantly to nuclear proliferation and WMD acquisition:

The Department of the Treasury today designated Bank Sepah, a state-owned Iranian financial institution for providing support and services to designated Iranian proliferation firms . . . “Bank Sepah is the financial linchpin of Iran's missile procurement network and has actively assisted Iran's pursuit of missiles capable of carrying weapons of mass destruction,” said Stuart Levey, Treasury's Under Secretary for Terrorism and Financial Intelligence (TFI).

The discovery of information, at issue now in the Peterson plaintiffs’ litigation in Northern District of California and the Northern District of Illinois, could facilitate U.S. government efforts to break up proliferation networks and support for international terrorism. The potential for the serious interruption of financial support for the Iranian weapons and terrorism pipeline is illustrated by the groundbreaking restraint of over $2 billion in Iranian funds at a financial institution in New York City, which is now the subject of an ongoing garnishment action.

---

Deborah Peterson, et al. (N.D. Ill. filed July 7, 2008). The motion to intervene was granted on October 16, 2008.

105 Existent case law supports broad based discovery against an agency or instrumentality of a foreign state. Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468 (9th Cir. 1992).


107 The matter remains under seal and subject to a protective order. Peterson v. Islamic Republic of Iran, CA 01-2094 docket Entry #439 (RCL) (September 30, 2009).
Under the Obama administration, the U.S. Treasury has expanded sanctions against Iran to further cripple Iran’s financial and industrial sectors. The first major step taken by the Obama administration against the Iranian regime went into effect on June 24, 2010 with the creation of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (“CISADA”). CISADA limited Iran’s ability to import refined petroleum and other industrial goods that enable the Islamic Republic’s civil and military industrial capacities. Further sanctions banning U.S. entities from dealing with the National Iranian Tanker Company took effect in July, 2012 along with other restrictions on Iranian crude oil distribution, all contributing to a substantial one-third drop in the exchange value of Iran’s currency against the U.S. dollar in October 2012. The U.S. government estimates that crude oil sales account for roughly half of Iran’s national annual revenue.

In a concerted effort to destabilize Iran’s central banking structure and promote non-proliferation, the National Defense Authorization Act for 2012 gave the first provisions sanctioning the Central Bank of Iran, Bank Markazi, by restricting U.S. entities from doing business with it. In an unprecedented move against the Iranian financial structure, President Obama issued Executive Order 13599 on February 5, 2012, blocking and freezing all assets of the Central Bank of Iran held in the U.S. or by any U.S. citizen. Freezing assets tied to Iran’s Central Bank opens doors for victims of terrorism who have secured judgments against Iran in U.S. courts currently searching for assets to compensate their civil judgments.

Those plaintiffs seeking compensation in judgments against Iran were given momentum on August 10, 2012 when President Obama signed into law Section 502 of the Iran Threat Reduction and Syria Human Rights Act of 2012, part of the newest Iran sanctions, the “Iran Threat Reduction and Syria Human Rights Act of 2012.” Section 502, entitled “Interests in Certain Financial Assets of Iran,” stripped the immunity previously provided under the FSIA from assets of the Central Bank of Iran discovered in U.S. banks. The new provision established that Iranian Central Bank assets discovered in the Peterson case in New York banks “shall be subject to execution or attachment … to satisfy any judgment to the extent of any compensatory damages awarded against Iran.” 112 Securing the funds is still an ongoing legal battle, but Section 502 gives the Peterson plaintiffs a clearer route to securing compensation. The supportive political provisions are certainly useful, but without more comprehensive support from the Obama administration in cases against state sponsors of terrorism, plaintiffs will continue to struggle to compensate their judicial victories.

In perhaps the greatest nod to the success of these lawsuits in advancing the cause of victims of terrorism, a senate and house bill has been advanced by Canadian legislators to largely replicate the U.S. system for lawsuits against state sponsors of terrorism. 113 If the Canadian government agrees with the efficacy of the program advanced by U.S. private advocates for victims of terrorism, then the U.S. government should support these efforts and cooperate with its victims of terrorism in their search for assets to satisfy any outstanding judgments. Only by overcoming the obstacles that have prevented victims from collecting upon their judgments can the anti-terrorism litigation scheme prove its

utility. And only the utilization of the public-private partnership has succeeded thus far in procuring that level of success. The Chief Judge of the District Court for the District of Columbia recently issued an opinion that noted the endemic obstacles that have continuously hobbled victims of terrorism:

Despite the best intentions of Congress and moral statements of support from the Executive Branch, the stark reality is that the plaintiffs in these actions face continuous road blocks and setbacks in what has been an increasingly futile exercise to hold Iran accountable for unspeakable acts of terrorist violence.\textsuperscript{114}

VII. THE USE OF TRIA AS AN ENFORCEMENT TOOL

The Terrorism Risk Insurance Act of 2002 ("TRIA") was adopted as Pub. L. No. 107-297, 116 Stat. 2322 (2002) and is codified at 28 U.S.C. § 1610, Note. Congress enacted TRIA in 2002 as a footnote to 28 U.S.C. § 1610 in order to facilitate the ability of the victims of terrorist attacks to collect upon their judgments. In relevant part, TRIA Section 201(a) provides:

\textit{Notwithstanding any other provision of law . . . in every case in which a person has obtained a judgment against a terrorist party on a claim based upon an act of terrorism, or for which a terrorist party is not immune under section 1605(a)(7) of title 28 United States Code, the blocked assets of that terrorist party (including the blocked assets of any agency or instrumentality of that terrorist party) shall be subject to execution or attachment in aid of execution in order to satisfy such judgment to the extent of any compensatory damages for which such terrorist party has been adjudged liable.}

TRIA § 201(a) (emphasis added). Thus, to execute upon the blocked assets of a "terrorist party", a plaintiff must establish the following facts: (1) they have obtained judgments for compensatory damages; (2) against a "terrorist party"; (3) on a claim based upon an "act of terrorism, or for which a terrorist party is not immune under"; and (4) the blocked

\textsuperscript{113} Victor Comras, \textit{A Bulwark Against Terror}, National Post, editorial (September 11, 2009).
\textsuperscript{114} \textit{In re Islamic Republic of Iran Terrorism Litig.}, 659 F. Supp. 2d 31, 35-36 (D.D.C. 2009).
assets are "the blocked assets of" a "terrorist party" or "the blocked assets of any agency or instrumentality of" a "terrorist party." Conflicting approaches in the statutory interpretation of the provisions of TRIA in the Second Circuit has illustrated how courts evaluate the different policy considerations implicated by the utilization of TRIA.

The Second Circuit will hear the appeals in Hausler v. JPMorgan Chase Bank, 845 F. Supp. 2d 553 (S.D.N.Y. 2012) and Calderon-Cardona v. JPMorgan Chase Bank, 2011 WL 6155987 (S.D.N.Y. Dec. 7, 2011) jointly. The analysis of the TRIA in each line of cases differs in three key areas: (1) the statutory construction of the phrase "blocked assets of the terrorist party," (2) the underlying policy rationales that inform the interpretation, (3) whether TRIA preempts state law regarding ownership of property/assets.

The key distinctions between the opinions focus on the statutory interpretation of the phrase "blocked assets of that terrorist party." The Hausler line reads TRIA in conjunction with the appropriate regulatory scheme to comprehensively define which blocked assets can be attached and therefore preempt state property law. This approach is more victim-focused and emphasizes that the purpose of the statute is to provide comprehensive compensation for victims of terrorism. Furthermore, it asserts that using state law could lead to inconsistent judgments where some states allow the attachment of certain types of property while other states do not. The Calderon-Cardona approach breaks the phrase into two components and finds that TRIA does not define ownership sufficiently. Consequently, state law must supplement the federal scheme, and the petitioner cannot establish the second component because EFTs are not properly owned.

\[115\] See TRIA § 201(a); see also Weinstein v. Islamic Republic of Iran, 624 F.Supp.2d 272, 274 (E.D.N.Y. 2009), aff'd, 609 F.3d 43 (2d Cir. 2010); Weininger v. Castro, 462 F. Supp. 2d 457, 479
by the state or its instrumentalities under state law. This approach also defers to the
executive and does not want to read TRIA broadly because it may negatively impact the
executive’s ability to negotiate on the international stage.

In *Hausler I*, the court found that TRIA in conjunction with the CACRs
preempted state property law in establishing ownership.\footnote{Id. at 530-31.} The court relied on reading the
two together because the CACRs provided an explicit and broad definition of what
constitutes a property interest or asset.\footnote{Id. at 532-33 (noting that according to the C.F.R. “the term ‘interest’ when used with respect to property
shall mean an interest of any nature whatsoever, direct or indirect.”).} The plain language of the statute indicates that
blocked assets are determined in reference to the CACRs. The court additionally looks to
the legislative history of TRIA which indicates Congress had a broad purpose intended to
“deal comprehensively with the problem of judgments rendered on behalf of victims of
terrorism in any court of competent jurisdiction.”\footnote{Id. at 531 (citing H.R. Conf. Rep. No. 107-779 at 27).} The court construed the definition of
blocked assets very broadly to refer to any asset seized or frozen under the CACRs.\footnote{Id. at 533.} The focus here is on the broad remedial purpose of providing a remedy for victims of terrorism.

*Hausler II* was decided in February 2012, after *Calderon-Cardona* and *Levin*. The
court reaffirmed its original finding that state law was preempted by the definition of
blocked assets in TRIA.\footnote{Id. at 566.} The court distinguished *Calderon-Cardona* saying that the
court incorrectly splits the analysis of the phrase “blocked assets of that terrorist party”
into two pieces: “blocked assets” and “of that terrorist party.” *Id.* The *Hausler II* court
asserts that in reading the phrase as a whole it demonstrates that assets blocked pursuant
to the particular regulation or administrative action directed at the particular terrorist
party are available for attachment.\textsuperscript{121} This limits a party seeking a judgment against Iran
from executing against funds blocked pursuant to the CACRs because those are targeted
at Cuba, not Iran.

The Levin court, following Hausler, asserts that TRIA must be read in context
with the overarching statutory scheme of the FSIA.\textsuperscript{122} Furthermore, the court noted that
in Asia Pulp, the Second Circuit held that Jaldhi instructs that whether or not midstream
EFTs may be attached or seized depends upon the nature and the wording of the statute to
which attachment or seizure is sought, and in this case, TRIA defines which assets are
subject to attachment by reference to regulations pursuant to which the assets are
blocked.\textsuperscript{123} Essentially, Levin and Hausler I and II look at TRIA in the greater context of
regulations against the country. In each case, the states in question were Cuba and Iran,
both state sponsors of terrorism with aggressive statutory regulations in place restricting
trade and imposing sanctions.

Calderon-Cardona, took a different approach, splits the phrase “blocked assets of
that terrorist party” into two components and asserts that the petitioners cannot establish
that North Korea or one of its agencies or instrumentalities actually owns the EFTs in
question.\textsuperscript{124} The court asserts that TRIA does not specifically define property or property
ownership leaving a gap in the law that should be filled by reference to state law.\textsuperscript{125} The
court does acknowledge that the CACRs are functionally equivalent to the NKSRS.\textsuperscript{126}
The NKSRS, in the court’s view, do not properly define ownership leaving “ample room

\textsuperscript{121} Id. at 568.
\textsuperscript{122} Id. at 10.
\textsuperscript{123} Id. at 16-17.
\textsuperscript{124} Id. at 8.
for state law to supplement this federal regime."\textsuperscript{127} The analysis here hangs on the meaning of the word "of" regarding ownership. The court finds that EFTs do not qualify as an asset "of" or belonging to North Korea so they are not attachable.

\textit{Calderon-Cardona} actually decided the case based on the fact that North Korea is no longer declared a state sponsor of terrorism. The court shows deference to the Executive Branch in being able to use TRIA judgments as part of bargaining with a state sponsor of terrorism.\textsuperscript{128} Essentially, executive foreign policy trumps the victims' interest in judgment recovery.

The final decision from the Second Circuit might have an impact on terrorism victims' enforcement efforts in the United States, depending of course on how the opinion is written. Undoubtedly, the loser will seek review at the Supreme Court.

In the meantime, private litigants are using TRIA as an effective enforcement tool. Two recent decisions in the United States District Court for the Southern District of New York have confirmed TRIA's effectiveness. In \textit{Peterson}, the court analyzed whether the following assets were subject to enforcement under TRIA, and related statutes:

Bank Markazi is the Central Bank of Iran, an agency of the Iranian Government. By 2008, Bank Markazi had over $2 billion in bonds (the "Markazi Bonds") denominated in U.S. dollars held in an account with defendant Clearstream S.A. Those bonds have subsequently been split into two groups relevant to this action: first, $1.75 billion in cash proceeds of the bonds are held in an account at Citigroup in New York; these proceeds are subject to restraints imposed by the Court, by Executive Order, and by statute.\textsuperscript{129}

\textsuperscript{125} \textit{Id.} at 9.
\textsuperscript{126} \textit{Id.} at 10.
\textsuperscript{127} \textit{Id.} at 12.
\textsuperscript{128} \textit{Id.} at 6.
On February 23, 2013, the court found that the assets must be turned over to the plaintiffs. In *In re 650 Fifth Ave. & Related Props.*, the U.S. government filed a forfeiture action against two Iranian shell companies with assets in the United States:

In 2008, the United States Government commenced this in rem civil forfeiture action with respect to assets owned by Assa Corporation, an entity incorporated in New York, and its parent, Assa Company, Limited, a corporation domiciled in Jersey, Channel Islands, United Kingdom. The Government seeks forfeiture pursuant to two theories: first, that Claimants have engaged in violations of the International Emergency Economic Powers Act ("IEEPA") and certain Iranian Transaction Regulations ("ITRs") issued by the United States Treasury. The Government asserts that the Defendant Properties are proceeds traceable to such violations are subject to forfeiture under 18 U.S.C. § 981(a)(1)(C) (2009). Second, the Government claims that pursuant to 18 U.S.C. § 981(a)(1)(A), the same assets are separately subject to forfeiture as involved in the promotion and/or concealment of a money laundering transaction or as part of an international money laundering transaction.

The court ruled that the U.S. government proved that the assets belong to Iranian front companies that were shell companies acting on behalf of a Bank Melli, an Iranian state bank, to cover the government of Iran’s role in the use of the assets. Private litigants, using TRIA as their primary tool, have joined with the U.S. government to prove the case and to ensure that the Iranian entities do not overturn the finding on appeal.

**VIII. THE USE OF THE ANTI-TERRORISM ACT TO HOLD BANKS LIABLE AS PRIVATE FACILITATORS OF TERRORISM**

Though TRIA and the terrorism exception to the FSIA have proven powerful tools for the pursuit of civil actions against the state sponsors of terrorism, the cutting edge of private anti-terrorism litigation is occurring against banks not controlled by state sponsors of terrorism, but who launder money for terrorist organization. *Linde v. Arab*

---

131 *Id.* at *11.
Bank is comprised of the consolidated claims of thousands of victims and family members of victims injured or killed in Hamas terrorist attacks in Israel between 1995 and 2004. The Plaintiffs in Linde sued the Arab Bank, PLC (the “Arab Bank”), a Jordan-based international bank, for its role in laundering money for Hamas, the terrorist organization that carried out the attacks. The plaintiffs alleged the Bank knowingly provided direct material support by laundering tens of millions of dollars through its New York branch to U.S. government-designated Foreign Terrorist Organizations (FTOs) such as HAMAS and their agents, including Specially Designated Global Terrorists (SDGTs) and including via “insurance” payments made by Saudi militants to imprisoned and martyred terrorists and their families. This includes individual terrorists (including particular terrorists who committed attacks on the plaintiffs), senior Hamas operatives (including the Hamas “prime minister” in Gaza and the leader of Hamas’ military wing), charitable committees designated as SDGTs for their affiliation with Hamas, and even what the trial judge delineated as evidence of wire transfers to a senior US-designated Hamas leader identifying “Hamas” as the beneficiary, and evidence of multiple payments for families of suicide terrorists (identifying “martyr operations,” i.e., suicide attacks, as the causes of death). These cases raise two interesting issues: 1) the ability of foreign banks to use foreign bank secrecy laws to shield themselves from liability and 2) the development of a more realistic proximate causation standard to hold aiders and abettors of international terrorists responsible for their actions.

The filing of the case prompted the U.S. Office of the Comptroller of the Currency (OCC) to investigate the Bank in 2004, which resulted in a $24 million

---

132 Id. at *65-68, 77-80.
monetary penalty against the Bank, the requirement of establishing a $420 million
reserve, and the shutting down of its U.S. banking business by restricting the New York
branch from any banking activities. The OCC stated in an August 17, 2005 press release:

the agencies determined that the New York Branch of Arab Bank failed to
implement an adequate anti-money laundering program to comply with
the Bank Secrecy Act and manage the risks of money laundering and
terrorist financing in connection with United States dollar clearing
transactions. The New York Branch also violated the suspicious activity
reporting requirements of the Bank Secrecy Act.135

The OCC’s Acting Comptroller later told Congress that its “review disclosed that the
branch had handled hundreds of suspicious wire transfers involving individuals and
entities with the same or similar names as suspected terrorists and terrorist organizations
and that many of these individual and entities were customers of Arab Bank or its
affiliates.” As a result of this review, the OCC issued a cease and desist order,
emphasizing “[t]he inadequacy of the Branch’s Bank Secrecy Act controls over its funds
transfer operations is especially serious in light of the high risk characteristics of many of
the transactions” and ordering conversion of the Bank’s NY branch into an agency with
limited banking powers.

It has been close to a decade since the lead case, Linde v. Arab Bank, was filed
and our clients’ day in court has been delayed for years by Arab Bank’s refusal to
produce the banking records at the heart of the case based on so-called foreign banking
secrecy laws. Most of the evidence remains hidden behind a wall of bank secrecy laws,
primarily those of the Palestinian Authority, in addition to Lebanon and Jordan.136 The

134 Id. at 190.
trial court ruled in 2006 that foreign banking secrecy laws do not apply, but the Bank deliberately ignored multiple production orders. Arab Bank’s refusal to produce these records in violation of US law resulted in the trial court issuing sanctions in 2010 designed to restore a level playing field and to allow the jury to draw certain inferences about the Arab Bank’s conduct, based upon its calculated withholding. The Second Circuit subsequently upheld the trial court’s ruling in 2013. Any defendant in a U.S. civil case must produce the records under its control that go to the heart of a case, and the resulting sanction from the Bank’s refusal to produce was proper.

Notwithstanding the trial court and Second Circuit rulings, the Bank filed a petition for writ of certiorari to the Supreme Court in 2013, and the Kingdom of Jordan submitted an amicus brief in support of the Bank. On October 21, 2014, the Supreme Court invited the U.S. Solicitor General to file a brief expressing the views of the United States. The Supreme Court eventually denied the petition for certiorari.

The courts correctly ruled that foreign bank secrecy laws should not apply in ATA cases, as Congress had already decided between the competing policy goals behind banking secrecy laws and laws. Congress passed the ATA, 18 U.S.C. sec. 2331, et seq., to enable U.S. citizens to sue those who financially support acts of international terrorism. The ATA’s civil remedy plainly contemplates extraterritorial application. Acts of “international terrorism” are defined by the ATA in relevant part as acts that “occur primarily outside the territorial jurisdiction of the United States.” 18 U.S.C. § 2331(1)(C). Senator Grassley, who sponsored the original ATA act, explained that it “empowers victims with all the weapons available in civil litigation, including:

137 Linde v. Arab Bank, PLC, Case No. 4-cv-2799 (NG)(VVP), DE 166 and 272 (E.D.N.Y. Mar, 24, 2006 and Dec. 13, 2006).
Subpoenas for financial records, banking information, and shipping receipts—this bill provides victims with the tools necessary to find terrorists’ assets and seize them.” Given that the law explicitly empowers U.S. citizens to sue those who lend support to acts of international terrorism, the ATA was implicitly crafted to combat the financing of terrorism.

The Executive Branch has agreed. Specifically, in *Boim v. Holy Land Foundation for Relief & Develop.*, the Justice Department advised the Seventh Circuit Court of Appeals that “[t]he provision at issue -- 18 U.S.C. § 2333(a) -- was supported by the Executive Branch as an effective weapon in the battle against international terrorism; when correctly applied, it discourages those who would provide financing that is later used for terrorist attacks.” Thus, the Bank is precisely the type of defendant Congress had in mind when it passed the ATA. Allowing a foreign bank to raise a foreign banking secrecy law, over the denial of the trial court and appellate court, would nullify the ATA and deny Congress’s intent in passing it.

Though the Supreme Courts’ denial of the Arab Bank’s petition for certiorari has currently put to rest the issue of bank secrecy laws and the ATA, the question of what standard of culpability applies ATA bank cases has yet to reach the Second Circuit. The U.S.-national plaintiffs in *Linde* proceeded under the ATA, while the plaintiffs who are foreign citizens proceeded under the Alien Tort Claims Act (“ATS”), 28 U.S.C. § 1350. The ATA is a powerful statute for victims of terrorism in that it provides a private cause of action against individuals or organizations that provide “material

---

140 Id. at 191.
support,” such as financing, to terrorists and provides for treble damages and attorney’s fees. The Linde plaintiffs sued the Arab Bank not as an instrumentality of Jordan, or any other state, nor under the theory that the Arab Bank or Jordan sponsored terrorism. Rather, they argued that the Arab Bank, as a private actor, was civilly liable under 28 U.S.C. § 2333 for its material support of Hamas in violation of 18 U.S.C. §§ 2339A and 2339B, and financing of Hamas in violation of 18 U.S.C. § 2339C.

Specifically, the Linde plaintiffs’ claim that the Arab Bank “materially supported” Hamas rested on two factual theories. First, they alleged that the Bank administered a “death and dismemberment benefit plan” which allowed the Saudi Committee for the Support of the Intifada Al Quds to make cash payments to terrorists and their surviving family members (an incentive for suicide bombers). Second, the Linde plaintiffs alleged that the Arab Bank offered financial services to Hamas, a State Department-designated terrorist organization, such as bank accounts, wire transfers and other movement of funds.

The Arab Bank argued that under the ATA, plaintiffs must show that the “material support” was the “but for” cause of their injuries, that is, the Linde plaintiffs should have to prove that the financial services the Arab Bank provided to Hamas were used directly to perpetrate the terrorist attacks causing their injuries. The district court rejected this argument, finding instead that a “foreseeability” standard applied. Indeed, the jury instructions provide no mention of “but for” causation as an element of liability

---

141 See Boim v. Holy Land Foundation for Relief and Development, 549 F.3d 685, 690-91 (7th Cir. 2008).
143 Linde v. Arab Bank, PLC, Case No. 4-cv-2799 (NG)(VVP), DE 73 (E.D.N.Y. Sep. 2, 2005).
144 Linde v. Arab Bank, PLC, 706 F.3d 92, 97 (2d Cir 2013).
145 Id.
146 Case No. 4-cv-02799 (NG)(VVP), DE 942-1 at 21-22 (E.D.N.Y. May 08, 2013).
147 Id. at 7 (citing the judge’s ruling provided at oral arguments).
under the ATA. Under the heading of “proximate cause,” the court instructs the jury that plaintiffs have met their burden if they prove that their injuries were “reasonably foreseeable or anticipated as natural consequences” of the Arab Bank’s violation of the ATA. As the Ninth Circuit has noted, “[m]oney is fungible; giving support intended to aid an organization’s peaceful activities frees up resources that can be used for terrorist acts.” Accordingly, it makes little sense to require that plaintiffs show that specific funds laundered by a bank were used to fund specific terrorist activities. The jury returned a verdict of “liable” on all counts (24 terrorist attacks between March 28, 2001 and September 24, 2004). The damages hearings have yet to occur.

If upheld, this foreseeability standard will be an important step in holding banks responsible for their knowing facilitation of terrorist activities. Such a standard would make it much more difficult for banks to avoid liability by relying on bank secrecy laws and “willful” obstruction of discovery. This is the first civil verdict against a Bank under the ATA (it is also the first such case to go to trial) and as such could represent the beginning of a new era in civil anti-terrorism litigation.

IX. CONCLUSION

These types of cases significantly increase the cost of sponsorship of terror through punitive and compensatory damages and expose what would otherwise be secret networks for the facilitation of terror and also make doing business more difficult, as financial institutions increasingly scrutinize transactions. These cases may act as a type

---

148 Case No. 6-cv-01623 (BMC)(VVP), DE 923 (E.D.N.Y. Sep. 17, 2014).
149 Id. at 18.
150 Humanitarian Law Project v. Reno, 205 F.3d 1130, 1136 (9th Cir. 2000).
151 Case No. 4-cv-05564 (BMC) (VVP), DE 1182 (Sep. 22, 2014).
of private sanction—forcing corporations doing business with sponsors of terror to think twice if their actions could make them liable in U.S. courts. Recent successes in New York confirm that the Obama administration should expand its cooperation, even if in an unofficial capacity, because these lawsuits further U.S. government foreign policy goals, by creating serious disincentives for the continuity of sponsorship of terror.

Steven R. Perles
sperles@perleslaw.com
Edward B. MacAllister
emacallister@perleslaw.com
Perles Law Firm, PC
1146 19th Street, NW
Suite 500
Washington, DC 20036
202-955-9055

Opinion

What Putin Is Costing Russia

Former finance minister Alexi Kudrin projects up to $160 billion in capital will flee this year.

By Ilan Berman
April 20, 2014 5:24 p.m. ET

THE WALL STREET JOURNAL

Just how much is Vladimir Putin's Ukrainian adventure actually costing Russia? Quite a lot, it turns out.

New statistics from the Central Bank of Russia indicate that almost $51 billion in capital exited the country in the first quarter of 2014. The exodus, says financial website Quartz.com, is largely the result of investor jitters over Russia's intervention in Ukraine and subsequent annexation of Crimea.

As Quartz notes, this was the highest quarterly outflow of capital from the Russian Federation since the fourth quarter of 2008. While Russia can mitigate some of the damage because of its extensive foreign-currency reserves—estimated at more than $400 billion—the new Central Bank statistics signal that worse is still to come.

Russia's economic development ministry has downgraded the country's forecast to less than 1% growth this year; an earlier estimate had been 2.5%. The World Bank projects that the Russian economy could shrink nearly 2% in 2014. That would cost Russia in the neighborhood of $30 billion in lost economic output.

Meanwhile, the Russian government's bid to pressure Ukraine could end up backfiring. The state-controlled natural-gas giant, Gazprom, recently jacked up the price of gas to Ukraine by 80% and levied an $11.4 billion bill on Kiev for previously discounted energy sales. But observers say that the price hike could lead to a reduction in purchases as Kiev diversifies away from Russia toward friendlier European suppliers. This may already be happening. On April 9 the Ukrainian government retaliated by temporarily ceasing purchases of Russian gas, pending resolution of the pricing dispute.

Moscow's international standing is becoming increasingly tenuous. Russia has already been ejected from the G-8 and its path to accession in the Organization for Economic Cooperation and Development has been halted, at least temporarily. In the latest development, the Parliamentary Assembly of the Council of Europe stripped Russia of its voting rights in protest over its interference in Ukraine.

Russia's annexation of Crimea is turning into a costly boondoggle. The Kremlin has already earmarked nearly $7 billion in economic aid for the peninsula this year, funds that will be spent on everything from infrastructure to beefed-up pensions for local residents. Even when balanced against anticipated gains from Crimea's energy resources and savings on
Naval basing arrangements, among other factors, that's a cost Russia's sluggish economy can ill afford.

The situation could become even more dire if Western economic pressure, which is still minimal, is ratcheted up. U.S. Secretary of State John Kerry has threatened additional sanctions against Moscow in response to its instigation of pro-Russian protests in the Ukrainian cities of Kharkiv, Donetsk and Luhansk. Such measures, Mr. Kerry has indicated, could include broad restrictions against Russia's energy, banking and mining. These sanctions could have significant, far-reaching effects on the country's long-term economic fortunes.

President Putin is currently riding a surge of popularity at home, propelled in no small measure by his assertive moves in Ukraine. When tallied in mid-March by state polling group VTsIOM, Mr. Putin's approval stood at nearly 72%, a gain of almost 10 percentage points from earlier in the year.

But the longer the crisis over Ukraine lasts, the higher the economic costs to Russia are likely to be. Former Finance Minister Alexei Kudrin, for example, has projected that Moscow's maneuvers in Ukraine could result in up to $160 billion in capital flight this year, and he concluded that the Russian economy will stagnate as a result.

Sometime in the not too distant future, it might become considerably more difficult for the Kremlin to continue to ignore the real-world price that is associated with its policies.
Putin's Costly Ukraine Policy

- By Ilan Berman
- Mar. 18 2014 00:00
- Last edited 21:52

THE MOSCOW TIMES

There's no question that the Kremlin's policy toward Ukraine is paying concrete dividends, at least in Russia.

On March 7, tens of thousands of people rallied in Moscow's Red Square to support the Kremlin's expanding control over Crimea and formally incorporating the peninsula into the Russian Federation. Russian officials have taken up the call. In her recent meeting with the chairman of Crimea's parliament, Federation Council Speaker Valentina Matviyenko pledged that "if the decision is made, then Crimea will become an absolutely equal subject of the Russian Federation."

But what is less well understood is how much Russia's policy on Ukraine will end up costing the country and its people.

Already, Russia's struggling economy has been hit with major turbulence as a result of the Kremlin's military moves. The fallout has included a plunge in the value of the ruble and a significant decline in the country's MICEX stock index. Meanwhile, market analysts have predicted that capital flight from Russia — already high — will accelerate further, along with a drop in foreign direct investment.

Then there are the sanctions. On March 6, U.S. President Barack Obama signed a preliminary executive order authorizing sanctions against "individuals and entities responsible for activities undermining democratic processes or institutions in Ukraine."

In the aftermath of Sunday's referendum in Crimea, his administration issued another, containing preliminary sanctions on select Ukrainian and Russian officials. Meanwhile, a new bill now under consideration by the Senate would widen the number of individuals and firms in Russia that can be targeted for their role in the Ukraine conflict.

Europe is inching in this direction as well. In recent days, the European Union has agreed to a framework for similar economic sanctions against the Kremlin for its military incursion
into Crimea. In the wake of Sunday’s referendum, these curbs are being enforced, marking the first European sanctions against Russia since the end of the Cold War.

These are restrictions and penalties that Russia’s already-sluggish economy can ill afford. And still more economic pain is in the offing.

Relations between Russia and the West are arguably at their lowest ebb since the Cold War, calling into question Moscow’s long-coveted place in a number of international institutions. For example, the U.S., Britain, Canada, France, Germany, Italy and Japan have announced that they are halting preparations for the upcoming Group of Eight summit in Sochi, unless Moscow reverses course in Crimea. Meanwhile, talks over potential accession to the Organization for Economic Cooperation and Development have been temporarily suspended over Russia’s foray into Ukraine. A prolonged conflict will sink the G8 summit in Sochi for certain and is guaranteed to lead to greater economic isolation.

Thus, Russia has already begun to pay a high price for its intervention in Ukraine. It stands to lose a great deal more the longer it persists in its foreign adventurism. The real question, then, is whether such practical considerations will ultimately trump ideological and nationalistic ones.

Thirty-five years ago, the newly created Islamic Republic of Iran faced rising inflation and economic malaise as a result of international jitters over its uncompromising, expansionist worldview. But its supreme leader, Ayatollah Ruhollah Khomeini, refused to moderate his policies, famously stating that he had not staged a revolution to quibble over the price of melons. What followed were years of economic stagnation and domestic misery, as Khomeini’s Iran became an international pariah.

It remains to be seen whether President Vladimir Putin is similarly single-minded in his ambitions and dismissive of their impact on ordinary Russians.
Iran's Mullahs Blame Mahmoud
For the regime in Tehran, the Iranian president makes a convenient scapegoat for the plummeting rial and dire economic conditions.

By Ilan Berman

Oct. 10, 2012 4:09 p.m. ET

THE WALL STREET JOURNAL

You've got to feel a little sorry for Mahmoud Ahmadinejad. With his nuclear brinksmanship and inflammatory public rhetoric, Iran's firebrand president is accustomed to hogging the international spotlight. But recent days have seen him making news for a different reason entirely. Ahmadinejad is now fighting for his political life against domestic opponents who blame him for the country's current fiscal crisis.

The trouble began on Oct. 1, when Iran's national currency, the rial, plummeted some 17%, collapsing to a value of 34,700 to one U.S. dollar. The devaluation was not totally unexpected: The rial had been in steady decline over the past year as Western sanctions began to bite. Even so, the Oct. 1 plunge was unprecedented in its scope and devastating in its socioeconomic impact. Mass protests erupted in Tehran, forcing authorities to deploy riot police and resulting in skirmishes between civilians and security forces.

Since then, regime officials have announced a plan to crack down on speculators and black-market money changers in an effort to discourage a run on the rial. Illegal currency traders have been rounded up as cautionary examples.

But the long knives are out for Iran's president as well. Most recently, some 93 members of Iran's legislature, the Majlis, have issued a motion summoning Ahmadinejad to appear before them for a public accounting of his response to the economic crisis. Regime officials have also taken aim at the president, accusing him of firing competent ministers and playing politics with key government posts under his control.

For the Iranian regime, desperately trying to get a handle on the plummeting national currency, Ahmadinejad makes a convenient scapegoat on several fronts.

First, Iran's president is no longer a favorite of the country's clerical establishment. The past two years have seen the emergence of a real rift between Ahmadinejad and his onetime political protector, Supreme Leader Ali Khamenei, on a range of social, economic and political issues. So profound has this rupture become that Ahmadinejad and his followers are now pejoratively referred to as the "deviant current." Calls for their ouster from national politics were commonplace even before the rial crisis.

Ahmadinejad, secondly, has a long track record of ruinous fiscal policies — ones that almost certainly have made the current crisis worse, perhaps significantly. During his nearly eight years in office, Iran's president has increased government spending, doubled down on the
regime's extensive and costly domestic economic subsidies, and promoted "Islamic" banking rates that have made the country's financial institutions increasingly uncompetitive. He has done so, moreover, against the advice of domestic experts and leading economists alike, generating no shortage of popular ill will in the process.

Lastly, Ahmadinejad is already on his way out. He is nearing the end of his second term and cannot run for a third in next summer's elections. And thanks to his very public falling-out with the Supreme Leader, Ahmadinejad is no longer a serious contender for any government appointments or political posts following his presidency. This means, in political terms, that making an example out of him will likely prove cost-free.

None of this will help to ameliorate Iran's current crisis, or to solve the dire economic straits that ordinary Iranians find themselves in as a result of the regime's nuclear ambitions. But scapegoating Ahmadinejad—and administering a healthy dose of domestic repression—may help the regime to quell popular discontent as it tries to right the economy. The ayatollahs, at least, are banking on it.
The Economic and Financial Threat Domain

Roger W. Robinson, Jr.

The threat associated with the economic and financial capability/vitality of an adversary or potential adversary has been described as “threat finance.” In practice, however, the measures put in place to counter this threat, termed “Counter Threat Finance” (CTF), have defined it more narrowly as the fundraising and financing of criminal groups, narcotics smugglers, proliferators, terrorist organizations and pariah states through illicit networks (i.e., black market transactions, money laundering, sanctions busting, etc.) As a result, the target of current CTF programs is, for the most part, the flow of money and materiel directly into the possession or control of non-state bad actors and pariah states, such as Iran and North Korea, as well as the illicit means through which these transfers typically take place.

The economic and financial profile of an adversary, however, represents a threat that goes well beyond this target set. Economic and financial capabilities are critical not only to enabling actual adversary operations, but they can also provide the confidence that is required for an adversary to engage in operations to begin with. An adversary’s perception of their economic and financial vitality, survivability, the resiliency of their sponsorship network and their ability to leverage their economic and financial assets in seemingly benign commercial ways during pre-kinetic stages of conflict should all be viewed as important component pieces of “threat finance.”

The threat inherent in an adversary’s broader economic and financial profile is especially relevant when dealing with state actors (including already-isolated pariah states as well as those that might be better described as “potential” state actor adversaries). From a CTF perspective, economics and finance serves as the basis for a state’s military strength, as a key factor in their risk/benefit calculations vis-à-vis potential conflict and as a dimension of their own non-kinetic Phase Zero operations and strategies against other state actors.

For non-state actors as well, traditional threat finance has neglected to consider the full spectrum of risk that stems from an adversary’s economic and financial support structure. This support structure extends past an adversary’s immediate access to funding to the root sources of support on which they depend for their long-term sustainability, including their ability to reconstitute in the face of short-term adversity (often implicating the support of state actors).

Accordingly, a comprehensive view of threat finance necessarily involves a number of strands that can be somewhat dissimilar from one another. Below is a short list of the
different kinds of threats represented by the economic and financial profile of an adversary.

They include:

- the ability of state actors and non-state actors to pay for weapons and other threat-related operational logistics;

- the money laundering strategies of non-state actors;

- the sanctions-busting strategies of internationally isolated, pariah states;

- the vitality of a non-state actor's support network, including state sponsors, state sponsors of state sponsors and the degree of market knowledge, acceptance, scrutiny and/or support of these various layers of sponsorship;

- the economic and financial capability/vitality of state actors that are potential adversaries and the role of that vitality in their risk/benefit calculations concerning potential conflict with the United States;

- the Phase Zero efforts of adversaries to shape the international economic and financial landscape in their favor for strategic, non-commercial and security-oriented purposes.

Although the current approach to threat finance tackles dimensions of these problems that are indispensable and bare minimum requirements, it lacks an overarching strategic understanding of the issue area and a plan for confronting it. Indeed, the current approach largely misses the fundamental part that economics and finance plays in many other aspects of an adversary's capabilities, planning and preparedness, operations and pre-conflict decision-making.

The diffuse nature of the topic has likely led professionals working in this area to choose those aspects of the threat that are most urgent. Being aware of, and tracking, the bigger picture aspects of the problem, however, would be a valuable first step to filling the strategic void in this area.
U.S. Department of the Treasury
Terrorism and Financial Intelligence
Office of Foreign Assets Control (OFAC)

Additional Information – www.treas.gov/ofac

MISSION
The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

HISTORY
The Treasury Department has a long history of dealing with sanctions. Dating back prior to the War of 1812, Secretary of the Treasury Gallatin administered sanctions imposed against Great Britain for the harassment of American sailors. During the Civil War, Congress approved a law which prohibited transactions with the Confederacy, called for the forfeiture of goods involved in such transactions, and provided a licensing regime under rules and regulations administered by Treasury.

OFAC is the successor to the Office of Foreign Funds Control (the "FFC"), which was established at the advent of World War II following the German invasion of Norway in 1940. The FFC program was administered by the Secretary of the Treasury throughout the war. The FFC’s initial purpose was to prevent Nazi use of the occupied countries' holdings of foreign exchange and securities and to prevent forced repatriation of funds belonging to nationals of those countries. These controls were later extended to protect assets of other invaded countries. After the United States formally entered World War II, the FFC played a leading role in economic warfare against the Axis powers by blocking enemy assets and prohibiting foreign trade and financial transactions.

OFAC itself was formally created in December 1950, following the entry of China into the Korean War, when President Truman declared a national emergency and blocked all Chinese and North Korean assets subject to U.S. jurisdiction.
RESOURCES

OFAC Sanctions Lists
- Specially Designated Nationals List Page
- Consolidated Sanctions List
- Search OFAC's Sanctions Lists
- Sectoral Sanctions Identifications List Page
- Foreign Sanctions Evaders List Page
- Non-SDN Palestinian Legislative Council List
- Non SDN Iranian Sanctions List
- The List of Foreign Financial Institutions Subject to Part 561 (the "Part 561 List")

News and Frequently Updated Content
OFAC updates its website on a regular basis. Information on the latest changes to OFAC's site can be found below.
- OFAC Recent Actions
- Press Center

Sanctions Programs and Country Information
OFAC administers a number of different sanctions programs. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.
- Iran Sanctions
- Ukraine-related Sanctions
- Syria Sanctions
- Counter Terrorism Sanctions
- Counter Narcotics Sanctions
- Cuba Sanctions
- Other Sanctions Programs and Country Information

General OFAC Information and Guidance
In addition to providing guidance on specific sanctions programs, OFAC provides information on a number of sanctions-related issues that span multiple programs or that may affect specific industries.
- Frequently Asked Questions
- OFAC Information for Industry Groups
- Interpretative Rulings on OFAC Policy
- Civil Penalties and Enforcement Information
- OFAC License Application Page
- OFAC Reporting Forms
- OFAC Legal Library
- OFAC Training and Events
- Other non-Treasury sanctions-related resources
- Memoranda of Understanding Between OFAC and Bank Regulators
Panel VI:

Military Justice: Continuity or Change?

Moderator:
Major General Charles J. Dunlap, Jr.
The Military Justice System and Command Accountability

Major Charles J. Dunlap Jr., US Air Force

The Long Commission, which investigated the terrorist bombing of the Beirut Marine barracks, recommended punitive action against officers in the chain of command. The president, however, ruled out courts-martial. This article examines the concept of command accountability and the role of the military justice system.
Professional dereliction and incompetence have rarely been punished since World War II. . . . Failure to do so has bred an atmosphere of professional unaccountability that encourages, because it does not penalize, repetition of failure on the battlefield.¹

INTRODUCTION

In late December 1983, the “DOD Commission on the Beirut International Airport Terrorist Act, October 23, 1983,” chaired by Admiral Robert L. J. Long, US Navy, Retired, issued its report. The Long Commission, as it became known, found that the military officers in the chain of command were responsible for the security failure which resulted in the deaths of 241 Marines when a terrorist truck-bomb exploded in their Beirut, Lebanon, compound.² The commission recommended that appropriate administrative or disciplinary action be taken against these commanders.³ Nevertheless, President Ronald Reagan, saying that the commanders had “already suffered quite enough,” ruled out courts-martial for the officers and accepted the responsibility for the disaster himself.⁴

The president’s decision brought immediate criticism. One unidentified former senior military officer was quoted in The New York Times as saying of the president’s action:

I’m astonished that he moved so quickly to pre-empt the possibility of formal punishment. . . . If the system isn’t given a chance to establish accountability, how can you expect officers to fear the result of failure?⁵

Similarly, a Wall Street Journal editorial argued:

In relieving the military of even its minimum responsibilities, the President is suggesting that it has no responsibilities at all. That is anything but a recipe for avoiding new military embarrassments in the future.⁶

ANALYSIS OF THE POTENTIAL OFFENSES

The Uniform Code of Military Justice—or code—has no provision dealing exclusively with command accountability. Yet, at least three provisions of the code could apply to the commanders in the Beirut case: Article 92, dereliction of duty;⁷ Article 134, homicide based on simple negligences;⁸ and Article 99, misbehavior before the enemy.⁹ These articles state offenses which have no parallel in civilian criminal law. Likewise, these offenses share another unique characteristic—criminal liability based on a showing of only simple negligence.

Simple Negligence Standard

Nothing in the Long Commission Report suggests that the Beirut commanders could be blamed for anything more than simple negligence. However, the House Armed Services Committee concluded in its separate investigation that “very serious errors in judgment” had occurred.¹⁰ Although this conclusion indicates a greater degree of liability, the factual findings indicating only simple negligence were similar to the findings of
the Long Commission.\textsuperscript{11} Still, simple negligence makes criminal a wide range of conduct requiring proof of only a slight deviation from acceptable standards. Colonel William Winthrop, in his classic treatise, \textit{Military Law and Precedents}, defined it to include the "improper" execution of orders, the failure to take "proper precautions" and not "doing the best" in a given military situation.\textsuperscript{12}

The current \textit{Manual for Courts-Martial}\textsuperscript{13} is similarly broad in its explanation, describing simple negligence as a "lack of that degree of care which a reasonably prudent person would have exercised under the same or similar circumstances."\textsuperscript{14} This definition, found in the discussion of Article 92, is altered slightly in the discussion of Article 99 wherein simple negligence is described as the "absence of conduct which would have been taken by a reasonably careful person."\textsuperscript{15} Similarly, the explanation of negligent homicide under Article 134 uses the "reasonably careful"\textsuperscript{16} language.

Despite these minor variations, the phrases describe, as law Professor William L. Prosser puts it, a standard of conduct not of "any ordinary individual, who might occasionally do unreasonable things; he is a prudent and careful man, who is always up to standard."\textsuperscript{17} It is against this standard that the Beirut commanders must be judged.

\textbf{Dereliction of Duty}

The most common offense suggested by Jeffery Record and the other critics is dereliction of duty. It is important to note that the evaluation of a supposed dereliction must be based on the facts as they appeared at the time of the alleged offense, not afterward. As the Army Board of Review stated in the \textit{United States v. Ferguson},\textsuperscript{18} "In testing for negligence the law does not substitute hindsight for foresight." This case also held that a commander does not have to be more than "reasonable" to escape criminal liability. Conceding that the commander "could have done more," the board, nevertheless, reversed Lieutenant Ferguson's dereliction conviction for not sufficiently briefing a subordinate on a safety matter.\textsuperscript{19} Contrary to the trial court, the board found the commander's actions minimally adequate.

Lack of malicious intent does not excuse the offense, however. For example, Major General Robert W. Grow, a military attaché to the Soviet Union, was convicted of dereliction of duty for failing to secure his personal diary.\textsuperscript{20} Included in it were references to material which was technically classified. Because the same information was widely available in the media, the general treated his memoir as if it were "a copy of the Saturday Evening Post."\textsuperscript{21} Unfortunately for the general, persons unknown photocopied the diary, and embarrassing excerpts appeared in an East German paper. Parenthetically, this case also serves as a precedent for prosecuting a senior officer for what may be regarded, because of its maximum penalty of only three months' confinement, as a relatively minor offense.\textsuperscript{22}

\textbf{Negligent Homicide}

A more serious charge against the Beirut commanders would be negligent homicide under Article 134. Punishable by up to one year in prison for each death,\textsuperscript{23} this offense uses essentially the same simple negligence standard. In the \textit{United States v. Kick},\textsuperscript{24} the Court of Military Appeals acknowledged that criminal liability for crimes based on simple negligence was virtually unknown in civilian law. The court, nevertheless, af-
firmed the conviction by citing the "special need in the military to make the killing of another as a result of simple negligence a criminal act." Because of the use of weapons, explosives and other dangerous instruments, the court found that "society demands protection." Despite this judicial acknowledgment of the special need for accountability in the military, no published case reports the prosecution of a commander for the negligent homicide of his troops. Very likely, this omission is simply the result of a reluctance to extend criminal responsibility to a commander for an act which, as in the Beirut case, was initiated by an enemy. Nonetheless, no legal barrier prevents such a prosecution if the commander's negligence played, in the words of the Court of Military Appeals, a "material role in the victim's decease." Misbehavior Before the Enemy By far, the most serious of the potential charges against the Beirut commanders is the one posed by Article 99. This article, which provides for the imposition of the death penalty, prohibits several forms of misbehavior before the enemy. It condemns military personnel who, through "neglect, . . . endanger the safety of any . . . command." The Manual for Courts-Martial explains that the "before the enemy" element is not defined in terms of distance but is a tactical relation which would include at least the ground commanders in Beirut. "Enemy" is loosely defined to include any "hostile body." For example, in the United States v. Monday, the 1965 Dominican Republic operation, resembling in many ways the Beirut situation, fulfilled the Article 99 prerequisites. As the examination of these three articles of the code has shown, a court-martial, if it came to the same conclusions as the Long Commission, could lawfully adjudge long prison terms for the Beirut commanders. Indeed, the ground commanders could face the ultimate punishment—execution. Nevertheless, no trial will take place despite the seriousness of the potential charges. The support for this decision demands examination.

ANALYTICAL SUPPORT FOR THE DECISION

Purpose of the Military Justice System

The purpose of the military justice system is broader than that of the civilian system. As Captain Edward M. Byrne observes in his book Military Law:

Civilian criminal law seeks to restrict and regulate behavior so that people can live together in peace and tranquility. Military justice has a similar and yet more positive purpose. Military justice must, of necessity, promote good order, high morale, and discipline.

The goal of this "more positive purpose" is to achieve the military mission. The entire rationale of the military justice system is to help provide the nation with a force capable of winning wars. Therefore, the paramount factor in military justice decisions should be the interests of the military mission.

The US Supreme Court has readily acknowledged the primacy of the military mission over individual interests. In the often-quoted case of Burns v. Wilson, the court said, "The rights of men in the armed forces must perforce be conditioned to meet certain overriding demands of discipline and duty." Of course, a military member still has a right to a fair trial requiring proof of guilt beyond a reasonable doubt. But the decision to refer a case to
trial where, as in the Beirut case, reasonable evidence of individual guilt exists is entirely at the discretion of the court-martial convening authority. Such a decision should be based on clear military interests and should not be clouded by subjective perceptions that those accused had "already suffered quite enough."

Regardless of the evidence of guilt, nothing in the code or the *Manual for Courts Martial* requires the convening authority to refer a particular case to trial. In fact, the manual merely states that a commander "may refer" a charge but is "not obliged" to do so. In practice, many cases are disposed administratively, as was the Beirut case when three commanders received "letters of caution." Other command accountability cases are resolved through the expediency of the relief of command. To determine whether a court-martial is necessary, a judgment must be made that court-martial punishment would enhance the military’s ability to accomplish its mission.

Rehabilitation

Court-martial punishment traditionally addresses three theories: rehabilitation, deterrence and retribution. Rehabilitation by court-martial punishment is seldom appropriate in command accountability cases based on simple negligence. For example, behavior modification, often a goal of rehabilitation, is not easily adapted to these cases. For most commanders, such as those in the Beirut case, there is simply no pattern of criminal behavior to modify. Besides, a conviction would virtually end the chances of those accused for further command, and this could very well be harmful to the military mission.

Commanders, including those in the Beirut case, are usually highly trained and motivated professionals—valuable assets to the military mission. General Sir John Hackett, a much decorated former British army commander, suggests that a failed commander given another chance is a "wonderful investment." He explains:

*An opportunity to re-establish himself in his own esteem, when he has forfeited it, is something for which a man will give you a great deal in return. . . . and the return is often a bountiful one.*

Thus, it appears that the rehabilitation theory may best be served in the Beirut case by returning the commanders to duty.

Deterrence

Deterrence is the theory most attractive to the critics of the Beirut decision. Presumably, the harsh punishment of those commanders would deter others from making similar mistakes. The end result of this process would be, theoretically, more competent, effective leaders. As attractive as this may sound, careful analysis shows that the result may well be just the opposite. Consider the Soviet model.

The Soviets employ a deterrence theory in dealing with their commanders. Military analyst Andrew Cockburn reports that Soviet officers at all levels of command fear stiff punishments for even minor transgressions. As a result, officers cover up errors and, even worse from the standpoint of military effectiveness, initiative is blunted.

The Soviets do, however, recognize the practical military difficulty their approach raises. Colonel General Oleg Kulishev pleaded in an article in the *Soviet Military Review* for punishment for the officer who is "afraid" to take responsibility, "not the one who showed initiative but did not
achieve success." Nevertheless, Cockburn says the reformers are making little progress in fostering initiative among Soviet officers.47

Furthermore, the US Supreme Court recognizes that the fear of a legal penalty can undermine a commander’s effectiveness. In barring lawsuits by enlisted personnel against commanders for alleged constitutional violations, the court, in the 1983 case of Chappell v. Wallace, cited “the special nature of military life” and the “need for unhesitating and decisive action by military officers” as the rationale for its decision.48 Likewise, Martin Blumenson and James L. Stokesbury point out in their book, Masters of the Art of Command, that officers who constantly look “over their shoulder to see whether the ax is about to fall are diverting attention and energy from the more important matters on the battlefield.”49

Criminal action against commanders for simple negligence could also greatly aggravate what is widely viewed as one of the most serious problems facing the military today—careerism. Excessive anxiety about one’s career is an attitude sometimes attributed to military commanders. According to psychologist Norman F. Dixon, in military organizations, “the penalty for error is very much more substantial than the reward for success.”50

Dixon believes that this negative reinforcement breeds a fear of failure that stifles good leadership.51 Certainly, any punishment would tend to feed this fear, but the prosecution of the Beirut commanders based on simple negligence would likely result in a new and even greater level of anxiety among commanders. The probable consequence would be less effectiveness in officers faced with command under similarly trying circumstances.

As we have seen, the deterrence concept might well succeed in causing other commanders to change their actions. But the military benefit of such a change is dubious at best. Since court-martialing the Beirut commanders to deter others would not produce the kind of leader the military needs, the military justice system would not have been served by such a prosecution.

Retribution

Retribution is the theory of punishment most applicable to command accountability cases. Byrne defines it as “the concept that a person has an ultimate responsibility for his acts and, if he has committed a crime, deserves punishment.”52 In military terms, the failure to exact retribution through appropriate channels can have a devastating effect on morale. Witness the fact that US officers were assassinated in Vietnam by their own troops.53 Reasons for this situation were varied and complex, but at least part of the blame lay in the apparent perception that the system was not dealing with officers who were unnecessarily risking the lives of their troops.54 In the Beirut case, however, there is no evidence of such a perception. In fact, a prosecution might well have hurt the morale of the Marine Corps, and this possibility, according to The New York Times, was a factor in the president’s decision.55

Another factor The Times reported was the president’s desire to minimize the impact of the Long Commission Report on his policy in Lebanon.56 Similarly, analyst Patrick J. Sloyan suggests that the president wanted to avoid airing at a court-martial an alleged dispute between the Joint Chiefs of Staff and the White House over the role of the Marines in his Middle East policy.57 Despite implications to the
contrary, the desire to avoid negative public opinion is a legitimate consideration in command accountability cases. Clearly, public support and confidence are in the interests of the military. Colonel Harry G. Summers Jr., in his book *On Strategy: A Critical Analysis of the Vietnam War*, sees public support as a key to the successful use of military force. Therefore, if retribution by means of a court-martial is necessary to retain public confidence in the military, then, this theory should predominate in command accountability cases.

In cases such as that of Beirut in which a large number of lives were lost, the public may find any disposition short of court-martial unacceptable. Administrative actions, as devastating as they may be for the officers personally, may be perceived by the public as a mere "slap on the wrist." However, unlike deterrence, there have been no calls for retribution in the Beirut case. Still, a demand for retribution by the public could have justified a different decision. This would not be "scapegoating" because scapegoating implies the prosecution of innocent persons which, if the Long Commission’s findings are correct, is not the case with the Beirut commanders.

The "X" Factor

Besides the traditional theories of court-martial punishment, an additional factor must be considered in the decision to refer a command accountability case to trial—the unpredictability of the outcome, or the x factor. Members of a court-martial panel may decide not to convict an individual despite seemingly conclusive evidence of guilt. They may also decide to adjudge little or no punishment even if they do bring a conviction. Both of these phenomena occurred in the courts-martial which resulted from the collision of the USS *Belknap* and the carrier USS *John F. Kennedy* in 1975.

In the military justice system, the commander’s fate is decided by other military officers. Current Chief Judge of the Court of Military Appeals Robinson Everett explains that, since military juries are drawn from the same profession, there is "a much higher probability that the persons who hear the case will understand and be responsive to the problems involved." In the Beirut case, few military professionals apart from the Long Commission were critical of the commanders’ performance. In spite of the evidence and the relatively easy legal standard involved, a prosecution before fellow officers cognizant of the difficult mission the commanders faced might well have been fruitless.

The decisionmaker must consider the damaging effects of a potentially unsuccessful prosecution. The public may consider it a self-serving whitewash by the military, while the military may conclude that the outcome eviscerates the concept of command accountability. The severity of these effects on the military mission may well lead a decisionmaker to conclude that prosecution is ill-advised.

CONCLUSION

We have now considered why the decision not to court-martial the Beirut commanders, even assuming their guilt, was warranted in the interests of both the military mission and the military justice system. All commanders should be aware of their vulnerability to criminal charges under the Uniform Code of Military Justice because of the simple negligence standard.
Rather than setting a precedent of abdicating commanders of their accountability, the Beirut proceedings merely reaffirm the principle that each case must be decided upon its own particular set of facts and circumstances. As we have seen, the code provides stiff punishments to enforce accountability. Yet those punishments need not always be imposed to have the desired effect as this account by the ancient historian, Livy, illustrates:

In the Sammite wars a certain Praetean praetor had been slow in bringing up the reserves. When back in camp after the battle the Roman commander, Papirius Cursor, came to the praetor’s tent and called him out. He then commanded a lictor to prepare his axe; and after waiting in silence until the axe was ready—while of course the praetor stood aghast expecting the next command to be for his execution—Papirius continues to the lictor: “Come, cut this root; someone will stumble on it.”

Clearly, a court-martial is a potent tool with which to enforce command accountability. It can present a convenient and enticing option to the decisionmaker who is faced with a military tragedy. But, as the analysis of the Beirut case shows, it may very well be the wiser man who forgoes its use.

NOTES

1 Jeffrey Record, Is America's Officer Corps Inept? US News & World Report, 27 February 1984 p 38
3 ibid
7 Uniform Code of Military Justice, Article 92, Public Law 505, Act of May 5, 1950, 64 STAT 108 (64 Statutes at Large 108), 10 USC 892 (Title 10, US Code, Section 892) (1976)
14 ibid, Part IV, paragraph 153(3c)
15 ibid, paragraph 23c(3a)
16 ibid, paragraph 85c(2)
18 United States v Ferguson, 12 CMR 570 (Court Martial Reports, Volume 12 p 570), (A B R (Army Board of Review) 1953) p 578
19 ibid, pp 576 77
20 United States v Groe, 11 CMR 77, 3 USCMR 7 (US Court of Military Appeals Volume 3, p 77) (1953) p 80
21 ibid, p 86
22 Manual for Courts Martial United States, 1984 op cit. Part IV, paragraph 163(3a)

52 February 120
Tuition Assistance. Scheduled changes to the Army's Tuition Assistance Program that would have cut benefits and required soldiers to use their GI Bill while still on active duty have been canceled. A restoration of budget funds now allows the Army to keep tuition assistance rates and policy unchanged. The proposed changes, which would have taken effect in October 1984, would have required soldiers to use GI Bill benefits before becoming eligible for tuition assistance. The current rates now in effect are at the maximum congressional limits—90 percent and above for soldiers E5 and above with less than 14 years' service and 75 percent for all others.

Soldiers who are eligible for assistance under the GI Bill should still consider using it while in the service. Benefits under the GI Bill expire 31 December 1989, and extension beyond that date is uncertain.
THE MODERN AMERICAN MILITARY

EDITED BY DAVID M. KENNEDY

OXFORD UNIVERSITY PRESS
Top Ten Reasons
Sen. Gillibrand’s Bill is the Wrong Solution to Military Sexual Assault

CHARLES J. DUNLAP, JR.

ABSTRACT

Over the years Congress has made plenty of efforts to “improve” the military justice system for a variety of reasons, but few matters have generated more offerings than did the Pentagon’s report this past spring of an estimated 26,000 victims of “unwanted sexual contacts” in the armed forces. Some initiatives to address this very critical problem, like the bipartisan effort of Senators Barbara Boxer and Lindsey Graham, look promising; others, not so much.

However, none are as misguided as Sen. Kirsten Gillibrand’s proposal. Indeed, it is hard to think of a proposal that could be more wrong for the military, and especially for the victims of sexual assaults.

Sen. Gillibrand wants to remove commanders from the military justice process and replace them with a new, 600-person bureaucracy which would have lawyers as the “deciders” in disciplinary matters involving sexual assault and other serious cases. Her proposal is based on a popular narrative that is filled with false impressions such as the notion that the majority of the estimated 26,000 victims are women (actually, 53% are men); that military personnel do not “trust” their commanders (polls show they do); that the handful of foreign militaries who have removed their commanders have shown progress in combating sexual assault (they have not); and that prosecutor-centric systems like the one Sen. Gillibrand wants to impose on the military are more successful than the military’s in suppressing sexual assault (the evidence shows they are less so).

Most troubling is the fundamental lack of a real understanding in Sen. Gillibrand’s proposal as to what solves problems in the armed forces. It is axiomatic in the military that everything important is commander-led. This is particularly true with respect to the matters of morale and discipline that are so central to the warfighting capabilities for which commanders — not lawyers — are ultimately responsible and accountable. Lawyers, even those thoroughly expert in the law and indubitably well-intentioned as those serving in the armed forces, simply do not, and could not, have the broader insights and experience that commanders acquire through years of leadership, and by bearing the grave burden of sending young Americans in harms’ way to do the Nation’s business. Commanders are uniquely and irreplaceably equipped to exercise disciplinary authority in what the Supreme Court recognizes as the military’s “separate society.”

This essay argues that combatting sexual assault through the military justice system is just too important to be anything other than commander-led, and offers ten reasons why Sen. Gillibrand’s proposal will hurt not only the military’s readiness and warfighting capability, but also sexual assault victims. In addition, it describes legislative initiatives that should be examined, but are not being considered by anyone in Congress.

INTRODUCTION

Over the years Congress has made plenty of efforts to “improve” the military justice system for a variety of reasons, but few matters have generated more offerings than did the Pentagon’s report this past spring of an estimated 26,000 victims of “unwanted sexual contacts” in the armed forces. Some initiatives to address this very critical problem, like

Copyright © 2013 by Charles J. Dunlap, Jr.
* Major General, USAF (Ret.), Professor of the Practice of Law and Executive Director, Center on Law, Ethics and National Security, Duke Law School.
Nov. 28, 2013

Ten Reasons

The bipartisan effort of Senators Barbara Boxer and Lindsey Graham, look promising; others, not so much. However, none are as misguided as Sen. Kirsten Gillibrand’s proposal.

Sen. Gillibrand thinks the “solution” to sexual assaults in the armed forces is to remove disciplinary authority from field commanders and give it to a new, $113 million, 600-person bureaucracy that she wants the Pentagon to create. It is hard to think of a proposal that could be more wrong for the military and especially for the victims of sexual assaults.

As will be expanded upon below, the attack on the military justice system is curious since the armed forces are hardly the epicenter of the blight of sexual assault in our society. Professor Rosa Brooks of Georgetown Law School points out the enormous scope of the problem in the civilian community by observing that “[a] 2010 study by the Centers for Disease Control (CDC) found that 18.3 percent of civilian women had been raped at some point in their lifetime, while 27.2 percent had experienced ‘unwanted sexual contact.’” Indeed, the Pentagon survey found that 30 percent of women and 6 percent of men in the military indicated they experienced “unwanted sexual contact” prior to entry into the armed forces.

One would think, therefore, that a serious effort to address sexual assault would have Sen. Gillibrand and others starting by investigating why so many young people come to the military already victimized. Such an examination might start with the nation’s colleges and universities, as they share the military’s youthful demographic.

One might think, for example, that since women outnumber men on college campuses the research might show that sexual assault was a lesser problem at universities, but that does not seem to be the case. In fact, Professor Brooks and others believe the problem of sexual assault is even more pronounced on America’s campuses than it is in the armed forces.

The numbers appear to support their conclusions. Although there are no figures for all “unwanted sexual contact” in terms of actual assaults, the Centers for Disease Control reports that since entering college an astonishing 19% of women have experienced the most aggravated form of unwanted sexual contact, that is, attempted or completed sexual assault. Given those statistics, it is unsurprising that Brooks concludes that “the military appears to have done a better job than most colleges of reducing the sexual assault rate and increasing women’s willingness to report assaults to the authorities.”

A very recent article in Princeton University’s newspaper also seems to support Brooks’ conclusion by describing a survey showing that 15% of its undergraduate women reported not simply experiencing the “unwanted sexual contact” of the Pentagon survey (which could include an unwanted hug mistakenly given by someone with no expectation that it would be perceived as “sexual”) but actual “non-consensual vaginal penetration during their time at the University.” Would not all this suggest that the military should be something of an example - as opposed to a target - in the nation’s battle against sexual assault?

Apparently, however, Congress does not see it that way, as it has shown little appetite for confronting colleges or universities. This is tragic for sexual assault victims, especially considering how leniently some universities treat transgressors. Atlantic Magazine.
Nov. 28, 2013

Ten Reasons

reports that at Yale, of six students found to have committed "sexual misconduct" since January 1st, 2013, "only one was suspended." The magazine adds that "[f]our received a 'written reprimand' - a letter from the administration clarifying that Yale does not tolerate sexual misconduct - but [Yale took] no tangible disciplinary action."

Exactly why Sen. Gillibrand and others in Congress berate the military’s efforts yet tolerate "no tangible disciplinary action" for sexual assaults at a university that reaps hundreds of millions in Federal grants is hard to figure. Could it not do more? For example, why not suspend a university’s eligibility for Federal largess pending the enactment of tough standards for dealing with sexual assault? Why not, as some have suggested, levy fines on institutions out of compliance with Title IX of the Education Amendments of 1972?

Of course, it is beyond dispute that any and every sexual assault needs to be addressed, whether it arises in the military, on college campuses, or anywhere else. For if we are inclined to believe the number she quotes so readily, it is quite noteworthy that neither Sen. Gillibrand nor any of her supporters have ever explained why the commander-led system she criticizes so much nevertheless showed a 44% decline in the number of estimated victims between 2006 and 2010 and, even with the recent uptick, still shows an overall decline since 2006.

In fact, the sharp increase recently seen in servicemembers willing to come forward under the current commander-led system to report sexual assaults is a major development as it clearly undermines the central pillar of Sen. Gillibrand’s argument for her legislation, that is, that victims are afraid to report sexual assault.

If the Pentagon has already seen a 46% increase in reporting under the existing system, why do we need Gillibrand’s change that would rip apart a system that is showing substantial improvement? As Sen. Claire McCaskill (an ardent supporter of victims’ rights but opponent of Gillibrand’s bill), put it, the "new statistics of drastically increased reporting [are] a strong indicator that retaining a limited role for commanders, while instituting historic, aggressive reforms, is the key for curbing sexual assaults."

But there is much more wrong with Sen. Gillibrand’s idea. Indeed, reams can be written detailing why Sen. Gillibrand’s proposal for the armed forces is so misguided, but for the busy reader, this essay limits the critiques to the top ten reasons.

The Top Ten

1) It will unnecessarily hurt victims of sexual assault.

Sen. Gillibrand wants to yank commanders out of the disciplinary process in favor of lawyers, but victims will find that even well-intentioned lawyers are less able to vindicate their claims than are commanders. Because American Bar Association rules dictate that prosecutors not pursue cases in the "absence of sufficient admissible evidence to support a conviction," lawyers gauge which cases to take to trial based upon whether or not they subjectively think juries will conclude that the admissible evidence meets the demanding "beyond a reasonable doubt" standard.

Military commanders, however, see things differently because they have a wider set of responsibilities, including maintaining the morale and discipline so essential to leading
troops in combat. Thus, military law only requires them to find “reasonable grounds to believe that an offense has been committed” in order to send a case to trial.

This appears to be why in the recent case of Naval Academy midshipmen accused of sexual assault the commander referred the case to trial against the recommendation of a military judge who investigated the case. But under Gillibrand’s proposal, the decision of a lawyer that the cases should not be pursued would have trumped the military commander’s view that the case needed to be prosecuted.

The reality is that military commanders are more disposed to send allegations of sexual assault to trial than are many civilian prosecutors. Sen. McCaskill explains that “[n]o data has been offered to show that commanders decline to refer cases for court martial. Data does show that in the past two years, commanders referred 96 cases for court martial that prosecutors declined to pursue-meaning 96 victims had their day in court because of commanders.”

Additionally, Gail Heriot, a professor of law at the University of San Diego and a member of the U.S. Commission on Civil Rights, reports a Fiscal Year 2011 study of rapes occurring in a civilian setting under circumstances where both civilian and military authorities had jurisdiction. She said that on “those occasions...in which the civilian jurisdiction took the lead, prosecution rates were 11 percent. In contrast, the military’s prosecution rate was 55 percent.” Yet Gillibrand wants the military to model itself after such a markedly less victim-responsive arrangement.

More generally, the military takes to trial 21% of all reported cases, while in the lawyer-driven civilian sector process — the kind of system Gillibrand wants to impose — only 19.5% of cases make it to the courtroom. While a 1.5% differential does not seem like a huge difference, when translated into real numbers, it is really significant. Scores of victims seeing their cases being pursued in the current, commander-led system would not see them being prosecuted in civilian courts.

In short, it is a mistake for anyone — but particularly rape victims — to think that a lawyer-centric scheme will be as aggressive in pursuing their cases as the commander-led system Sen. Gillibrand wants to dismantle. It is sadly predictable that the prosecutions in the armed forces would fall to the civilian rates or even lower. Under Gillibrand’s proposal, too many military sexual assault victims would perceive the system as failing them yet again.

2) It will impose a civilian-like process that has shown utterly no sign that it is more successful (and often less successful) at preventing sexual assault than the military’s commander-led system.

Benjamin Franklin once observed that “an ounce of prevention is worth a pound of cure.” As already suggested, the evidence shows that the military’s commander-led criminal justice system has proven to be been far more successful at preventing sexual assault in the armed forces than has the prosecutor-centric civilian system that Gillibrand wants to impose on the military.

Specifically, in 2012, the Centers for Disease Control reported a survey that showed during the previous twelve months, 5.6% of women, and 5.3% of men suffered sexual violence in the civilian population. What makes these percentages even more appalling is
that they do not include rape. When rape is added, for women it approximates to an overall rape and sexual violence rate of 6.7 percent.

If those percentages from the civilian community were applied to the armed forces, an estimated 77,000 sexual assaults would have to occur to equal the estimate as to what happened in civilian society. Yet the Pentagon report that Senator Gillibrand and her supporters rely upon actually estimates the much lower figure of 26,000 “unwanted sexual contacts” – far less than what the percentages from civilian society would project.

Inexplicably, Sen. Gillibrand wants to uproot the commander-led process that these statistics indicate is approximately three times more successful in deterring sexual assaults than the prosecutor-centric civilian system she wants the military to emulate. Professor Brooks may put it best when she says that:

[ Sexual assault in the military] is a genuine and serious problem, but the frantic rhetoric may be doing more harm than good. It conceals the progress the military has made in developing effective sexual assault prevention and response programs, and it distracts us from the even higher rates of sexual violence in comparable civilian populations.

Brooks argues persuasively that the “military seems to be doing something right, since it has been able to bring sexual assault rates down below those prevalent in comparable civilian populations.” The military is “doing something right” because its commander-led system works as well or better than the civilian model.

3.) It will remove commanders – who have direct responsibility for success in combat – from taking tough action they need to take to maintain morale, good order and discipline, and it will shift accountability for sexual assaults away from them.

Because commanders are more focused on battlefield victories than they are concerned about courtroom victories, this gives them a different mindset about prosecutions than the military lawyers who Gillibrand wants to be ‘the deciders’ in sexual assault and other cases of serious crimes. Colonel Jeannie Leavitt, the first woman to command an Air Force fighter wing, made this clear in her testimony before Congress last June.

According to Senator Carl Levin, Leavitt “told our committee that she could ‘absolutely see the scenario where a prosecutor may not choose to prosecute a case,’ because of the uncertainty of a conviction, but that [as] the commander, I absolutely want to prosecute the case because of the message it sends, so that . . . my airmen understand that they will be held accountable.”

This is yet another illustration as to how the thinking of a military commander can markedly differ from that of a lawyer. Sending clear messages to troops is an essential attribute of effective military leadership, but Sen. Gillibrand’s proposal deprives commanders of a powerful tool for conveying such messages. “Messages” from even the finest staff lawyers, just would not – and could not – fill the resulting void.

Sen. Gillibrand also does not seem to realize how important accountability is to an effective defense establishment, notwithstanding Colonel Leavitt’s reference to it. If Sen. Gillibrand’s proposal is enacted, commanders could rightly say sexual assault is the
“lawyers” problem because they, not the commanders, would have control of disciplinary action.

Yet military lawyers, as talented and as hard working as they are, simply are not in nearly as strong a position to holistically address the many aspects of the problem of sexual assault as are commanders with disciplinary authority. Without disciplinary authority commanders become mere managers, but to address as serious an issue as sexual assault, commanders need to lead the disciplinary process and be accountable for it.

4.) It fails to appreciate the purpose of military law, and the vital role commanders play in it.

According to Sen. Gillibrand, she proposed her legislation not because it would be better for national security, but because, she claims, “victims have asked.” No criminal justice system, in the military or anywhere, ought to be shaped by what accusers want. Quite the contrary, the Constitution’s Bill of Rights, is based on protecting the citizenry against the accusatory powers of the state.

Moreover, a central failing of Sen. Gillibrand’s proposal is that it does not reflect - or even recognize - the larger purpose of military law as compared to civilian jurisprudence. The Manual for Courts-Martial makes it clear that a purpose of military law is to “promote justice” as well as “to assist in maintaining good order and discipline in the armed forces,” but all of this is done not to advance the interests of any individual or even group of individuals (short of the citizenry writ large) - however deserving. Rather, the purpose of military law is “to promote efficiency and effectiveness in the military establishment, and thereby strengthen the national security of the United States.” Therein lies a key problem with Sen. Gillibrand’s proposal.

Perhaps because Sen. Gillibrand, like many of her supporters, has no military service or related experience on her resume, her proposal and her statements in connection with it reflect almost no appreciation for the potential harm to the nation’s security her bill could cause. She and her supporters seem to have forgotten that the Supreme Court has found that “no governmental interest is more compelling than the security of the Nation.”

Commanders are keenly aware of this paramount government interest, and it gives them even more incentive to purge sex offenders from their units because of its obvious effect on morale and discipline so necessary for success in combat. This is why so many with actual military experience find it bizarre that Sen. Gillibrand thinks that there is some kind of “conflict of interest” in a commander taking action against a member of his or her unit.

Whatever an “interest” may be to a civilian like Sen. Gillibrand, to a commander and, indeed, all members of the military, there is - as the Supreme Court puts it, “no governmental interest is more compelling than the security of the Nation.” Since the security of the nation is undermined by sexual assault because it destroys the comradeship among troops so essential to warfighting capability, the real “conflict” is between the commander and those whose criminal conduct is imperiling the overarching “interest” in the nation’s security.

In truth, commanders have unique insights in this regard because, unlike any prosecutor, they have the enormous burden of preparing young women and men to go in harms’ way
and, if necessary, kill other human beings in the name of the state. There is nothing like it in our civilian society. As the Supreme Court puts it, “the armed forces depend on a command structure that at times must commit men to combat, not only hazarding their lives but ultimately involving the security of the Nation itself.”

That “command structure” upon which the armed forces must depend needs to be held inviolate because of the warfighting mission. In order to carry out that mission which is, as the Court cogently describes it, “to fight or be ready to fight wars should the occasion arise,” disciplinary authority is essential and irreplaceable. When George Washington said that “discipline is the soul of an army,” he was echoing thousands of years of military history in which every successful commander in virtually all conflicts of any significance had the exact authority Sen. Gillibrand wants to take away.

Indeed, the Supreme Court recognizes that “[n]o question can be left open as to the right to command in the officer, or the duty of obedience in the soldier.” This is what is so dangerous about Senator Gillibrand’s amendment. By removing disciplinary authority from commanders and giving it to lawyers far from the battlefield, a question is, indeed, “left open as to the right to command in the officer, or the duty of obedience in the soldier.” This explains why almost every commander with authentic combat experience is so dead set against Sen. Gillibrand’s scheme.

Those in Congress most experienced with military matters understand why combat-experienced commanders are so opposed. As Sen. Carl Levin, Chairman of the Senate Armed Services Committee, put it:

> We cannot strengthen our efforts by weakening the authority of our commanders to act against sexual assault. Commanders were tasked again with making monumental those changes in military culture, from combatting racial discrimination in the 1950s to ending “don’t ask, don’t tell” in 2011. If we are to accomplish the change in military culture that we all agree is central to combatting sexual misconduct and sexual assault, commanders are essential. We cannot fight sexual predators if we make it more difficult to try and convict them. And we cannot hold our commanders accountable for accomplishing the needed change in culture if we remove their most powerful weapon in the fight.

**5.) It removes commanders from the disciplinary process even though the overwhelming majority of members of the armed forces, and their families, give their commanders the highest ratings in the battle against sexual assault.**

Sen. Gillibrand’s proposal is surprisingly indifferent to the support that the overwhelming majority of military members and their families have expressed for their commanders. According to the Pentagon’s own survey:

- 88 percent of women and 94 percent of men gave their leadership the highest rating for making it “clear that sexual assault has no place in the military;”

- 80 percent of women and 88 percent of men gave their leadership the highest rating for “promoting a unit climate based on mutual respect and trust;”
- 77 percent of women and 86 percent of men gave their leadership the highest rating for “leading by example” on this issue; and

- 73 percent of women and 85 percent of men gave their leadership the highest rating for “creating an environment where victims would feel comfortable reporting.”

Similarly, a June 2013 poll by the Pew Research Center found that military households—again, overwhelmingly—believed that the better way of handling sexual assault was for the military commander to handle the issue internally as opposed to Congress changing military law. More generally, the Pew poll found that: “[m]ost of those in military households (63%) have confidence in military leaders to do the right thing in handling the problem of sexual assault.” In other words, military households oppose Congress making any change in military law on this issue, not just Gillibrand’s proposal.

The Gillibrand bill reflects a basic misapprehension of the wants and needs of those of the vast majority actually serving in today’s military. Quite frequently the victims supporting Sen. Gillibrand’s bill are referencing experiences from years if not decades ago. Although everyone is sympathetic for what might have occurred in the past, relevant and effective solutions to military sexual assault must be based on the current military, not the military of past.

People in today’s armed forces—as well as their families—know that if there is a tough problem to be solved, the effort must be commander-led. That is the reality of military life in the 21st century, and those serving know it. That is why they support their commanders, and do want Congressional “fixes.”

6. It is inconsistent with the public’s opinion, which expresses vastly more confidence in military leaders than it does in any group of lawyers, including the Supreme Court.

Sen. Gillibrand’s proposal to replace military commanders with lawyers as the “deciders” in sexual assault cases profoundly misperceives the attitude of the public towards military leaders relative to lawyers.

Among the general public—despite being subjected to a virtual avalanche of negative antimilitary publicity on this subject—the Pew Research Center poll from last August showed that 52% have a great deal (or a fair amount) of confidence in military leaders to handle the sexual assault issue correctly, while only 37% have confidence in Congress to do so. Further, that 37% cannot be interpreted as support for Gillibrand’s bill because there are a plethora of Congressional offerings of which hers is just one.

What Sen. Gillibrand’s proposal fails to recognize is that the American public simply has considerably more confidence in military leaders than it does lawyers. According to a 2012 Harris poll, no group of lawyers—including the leaders of the civilian justice system and its courts—rates higher than military leaders in the public’s confidence. Similarly, another Pew poll shows that the public’s favorable view of military leaders (71%) far outstrips that of the Supreme Court (53%) and Congress (27%).

It is true that the landslide of negative, one-sided publicity has taken its toll, especially when a poll such as the one conducted recently by the Washington Post/A3C News asked its question in such a way as to invite answers favoring Sen. Gillibrand’s bill (which it
editorially supports). By casting the debate on Gillibrand’s proposal as between the attractive characterization of “independent military prosecutors” and the perfunctory and dismissive characterization of the commander-led systems as simply “the usual chain of command” it is not surprising that the former was more popular.

Why did not the poll cast the current system more accurately as “experienced commanders schooled in the challenges of military leadership”? Or some other more even handed way? Why did not the poll mention that prosecutor-centric systems take fewer cases to trial? Why did not the poll mention the cost? And should we not question a poll when the sponsoring organization has already expressed it editorial view?

Regardless, as Congresswoman Loretta Sanchez put it “lawyers will never carry the broad authority and legitimacy of a military commander.” And that is as true among the general public as it is within the armed forces itself.

7.) It will deprive commanders – unique in their experience and expertise – of a key tool in addressing sexual assault as a threat to military readiness.

Military readiness is a matter best addressed by military leadership, not staff lawyers. This is especially so when dealing with the intricacies of something so linked to readiness as sexual assault. For example, while commanders know that any sexual assault is a tragedy regardless of the gender of the victim, they nevertheless must deal with the popular narrative that assumes that most military sexual assault victims are female.

To be clear, if we accept the Pentagon’s extrapolation regarding the 26,000 oft-quoted number of estimated victims of “unwanted sexual contact” in 2012, the majority had to be what the New York Times calls “overlooked victims” -- men, not women. Although a 2010 survey conducted for the Air Force by the Gallup organization found that 61.3% of the men sexually assaulted were victimized by a female perpetrator, Gillibrand activist Susan Burke insists that the 2012 survey reflects “men raping men.”

Commanders are best positioned to deal with this complexity while recognizing that women, though comprising a minority of the estimated victims, have shown themselves much more willing to come forward with allegations of sexual assault. (Despite comprising only 47% of the estimated sexual assault cases, women account for 88% of the unrestricted reports that can initiate prosecution.)

Statements by politicians and others that suggest that women will be victimized if they serve in the military generate a threat to readiness that commanders must address. Their assertions, however mistaken, will naturally discourage women from joining. The military simply cannot afford to “write off” literally half the talent pool and expect to be ready to meet the demands of 21st century warfare. In addition to the readiness issue, commanders may also believe -- as experts do -- that solving sexual assault against women in the ranks involves increasing their numbers, something that their aggressive stance against sexual assault can only help.

In other words, the commander-led system has the flexibility – and, the broader expertise - to respond to the greatest threats to readiness than does a prosecutor-centric system.

Sen. Gillibrand’s proposal is flawed because the lawyers she wants to put in charge, (though no doubt expert legal technicians and earnest, competent officers) simply do not
have the broad-based experience in managing the larger issues of morale, discipline, and — ultimately — readiness that those who bear the mantle of command routinely experience. Attorneys, to include military lawyers, are also regulated by professional guidelines designed for a civilian setting and which do not easily accommodate the complex leadership challenges occasioned by what the Supreme Court calls the military’s status as “a specialized society separate from civilian society.”

In this context a commander’s broader experience in this “specialized society” permits a more nuanced and sophisticated application of disciplinary measures. And this is exactly what is needed in the fight against military sexual assault. For example, while the open service of gays in the military has, to date, been accomplished with relatively little turmoil under the commander-led disciplinary process Sen. Gillibrand wants to end, the upheaval caused by her bill could threaten that.

Challenges can still arise that demand a commander-led effort. Consider that one pundit has already claimed that “some evidence exists to substantiate the traditional concern…that open introduction of homosexuals into the military's intimate quarters will only aggravate sexual assault problems.” Whether he is accurate or not, command leadership needs to be at the center of a disciplinary process that has to address, as Gillibrand activist Susan Burke put it, “men raping men.”

Given the unusually sensitive political, social, legal, and operational issues associated with integration of gays openly serving in the military, it should be obvious that commanders — not staff lawyers — remain the ones best equipped to navigate and lead in this extraordinarily complex terrain. There simply could not be a worse time to remove commanders from their leadership position in the sexual assault disciplinary process than now.

Sen. Carl Levin, Chairman of the Senate Armed Services Committee, put it aptly:

> We cannot strengthen our efforts by weakening the authority of our commanders to act against sexual assault. Commanders were tasked again with making monumental those changes in military culture, from combatting racial discrimination in the 1950s to ending “don’t ask, don’t tell” in 2011. If we are to accomplish the change in military culture that we all agree is central to combatting sexual misconduct and sexual assault, commanders are essential. We cannot fight sexual predators if we make it more difficult to try and convict them. And we cannot hold our commanders accountable for accomplishing the needed change in culture if we remove their most powerful weapon in the fight
8.) It is in ‘denial’ about the fact that foreign militaries that removed the commander from the disciplinary process fail to show an increase in the number of sexual assault reports, and may have complicated prosecutions in a way that would be detrimental to the American military.

A cornerstone of Sen. Gillibrand’s argument for removing commanders from the disciplinary process is that victims allegedly do not trust commanders and, therefore, would be more likely to come forward under a prosecutor-centric system. She cites the handful of foreign militaries that have removed commanders as examples of the scheme she wants to impose upon American troops. Of course, the polls of U.S. troops and their families noted above show clearly that they do, in fact, trust their commanders, but as important on this issue is the data emerging about the foreign militaries she relies upon.

That evidence does not show that any of these foreign militaries have made any significant progress in halting sexual assaults. For example, “complaints of sexual harassment and assault in the [Israeli defense Forces] have increased by more than 80% in the past five years.” Canadian activists insist that their military is suffering from the same problem with sexual assaults that the U.S. military is facing, and media reports show that the Australian military is likewise dealing a myriad of allegations. As to the U.K, the Complaints Commissioner for British forces conceded in 2012 that she was “still unable to say that the Service [sexual assault] complaints system is working efficiently, effectively or fairly.”

More decisively, in a November 7, 2013 public hearing, the Response Systems for Adult Sexual Assault Crimes Panel established by Congress by Section 576 of the National Defense Authorization Act for Fiscal Year 2013 shows that Sen. Gillibrand is wholly mistaken about the impact of the removal of the commander from foreign military justice systems. Specifically, the panel said:

We...find that none of the military justice systems of our allies was changed or set up to deal with the problem of sexual assault, and none of them can attribute any changes in the reporting of sexual assault to changing the role of the commander. Lastly, we have seen or found -- we have found no evidence that the removal of the commander from the decision making process of non-U.S. military justice systems has affected the reporting of sexual assaults.

Furthermore, the impact on discipline in the U.S. military of the foreign systems would be very real and manifestly adverse. Consider that none of those relatively small militaries Sen. Gillibrand and her cohorts cite as prototypes for the American military have world wide security responsibilities comparable in size and complexity with those of the U.S.

In addition, none has been able to demonstrate that its lawyer-centric systems (which often involve civilian lawyers) are realistically deployable to combat zones as none -- despite more than a decade of war in Iraq and Afghanistan - has managed to complete a single trial in a combat theater. This has serious implications for the ability of any military justice system to address sexual assault.

The U.S. does not – and cannot go down the path advocated by the Gillibrand activists because the U.S. needs a ‘portable’ military justice system that can hold accountable
misbehavior in the field. As the Defense Policy Board concluded last May, while “good order and discipline [are] important and essential in any military environment, it is especially vital in the deployed environment. The military justice system is the definitive commander’s tool to preserve good order and discipline, and nowhere is this more important than in a combat zone.” It is that crucial tool thatSen. Gillibrand wants to take from the hands of the warfighters and give it to lawyers.

Additionally, because the foreign systems thatSen. Gillibrand lauds necessitate shipping miscreants home for criminal justice processing, it raises the obvious question: should sexual misconduct become an avenue out of a dangerous combat zone? Doing so erodes the deterrent value of having trials conducted in situ, and injures morale as the troops see accused get, in essence, a ticket home. Could it perversely incentivize sexual assault? We know that some soldiers can become so desperate to escape the terror of the front lines that they purposely injure themselves (hence the crime of malingering under military law). Could sexual assault become a new means of escaping a war zone? Do we want to find out?

It is also important to understand, as Sen. McCaskill clearly does, that those of “America’s allies that removed chain of command from these cases did so to better protect the rights of defendants—not the rights of victims.” In other words, if Sen. Gillibrand wants America to mimic foreign justice systems, doing so may well make it more, not less, complicated to vindicate victim’s charges, especially if the other features of foreign law are adopted. To be sure, we need to examine foreign law for possible good ideas, but it is simply incorrect to assume that these foreign countries facilitated sexual assault prosecutions by removing the commander from the disciplinary process.

In summary, there is zero evidence that removing the commander from the disciplinary process has done anything to help address the sexual assault problem in foreign militaries. Furthermore, these countries are left with highly civilianized military justice processes that have not demonstrated the world-wide utility of America’s commander-led system. What is crucial is that the U.S. military justice is effective in the vital deployed environment mainly because of the very commander involvement and focus thatSen. Gillibrand’s bill would eliminate.

9.) It will unnecessarily cost the military millions in scarce dollars, and will drain needed legal resources away from troops and their families.

It is a surprise to no one that the military is suffering from the unprecedented effects of sequestration and other budget cuts. That said, everyone would gladly spend the money to fund Sen. Gillibrand’s bill if it could really help military solve anything. The main problem is that it will not help; it will actually hurt the military’s efforts to combat sexual assault.

Plus, the cost to troops and this families for Sen. Gillibrand’s program is very real. According to General Ray Odierno, the Chief of Staff of the Army, Gillibrand’s bill is “detrimental to the military,” and it would also cost the Army “millions.” As already noted, informed estimates put the cost at $113 million for a staff of 600 lawyers and support personnel. Because there are no additional resources with her bill, the military will have to cut other programs to pay for it and to man it if enacted.
$113 million may not seem like much to some, but to military families, it matters a lot. For example, the National Military Family Association says that sequestration is forcing “$106 million in cuts in Impact Aid money that supports civilian schools educating military kids” Would it not be better to help the hundreds of thousands of military children than it would be to waste money on an unneeded and counterproductive bureaucracy?

Media reports also point out that commissaries, which are used by hundreds of thousands of active duty, retired, and National Guard personnel and their families, are suffering a $70 million cut. It is uncertain what additional cuts the military would need to make to fund Gillibrand’s bureaucracy, but what is clear is that in today’s military, $113 million is real money, and that military families are the ones who will likely pay the price. Again, should not our military households – who polls say do not want Congress changing military law - be considered?

What is more is that in an era of highly-constrained resources, Gillibrand’s bill does not provide for any additional military manpower for the 600-person lawyer-laden edifice she wants to build, and inevitably that will leave fewer military lawyers available for other duties. Make no mistake about it, the manning issue is a genuine issue for the military services. For example, 600 people represent about half of the entire legal capacity of the whole Marine Corps – officer and enlisted.

Put plainly, Sen. Gillibrand’s bill would mean fewer military lawyers would be available to counsel young servicemembers and their families on legal problems, fewer military lawyers to oversee multi-billion dollar procurements, and fewer military lawyers available to provide advice for warfighting commanders to ensure our actions are in compliance with international and domestic law. It cannot be overstated how valued military lawyers are to a range of essential duties, so their loss would be a serious blow to the clients on their already full agendas.

Moreover, those diverted resources do not even address the fact that the demands of the new bureaucracy would mean that fewer seasoned prosecutors, experienced defense attorneys, and victims’ attorneys with military justice expertise would be available to actually work on these cases. Quite clearly, morale, discipline of the overwhelming majority of military members as well as the military effectiveness of our armed forces would suffer.

10.) It is too tainted by bad data and the activities of “Washington-based advocacy groups with limited membership, participating in personal attacks, [and who] do not represent the views of all [sexual assault] survivors.”

Unfortunately, Sen. Gillibrand has relied upon bad data in making her proposal. For example, she credits the movie “Invisible War” with “shaping” her bill. However, experts have found it to be riddled with inaccuracies and unsupportable claims. One questioned whether it is “uninformed, dishonest, or both?” Most importantly, it has been slammed by some rape victims - yet it continues to be a centerpiece of the promotional efforts by Gillibrand’s supporters.

Interest groups have also distorted what should have been an open dialogue of all points of view. Regrettably, backers of Sen. Gillibrand’s bill include what Sen. Claire McCaskill characterizes as “Washington-based advocacy groups with limited
membership, participating in personal attacks, [and who] do not represent the views of all [sexual assault] survivors.” It is not surprising that such well-funded groups have inundated Congress with all kinds of propaganda, including much that could most charitably be described as “misleading.”

Furthermore, McCaskill’s reference to “personal attacks” is not an idle claim. Recently, Gillibrand advocates have sought to muzzle those within the armed forces who believe that a commander-led system better protects victims and would better preserve morale and discipline. What is disingenuous about that effort—which had no legal basis—is that Sen. Gillibrand herself says that the basis for her attack on the military justice system is what she says she heard from active duty victims. Should she not then also listen to those on active duty who think the commander-led system does do a better job for victims? Why try to muzzle those who disagree?

Perhaps Sen. Gillibrand and her supporters fear that as more facts emerge, and more analysis is obtained, the flaws in her proposal will become better known. This can be seen as she and her supporters are frantically trying to get legislation passed before a Congressionally mandated panel completes its work. As one observer put it: “[i]n what seems like a case of ready-fire-aim, Congress is rewriting military sexual-assault laws and policies without waiting for the recommendations of an expert panel that lawmakers themselves once deemed necessary.”

What is particularly disturbing is that the data that Sen. Gillibrand claims supports her proposal has become increasingly discredited. Lindsay Rodman, a brilliant young Marine captain with first-hand knowledge of how the Pentagon survey was conducted (which underpins Sen. Gillibrand’s contentions about the military justice system), has ripped its methodology in her Wall Street Journal op-ed. This Harvard-educated lawyer said “It is disheartening to me, as a female officer in the Marine Corps and a judge advocate devoted to the professional practice of law in the military, to see Defense Department leaders and members of Congress deal with this emotionally charged issue without the benefit of solid, verifiable data.”

Likewise, Paul Lavrakas, the president of the American Association for Public Opinion Research, was “troubled that three years of survey data produced such different estimates” and added that when “you see them jump around like that, the first thing that comes to mind is there’s something wrong with the numbers.” Because of the flawed data, Captain Rodman rightly fears that solutions from Capitol Hill “will only make things worse” for sexual assault victims.

NEEDED LEGISLATION THAT NO ONE IS PROPOSING

It is true that the fight against sexual assault would benefit from new legislation, and Congress could start with fixing the current law criminalizing sexual assault. Unfortunately, Congress’s recent record of tinkering with military sexual assault law is hardly encouraging. Its 2006 revision was so badly botched that one military judge quipped “If you had 100 monkeys with a typewriter, they’d probably come up with something like this.” Unsurprisingly, the all-civilian Court of Appeals for the Armed Forces gutted the law on Constitutional grounds.

The next effort—which came into effect in 2012—is also proving problematic. Disappointingly, Congress did not adopt the clear and easily understood definition of
rape that the Department of Justice announced (also in 2012): “The penetration, no matter how slight, of the vagina or anus with any body part or object, or oral penetration by a sex organ of another person, without the consent of the victim.” Instead, Congress imposed on the armed forces a complicated definition that, unlike the modernized Department of Justice definition, did not include “without consent.”

Thus, consent — as well as mistake of fact as to consent — is virtually eliminated as a defense in military cases, even though civilian jurisdictions typically provide just such a legal justification for sexual behavior. Military judges and others have tried various approaches to try to breathe a “consent” defense back into the law in an effort to preserve its legitimacy, but it remains to be seen if doing so is really Constitutional in the face of an explicit Congressional excision, as such judicial ‘legislating’ may — among other things - violate separation of powers doctrine.

Besides eliminating consent as a defense to sexual assault, Congress also eliminated the sexual component to certain constructs of what is chargeable as “rape.” For example, unlike the Department of Justice definition which criminalizes a form of rape as oral penetration “by a sex organ,” the definition Congress imposed upon the military defines the sexual act as including “the penetration, however slight, of the . . . mouth of another . . . by any object.”

The kind of intent required for completion of the elements of this form of “rape” under current military law is not something related to sexual gratification (or some other sexually-related mindset) as one might expect (and as is implicit in the Department of Justice definition), but with the sexually-neutral intent “to abuse, humiliate, harass, or degrade any person.”

What does all this mean? Factual situations manifestly underserving of characterization as the serious crime of “rape” could nevertheless be so designated because of flaws in Congress’s 2012 law. This does a real disservice to victims of rape (that is, as defined by the Justice Department), and the Gillibrand bill does nothing to remedy it.

For example, because of the “any object” language Congress put in the military definition of rape (as opposed to the “sex organ” language in the Department of Justice definition for rape involving oral penetration) someone throwing a pie in another’s face is a “rapist” if any portion of the pie penetrates the “mouth,” and it was thrown “with an intent to abuse, humiliate, harass, or degrade any person.”

Because of the lack of any required sexual intent, if today’s military law were in effect at the time and applicable to the perpetrators, it would make such improbable people as G. Gordon Liddy, Bill Gates, and (opponent of Sen. Gillibrand’s bill) Sen. Carl Levin, all “rape” victims because all were targets of a thrown pie. Is not calling this kind of behavior “rape” denigrating to true victims of the crime?

Think it could never be charged? Actually, there is no telling what prosecutors might charge. The Supreme Court is currently considering a case where a jilted wife is being charged with using a “chemical weapon” on her husband’s lover in contravention of Chemical Weapons Convention. A weapon of mass destruction? Not exactly given that the extent of victim’s injury was a simple thumb burn that was “treated” with “running water in the sink.”
Neverthelesss, this charge – which under state law would amount to little more than simple assault – was pursued by a Federal prosecutor under a similar system as that proposed by Sen. Gillibrand for the military. Additionally, if the law Congress imposed on the military in the 2012 law had been in effect in 1945, the sailor pictured in the iconic photo kissing the nurse in Times Square at the end of World War II could have found himself charged as a “rapist.” Boorish and even assaultive behavior? Maybe. But rape?

Clearly, it should not be possible for sexual assault victims, and particularly rape victims, to have their suffering trivialized by such an overbroad statute. Indeed, it is insulting to them. Yet Gillibrand’s bill does nothing to correct the obvious faults in current law.

Again, legislating the Department of Justice definition into the law would provide the clarity commanders and their military lawyers need to explain the prohibitions to the troops. It would also eliminate any ambiguity that might allow a rapist to escape punishment because of action an appellate court may find it needs to take on Constitutional grounds.

In addition, any legislation needs to ensure that those accused have their civil liberties protected, something that Sen. Gillibrand seems to overlook in her claim that her proposal is based on what accusers want. This is a special concern given reports of rising numbers of false accusations in the military. Unhappily, the system that Sen. Gillibrand wants the military to copy has produced hundreds of convictions which were proven wrongful by advances in DNA technologies.

What is more is that in the civilian setting people of color, to include principally African-Americans, have been disproportionately wrongly convicted by the kind of prosecutor-centric system Sen. Gillibrand wants for the military. Consider that African-Americans encompass just 13.6% of the U.S. population, yet FBI statistics show that they comprise 32.9% of those arrested by civilian authorities for forcible rape. Even though African-Americans are nearly three times more likely to be arrested by the kind of prosecutor-centric system Sen. Gillibrand wants for the military, it is also important to understand that they make up 61% of those exonerated by the Innocence Project (and another 9% are other people of color).

Military commanders are keenly attuned to threat of racial discrimination for many reasons. They know how critically important for morale and discipline – and, indeed, victory in combat – it is to ensure that unlawful discrimination does not devastate the comradeship and unit cohesion that military success requires. The imperative to keep the system free from discrimination is not simply a philosophical, idealistic, or legal requirement as it may be for Gillibrand’s proposed bureaucratic edifice; it is a matter of warfighting necessity for military commanders.

Finally, Congress ought to toughen the penalty for rape. It softened that penalty – to include even for child rape – by eliminating the death penalty even though it is not clear that doing so was Constitutionally mandated. There is a strong case to be made that retention of the death penalty for rape is crucially important for the armed forces because courts-martial may need to be used to try war criminals, to include especially those in an enemy force.

We have long known that rape in a wartime setting can involve motivations that could be very different than those that arise in a domestic, criminal law context. What makes
Congress’ relaxing of the penalties so frustrating is that they come at a time when we are seeing America’s enemies increasingly using rape as a weapon of war. Congress needs to restore the death penalty to military law so that it would be available, for example, for possible trials of future enemy war criminals. The death penalty could serve as a powerful deterrent to the use of rape as a weapon of war and, even if not deterring, it can serve justice for victims of such a horrific crime.

Instead of focusing on these urgently needed reforms, Sen. Gillibrand’s bill does nothing to address them. This is yet another reason why even those who believe the military justice system needs amendment ought to appreciate that any change must be the product of thoughtful, considered study and analysis (as is underway now by the panel Congress established) not simply highly-politicized machinations.

FINAL OBSERVATIONS

Military leaders know that taking the commander out of this disciplinary process will inevitably harm the warfighting effort. In 1947 then General Dwight D. Eisenhower warned about giving military justice authority to staff officers when he insisted that “there must be someone that is in the chain of responsibility, or the men in the field are not going to take it and like it.” He further warned (uncannily presciently given Sen. Gillibrand’s desire to substitute staff lawyers for commanders) that if “some staff officer with no responsibility for winning the war, who is not even subject to the supervision of the Secretary of War for the handling of this thing” acted in a military justice matter, “there is going to be resentment—and very deep resentment. I assure you there will be.” This is as true today as ever.

Sen. Gillibrand’s proposal is also flawed because it supposes that we can “prosecute” our way to a solution for sexual assault so endemic in society in general. We tried that approach with War on Drugs only to find, as Attorney General Holder recently said, that while we can be “coldly efficient in jailing criminals” our nation nevertheless simply “cannot prosecute or incarcerate” its way to personal safety. Let us not make the same mistake with the scourge of sexual assault.

In what is perhaps the most thoughtful commentary on this complex issue, Captain Rodman argues that what is needed is a “constructive dialogue on military sexual assault” and one that embraces the “gray areas.” This is needed, she says, to “shift the focus of the conversation away from the current self-perpetuating cycle of encouraging further prosecution to address a frustrating conviction rate.” Regrettably, that conversation is not taking place in Congress. As Rodman says, “[t]he agenda should be to identify the problem, to come up with a solution” and adds “That’s not what I see happening right now.”

To be sure, the ongoing Congressionally-mandated study will likely yield recommendations for changes in the military justice system. But until they have the opportunity to complete their work, there is no reason to jeopardize the ability of commanders to “provide for the common defense” through precipitous legislation that by its sponsors own assertion is not based on that most basic imperative. We must be sure we understand the unintended consequences of even the most well-meaned law. The security of the nation demands it.
Abstract: Military justice has never been intended as an exact replica of civilian justice. Historically, the need to maintain discipline under the enormous stress of combat and the high stakes of war impelled all militaries to create a separate and, in many ways, unique justice system. The result is a criminal law process in which military needs sometimes must take precedence over certain rights-centered formalisms of a nation's civilian justice system. However, beginning with the adoption of the Uniform Code of Military Justice in 1951, the two U.S. systems have become increasingly close, with the importation into the military realm of many of the procedural protections of the civilian system. Military justice retains its distinctive features, including the criminalization of absence, cowardice, and insubordination, as well as other offenses without civilian counterpart but which are indispensable for what the Supreme Court calls the armed forces' "separate society." In addition, some procedural differences continue to exist, including command selection of military "juries," as well as an appellate court system empowered to review de novo factual findings of a court-martial. Recently, the use of military commissions—which are separate from courts-martial—have been revised to address war crimes committed by nonstate actors. Today, issues have arisen about the ability of the military justice system to operate independently and effectively. In part, this is the result of well-intended efforts over several decades to "civilianize" and "judicialize" its
processes—modifications that have often proven ill-suited to combat zones. Even more problematic is the tendency of political leaders and interest groups to encroach on the role of commanders in military justice matters, and to inject other political influences that threaten the military justice system’s independence and effectiveness.

Groucho Marx, so the story goes, once quipped that “military justice is to justice what military music is to music.” To the distress of many in the armed forces, as well as to admirers of its justice system, that wisecrack continues to describe the military’s criminal jurisprudence in the minds of many Americans.

As with much humor, however, there is some truth in Marx’s jest. Just as military music has served a martial purpose for eons—trumpets did a pretty good job for Joshua and the Israelites at the battle of Jericho—so too has military justice served war fighters since virtually the beginning of organized conflict, because it plays a central role in establishing the discipline indispensable for martial success. In the Anabasis, Xenophon observed that “if discipline is held to be of saving virtue, the want of it has been the ruin of many ere now.” Maurice de Saxe, in his 1732 treatise on war, Mes Rêveries, contends that the “Romans conquered all peoples by their discipline. In the measure that it became corrupted their success decreased.” For his part, George Washington bluntly insisted that “discipline is the soul of an army. It makes small numbers formidable; procures success to the weak, and esteem to all.”

All of this suggests that military justice is not—and never has been—intended to be simply a doppelgänger for a civilian criminal justice system. Unlike its civilian counterpart, it is designed to help execute, if necessary, the difficult—and melancholy—task of getting human beings to kill, in the name of the state, and do so under circumstance where their opponents are bent upon doing the same to them. The current U.S. Manual for Courts-Martial (MCM) puts this stark purpose more delicately and rather more elliptically when it explains that “the purpose of military law is to promote justice, to assist in maintaining good order and discipline in the armed forces, to promote efficiency and effectiveness in the military establishment, and thereby strengthen the national security of the United
States."² Across nations, cultures, and time, military discipline has typically been unapologetically and, indeed, often necessarily, draconian. Throughout history, misbehaving soldiers have been punished in a variety of frightening ways, to include at times torture, maiming, and even summary execution. During the Revolutionary era, for example, the British army would impose punishments of up to one thousand lashes for relatively minor offenses.

In a way, it is not hard to understand why such harsh measures were needed: the tactics and weapons of the eighteenth century required troops to march shoulder to shoulder to within seventy-five yards of their adversary. At that point the infantrymen would fire volley after volley into the similarly packed ranks of their adversary to achieve the effect of mass fire with their oft-inaccurate muskets. Additionally, the crammed-together troops might also face withering exchanges of cannon fire from almost point-blank range. Anyone injured in such blasts faced, at best, the horrifying prospect of rudimentary medical care, including the high probability of amputation. It took uncompromising discipline to steel soldiers for this terrifying environment.

Given such verities, it is unsurprising that the Continental army adopted Britain’s military justice code, the Articles of War, with relatively few changes. That system, with periodic adjustments and improvements, largely persisted through World War II. In that conflict, which saw sixteen million Americans serving in uniform, over two million courts-martial of U.S. troops took place. Most of those trials were conducted without lawyers or legally trained personnel, and this and other deficiencies led to much criticism after the war. As one commentator put it,

Many of these citizens also had some very unpleasant experiences with the military justice system. At that time, the military justice system looked quite different than it does today and did not offer accused the protections afforded by the civilian courts system. It was a system that was foreign to many American citizens and they disapproved of the way criminal law was being applied in the military.³

To address these concerns, Congress passed major reform legislation in 1951 that replaced the Articles of War with the Uniform
abandoned the “service connection” test in favor of essentially “green card” jurisdiction (in reference to the then green identification cards that members of the armed forces carried). It reestablished personal jurisdiction in courts-martial based exclusively on the military status of the accused.

Perceptions about the supposed callousness of the system, and even questions about its legitimacy, continue to haunt military jurisprudence. As recently as 2009, Chief Justice John Roberts cited with approval the 1957 case of *Reid v. Covert* for the proposition that “traditionally, military justice has been a rough form of justice emphasizing summary procedures, speedy convictions and stern penalties with a view to maintaining obedience and fighting fitness in the ranks.” What is remarkable about his comment is that what is apparently believed to be a “rough form of justice” is, nevertheless, acceptable in the military of a democratic superpower.

Actually, the notion that the military system is a “rough form of justice” is not borne out by most objective analyses. A 2012 study by the Congressional Research Service amply demonstrates that military courts generally provide the same procedural safeguards as those found in civilian federal criminal trials. In a comparison to state court criminal proceedings using a hypothetical case arising in the state of Virginia as an example, two military attorneys found that in nearly every instance the armed forces provided as much as or more due process for a defendant. In particular, the greater resources available to military defense counsel were highlighted.

Rather ironically, it is not altogether clear that the founding fathers ever intended courts-martial to involve the elaborate procedures they employ today. For example, the Constitution specifically exempts the military from the Fifth Amendment requirement for a grand jury indictment. Furthermore, the Court in *Covert* observed that “it has not been clearly settled to what extent the *Bill of Rights* and other protective parts of the Constitution apply to military trials.” That 1957 dictum remains largely true today, as a CAAF judge explicitly noted in her 2005 dissent in *U.S. v. Mizgala*.17
Thus, it can be argued that the rights of service members in disciplinary matters are much dependent upon the largesse of Congress.\textsuperscript{18} As the Supreme Court said in the 1953 case of \textit{Burns v. Wilson}:

The rights of men in the armed forces must perforce be conditioned to meet certain overriding demands of discipline and duty, and the civil courts are not the agencies which must determine the precise balance to be struck in this adjustment. The Framers expressly entrusted that task to Congress.\textsuperscript{19}

However, for its part, CAAF claims rather inexplicably that “the Supreme Court has assumed the Bill of Rights applies to the military” and insists it applies “absent military necessity or operational needs.”\textsuperscript{20} As a practical matter, the effectiveness—and fairness—of the system depends upon those who practice in it. These are principally military lawyers called JAGs (the acronym for their formal title of “judge advocates”). JAGs are not just licensed lawyers, but today are among the best and brightest the legal profession has to offer; in recent years only one in twenty applicants has been accepted by the service JAG corps.

Once a lawyer is licensed in a U.S. jurisdiction and commissioned into one of the services, the UCMJ requires the judge advocate general (the senior lawyer of each of the services) to certify the individual as competent to defend persons in courts-martial. In addition, the judge advocate general of each of the services has statutory responsibilities to supervise his assigned JAGs and to provide oversight of the administration of military justice throughout the armed forces. As a check on abuses in the field, JAGs are entitled by law to communicate directly with senior JAGs, notwithstanding any efforts by field commanders to the contrary.\textsuperscript{21}

Many offenses prosecuted in the military justice system involve the same sort of crimes (e.g., assault, larceny, DWI) denounced in any criminal code. Indeed, the third clause of Article 134 of the UCMJ (the “catchall” article\textsuperscript{22}) permits the assimilation of virtually the entire federal criminal code into military law. There are, however, limits to integrating civilian law into the code. In the 2012 case of \textit{U.S. v. Hayes}, CAAF refused to permit bootstrapping \textit{state} criminal codes into the UCMJ.\textsuperscript{23}
Even among “conventional” offenses there are some differences based on the special considerations of military service. For example, Article 134 criminalizes deaths that are the result of simple negligence, a standard of culpability commonly found in civil lawsuits but not in the criminal courts. In the 1979 case of *U.S. v. Kick*, the Court of Military Appeals explained,

There is a special need in the military to make the killing of another as a result of simple negligence a criminal act. This is because of the extensive use, handling and operation in the course of official duties of such dangerous instruments as weapons, explosives, aircraft, vehicles, and the like. The danger to others from careless acts is so great that society demands protection.24

Of course, the UCMJ contains a variety of offenses that are unique to the military. Absence offenses are a good example. Desertion—which is quitting one’s post with the intent to stay away permanently—carries the death penalty if done in time of war. Quite obviously, no armed force can tolerate troops abandoning their duties, especially in the face of combat. Lesser absences are also criminalized. In the military, being even a minute late for work during peacetime is a crime punishable by up to a month in jail. Of course, that measure of punishment is rarely imposed, but “failure to repair” (as lateness is termed in the military) commonly results in an administrative forfeiture of pay or even a reduction in rank.

The criminalization of absence offenses is one illustration of how the UCMJ helps create a mind-set of obedience and attention to detail that is so necessary for success in war. Another example—and one that often perplexes civilians—is dereliction of duty. There are several dereliction offenses, depending on whether the failure to execute an assignment was willful, negligent, or the result of culpable inefficiency.

The MCM does, however, make it clear that when the failure to complete that task is genuinely the result of inability—such as when a soldier repeatedly fails to pass his marksmanship test despite earnest effort—he is not criminally liable (although he may find himself required to put in many extra hours of practice, to include time that
otherwise might have been off-duty). Still, when a military member’s failure to do his duty is, in fact, willful or negligent, then the punishment is more severe than for someone who fails to complete a project for a civilian company or organization.

The UCMJ also lists a number of offenses designed to help control the natural terror that combat can produce in individuals. Besides desertion in wartime, capital punishment may also be imposed for behaviors that may seem rather innocuous or even inexplicable to civilians, but is understandable given the paramount interests of a military organization at war. Thus, “sleeping on post,” failing to do the “utmost” to “encounter the enemy,” and “shamefully” surrendering are all death penalty offenses. Additionally, execution is authorized for “cowardly conduct,” which the MCM defines as “misbehavior motivated by fear.”

To be sure, a serviceman’s mental state can exonerate him if—as is typical in civilian jurisprudence—he suffers from “a severe mental disease or defect” and as a result of that he is “unable to appreciate the nature and quality” of the act or its “wrongfulness.” Post-traumatic stress disorder (PTSD), for example, does not, per se, excuse misconduct, absent a showing it has the effect discussed above; it may, however, be raised as a matter of mitigation of any sentence.

Despite the rather large number of UCMJ offenses that carry the death penalty, no service member has been executed since 1961. Six soldiers are currently on death row at the U.S. Disciplinary Barracks in Fort Leavenworth, Kansas, but none is there for a conviction for uniquely military offenses; all are sentenced for crimes that include premeditated murder as at least one of the charges.

The armed forces necessarily place a premium on the obedience of orders. In the 1890 case of In Re Grimley, the Supreme Court noted that an “army is not a deliberative body.... [Its] law is that of obedience. No question can be left open as to the right to command in the officer, or the duty of obedience in the soldier.” In the 1983 case of Chappell v. Wallace, the Court was equally unambiguous when it said, “The inescapable demands of military discipline and obedience to orders cannot be taught on battlefields; the habit of immediate compliance with military procedures and orders must be virtually reflex, with no time for debate or reflection.”
Nonetheless, military law imposes no obligation to obey an unlawful order. Although all orders are presumed lawful, and soldiers disobey them at their peril, there are limits to the "orders" defense. In the infamous Vietnam-era My Lai massacre case, Army lieutenant William Calley claimed his murderous behavior was in response to superior orders he had allegedly received. The Court of Military Appeals, after noting that Calley was "convicted of the premeditated murder of 22 infants, children, women, and old men" who were his prisoners, rejected out of hand the assertion that Calley's intelligence was such that he might not have known that the supposed order was unlawful. The court dryly observed that "whether Lieutenant Calley was the most ignorant person in the United States Army in Vietnam, or the most intelligent, he must be presumed to know that he could not kill the people involved here."31

However, when an order is not actually unlawful, the fact that it may be unreasonable or contrary to one's personal belief does not excuse disobedience. Indeed, the MCM explicitly states that the "dictates of a personal conscience, religion, or personal philosophy cannot justify or excuse the disobedience of an otherwise lawful order."32 Thus, in U.S. v. Rockwood, an Army captain's conviction for offenses related to his departure from his base against his superior orders during the 1994 Haiti relief mission was sustained on appeal despite his claim that he had a moral and legal obligation under international human rights law to inspect the admittedly deplorable conditions of Haiti's National Penitentiary.33 Such decisions, the court found, were the prerogative of command, not of individual subordinate soldiers.

Among the more fascinating aspects of the UCMJ are the provisions related to commissioned officers. Subordinates can be punished not just for disobeying officers, but also for being disrespectful in acts or language. In this regard, the MCM pointedly states that "truth is no defense." At the same time, however, officers are held accountable in ways enlisted personnel are not. In finding that officers can be sent to trial for offenses that are typically handled administratively when involving enlisted personnel, the CMA observed that
the Armed Services comprise a hierarchical society, which is based on military rank. Within that society commissioned officers have for many purposes been set apart from other groups. Since officers have special privileges and hold special positions of honor, it is not unreasonable that they be held to a high standard of accountability.\textsuperscript{34}

One of the special restrictions placed on officers is the prohibition in Article 88 against “contemptuous words” against the president, the secretary of defense, and other civilian officials. Though the MCM cautions that “private conversations should not ordinarily be charged” and that adverse criticism “even though emphatically expressed” ordinarily should not be alleged, speech is criminalized in a way that would be unconstitutional in civilian society.\textsuperscript{35}

In one of the rare instances where an Article 88 violation was prosecuted, Lieutenant Henry H. Howe was convicted for attending a demonstration in 1965 in El Paso, Texas, while carrying a sign that said “LET’S HAVE MORE THAN A ‘CHOICE’ BETWEEN PETTY, IGNORANT, FASCISTS IN 1968” and, on the other side, “END JOHNSON’S FASCIST AGGRESSION IN VIETNAM.” The CMA upheld the conviction against First Amendment challenges, finding that what Article 88 properly sought to “avoid is the impairment of discipline and the promotion of insubordination by an officer” and that under the circumstance the conduct constituted “a clear and present danger to discipline within our armed services.”\textsuperscript{36}

Unlike Article 88, which is rarely alleged, Article 133—which denounces “conduct unbecoming an officer and a gentlemen”—is not infrequently included on charge sheets involving officers. In another Vietnam-era case, \textit{Parker v. Levy}, the Supreme Court examined whether “conduct unbecoming an officer” was too vague a standard to which to attach criminal liability.\textsuperscript{37} Levy, an Army doctor and commissioned officer, was convicted for making statements to enlisted troops such as that he did not “see why any colored soldier would go to Viet Nam: they should refuse to go to Viet Nam and if sent should refuse to fight” and that “Special Forces personnel are liars and thieves and killers of peasants and murderers of women and children.”
In rejecting Levy’s habeas corpus petition,38 the Supreme Court observed that it had “long recognized that the military is, by necessity, a specialized society separate from civilian society” and that the “military has ... by necessity, developed laws and traditions of its own.” Those differences, the Court said, arose from the fact that “the primary business of armies and navies is to fight or be ready to fight wars should the occasion arise.”

Thus, the Court believed that notwithstanding the broad language of Article 133, Levy could have no reasonable expectation that using the words he did under the circumstances would be anything other than violative of the UCMJ provision. In so concluding, the Court pointed out that the “fundamental necessity for obedience, and the consequent necessity for imposition of discipline, may render permissible within the military that which would be constitutionally impermissible outside it.” Today, Article 133 charges often incorporate the elements of a wide range of offenses, to include relatively minor ones. Although prosecutors are required to prove the additional element that the misconduct was “conduct unbecoming an officer,” any conviction permits the dismissal of the officer (the equivalent of a dishonorable discharge for an enlisted person).

Of course, not all violations of the UCMJ automatically result in a court-martial. Commanders are urged to attempt to resolve misbehavior at the lowest possible level, and most disciplinary measures are administrative, not judicial. For example, commanders and supervisors will employ corrective measures to include oral and written counselings, admonitions, and reprimands. For the vast majority of troops, these administrative tools are sufficient for correcting behavior.

More aggravated situations, yet still “minor offenses,” can be handled by a commander via a nonjudicial procedure under Article 15 of the UCMJ.39 These are summary administrative proceedings, often conducted by commanders without the involvement of legal personnel, that permit the imposition of limited fines, restrictions, extra duties, and—where facilities are available—correctional custody. Correctional custody is designed to be akin to confinement, but more of a reversion to the strict regime of boot camp in order to reinstill military virtues in the offender and return him to duty. (It
is reported that punishment pursuant to Article 15 is what is being recommended in the December 2011 incident involving the burning of Korans in Afghanistan. In cases where an individual is deemed unsuitable for further service, but not for reasons warranting a court-martial, administrative discharge may be directed.

If a particular disciplinary situation appears to warrant more than administrative disposition, criminal charges are “preferred” on the accused as the first step in the court-martial process. While military law permits any person “subject to the Code” to prefer charges, it usually falls to the immediate commander to do so. Depending upon the seriousness of the allegation, the commander may decide—with the advice of his or her JAG—to dismiss the charges or to resolve them administratively. The commander, if authorized to convene courts-martial, can also “refer” the case to a summary or special court-martial. If, however, the charges are serious enough, he may order a formal investigation pursuant to Article 32 of the UCMJ.

Article 32 investigations are often considered to be a statutory substitute for the grand jury process, even though the Constitution explicitly exempts military cases from that requirement. In practice, Article 32 hearings are much different from grand jury proceedings in that they are usually public proceedings with the accused present and accompanied by counsel. The accused (or, more likely, his lawyer) is permitted to interrogate government witnesses and call his own.

In many ways, the Article 32 hearings have evolved into mini-trials where allegations are sometimes “litigated,” even though the hearings are, technically, merely investigations. The hearing officer, ordinarily a JAG, will draft a report that will be forwarded to the commander along with the assembled evidence and transcripts of testimony. The hearing officer will make a nonbinding recommendation as to how the charges should be resolved.

Several types of courts-martial exist to which a commander can refer charges: summary, special, and general. They are mainly distinguished by the maximum punishments that can be imposed. A summary court can jail a soldier for thirty days, but not impose a discharge. A special court-martial can confine a defendant for up
to a year, and the sentence can include a bad conduct discharge. A general court-martial can adjudge any punishment up to the maximum authorized for the crime, to include death and a dishonorable discharge. Besides the stigma attached to a "bad conduct discharge" and a "dishonorable discharge" (called a "dismissal" when imposed upon an officer), these punitive separations can cause the loss of eligibility for many federal and state veterans' benefits.

The court-martial itself draws much from civilian trial processes. One key difference is that the "jurors" (called "members" in military parlance) are not randomly selected, as they generally are in civilian cases, but rather selected by the commander, based, as the UCMJ requires, on a determination that the officers are "best qualified by reason of age, education, training, experience, length of service, and judicial temperament." Though the concern is often understandably raised that a commander could "pack" a court panel to achieve a desired result, in practice such is rarely the case.

There are a number of reasons for this, beginning with the fact that the independence of the officers selected (the panel may include up to one-third enlisted members if an enlisted accused so requests) is protected by Article 37 of the UCMJ, which prohibits any effort to coerce or unlawfully influence the members or, for that matter, the military judge or counsel for either side. In addition, the appellate courts, and especially CAAF, have been exceptionally rigorous in their effort to root out "unlawful command influence," which it has long condemned as the "mortal enemy of the military justice system."

Court-martial panels also differ from most civilian courts in their size, as well as the manner in which they come to their findings. Summary courts-martial consist of a single officer, while special courts need at least three members, and general courts must have at least five. If the accused does not choose to be tried by military judge alone, his case will be decided by a secret written ballot of the members during their closed deliberation. In military cases, however, a conviction requires only a two-thirds agreement of the panel; there are no "hung juries" in military trials. In addition, the sentence also is decided by the members (if the accused does not elect trial by military judge
alone). Like the finding, a sentence requires a two-thirds vote, unless the sentence includes confinement for more than ten years (requiring a three-fourths vote) or death (unanimous agreement is mandated).

Besides incarceration, military sentences can include reprimands, fines and forfeiture of pay, hard labor without confinement, reduction in grade, and a punitive discharge. Although not yet tested for constitutionality, death is the only authorized punishment for spying in violation of Article 106 of the UCMJ. Other military death penalty cases usually require procedures similar to those found in civilian jurisprudence, including the presentation of aggravating factors.

The appellate process for court-martial convictions is more elaborate than that typically available in civilian settings. Although its extent largely depends upon the severity of the punishment imposed, it typically begins with review by the commander who convened the court-martial. That review, aided by the advice of a judge advocate, cannot result in a reversal of acquittal to any charge or any increase in sentence, but only in the approval of the adjudged findings and sentence, or a mitigation of either in some way.

Again, depending upon the severity of the sentence, the next level of review ordinarily is conducted by the court of review of each individual service. What is unusual about these courts is that they are empowered not only to act on errors of law, but also to conduct a fresh (de novo) review of the facts and overturn the case—even in the absence of legal error—if they find the proof insufficient. Moreover, they may reassess the appropriateness of the sentence and diminish it if they wish. Essentially, they can only affirm the decision or act in some way to the defendant’s benefit.

The next level of appeal is to the Court of Appeals for the Armed Forces. As already noted, the CAAF is empowered to review only errors of law (except in the Coast Guard, the judges in service courts of review are military appellate judges). Unlike the service courts of review, however, CAAF’s powers are limited to errors of law. Beyond CAAF, appeal can be made to the Supreme Court,
but only in limited circumstances. As the Congressional Research Service put it,

[The Supreme Court's] power to review military cases generally extends only to cases that the CAAF has also reviewed. For this reason, the CAAF's discretion over the acceptance or denial of appeals often functions as a gatekeeper for military appellants' access to Supreme Court review. If the CAAF denies an appeal, the U.S. Supreme Court will typically lack the authority to review the decision. In contrast, criminal appellants in Article III courts have an automatic right of appeal to federal courts of appeals and then a right to petition the Supreme Court for review.\textsuperscript{44}

An issue related to military justice—but very separate—is the matter of military commissions. Military commissions have a long history in the United States. They were used during the Mexican War, and thousands of Americans were tried by military commission during the Civil War, including anti-Lincoln conspirators. However, in 1866 the Supreme Court in the case of \textit{Ex Parte Milligan} found unconstitutional the domestic use of military commissions against nonbelligerents in areas where the courts were still functioning.\textsuperscript{45}

During World War II, civilians in Hawaii were tried by military tribunals under the authority of the Hawaii Organic Act, which permitted declarations of martial law. However, the Supreme Court applied its \textit{Milligan} precedent in finding that despite the statutory authorization, such trials were unconstitutional where U.S. civilian courts were able to function.\textsuperscript{46}

Nevertheless, when German saboteurs—including a naturalized American citizen, Herbert Haupt—were delivered to U.S. shores by a Nazi submarine in 1942, the Court distinguished \textit{Milligan}. In denying the saboteurs' petition for habeas corpus, the Supreme Court concluded in \textit{Ex Parte Quirin} that "those who, during time of war, pass surreptitiously from enemy territory into our own, discarding their uniforms upon entry, for the commission of hostile acts involving destruction of life or property, have the status of unlawful combatants punishable as such by military commission."\textsuperscript{47}
As to the American citizen among the saboteurs, the Court said:

Citizenship in the United States of an enemy belligerent does not relieve him from the consequences of a belligerency which is unlawful because in violation of the law of war. Citizens who associate themselves with the military arm of the enemy government, and with its aid, guidance and direction enter this country bent on hostile acts are enemy belligerents within the meaning of the Hague Convention and the law of war.

Those “consequences” included being subject to trial by a military commission. Six of the eight—including Haupt—were executed within weeks of their conviction.

Following World War II, General Tomoyuki Yamashita, the Japanese commander in the Philippines, where horrific atrocities were committed by his troops, was tried by military commission. Charged not with personally committing or ordering war crimes, but rather with “unlawfully disregarding and failing to discharge his duty as a commander to control the acts of members of his command by permitting them to commit war crimes,” he was tried and convicted by military commission. In denying his application for leave to file a petition for a writ of habeas corpus and writ of prohibition, the Supreme Court found his commission trial lawful, even though hostilities had ended. Yamashita was hanged on February 23, 1946.

The case has been widely criticized, but still stands for the important principle of command accountability, respondeat superior, the concept that commanders are responsible for the actions of their subordinates. Today, command responsibility incorporates requirements for some “information of knowledge that triggers a duty to act” with respect to “ongoing or anticipated law of war violations by subordinates,” as well as a “causal relationship between the commander’s omission and the war crimes committed by the subordinate.”

In the aftermath of 9/11, military commissions took on something of an unprecedented role when President George W. Bush issued his “Military Order” concerning detention of terrorism suspects,
as well as their potential trial by military commission.\textsuperscript{50} It seems as if the design for the commission process used an improved version of the much-respected Nuremberg trials as the template. Those proceedings were not, however, military commissions conducted under U.S. law, but rather were international tribunals.

Regardless, it is doubtful that the processes used at Nuremberg could survive scrutiny today (e.g., the Nuremberg defendants did not have the right to remain silent, or challenge the impartiality of the fact-finding judges). Indeed, William Shawcross argues that Nuremberg offered defendants fewer rights than did the military commissions created by the Bush administration. According to Shawcross, any “German in the dock at Nuremberg would be astonished to learn of his rights, privileges, and entitlements, if he were suddenly transferred by time machine to the court in Guantanamo.”\textsuperscript{51}

In any event, in 2006 the Supreme Court in \textit{Hamdan v. Rumsfeld}\textsuperscript{52} held that the military commissions devised by President Bush violated both the UCMJ and international law. This generated a number of statutory and regulatory changes, which ended with the implementation of the Military Commission Act of 2009.\textsuperscript{53} Although some scholars remain dissatisfied with commissions as formulated today,\textsuperscript{54} a comparison with courts-martial under the UCMJ suggests that the commissions are generally on firm legal footing, even as issues such as the scope of the charges triable by military commissions persist.\textsuperscript{55}

While courts-martial remain distinct from military commissions, an issue has emerged with them that relates to a fundamental concern of the commission cases: When can military authorities try a civilian who is not an enemy belligerent? As Professor Stephen I. Vladeck points out, “The Supreme Court repeatedly recognized categorical constitutional limits on the military’s power to try civilians (including contractors), at least during ‘peacetime.’”\textsuperscript{56} Additionally, Vladeck notes that the CMA invalidated trials of contractors during the Vietnam War: because the conflict was never formally "declared" a war, it did not fit the statutory construct permitting the trial of “civilians accompanying the force” as provided by the UCMJ.\textsuperscript{57}
However, after a foreign contract employee of the Army assaulted another contract employee in Iraq in 2008, the alleged offender found himself tried by a U.S. court-martial. In discussing jurisdiction, the Army court of review observed that the law had changed since the Vietnam-era cases:

In 2006, Congress amended Article 2(a)(10), which had long authorized UCMJ jurisdiction over “persons serving with or accompanying an armed force in the field” during “time of war.” This amendment was effected by replacing the temporal requirement of a “time of war” with “time of declared war or contingency operation.”

Because of the statutory revision, the Army court concluded that since the incident occurred at an overseas combat outpost during actual hostilities, court-martial jurisdiction was properly found. CAAF agreed and affirmed the conviction, but the case is likely to make its way to the Supreme Court.

Military law today is a well-developed corpus of jurisprudence, but one not without controversy. Incidents from the wars in Iraq and Afghanistan indicate an erosion of discipline. Allegations that soldiers engaged in the killing of civilians for “sport” in 2010 were followed by accounts in late 2011 and 2012 of other acts of indiscipline, including reports of troops burning Korans, urinating on Taliban corpses, and posing with body parts of enemy fighters, not to mention the shocking allegations of the cold-blooded murder of seventeen Afghans civilians by a U.S. Army sergeant.

Senior military officers and defense officials admit they are deeply troubled by the events, because they keenly understand the destructive effect of indiscipline on the military's ability to accomplish its mission. Secretary of Defense Leon Panetta told troops recently that “these days, it takes only seconds for one picture to suddenly become an international headline ... and those headlines can impact the mission we’re engaged in, they can put your fellow service members at risk, they can hurt morale, and they can damage our standing in the world.”

Panetta is echoing a point that former commandant of the Marine Corps General Charles C. Krulak made in 1999: that given
the enormous power of instant, worldwide media, every act carries potentially strategic consequences, even those committed by very junior troops in remote locations. Krulak presciently explained,

In many cases, the individual Marine will be the most conspicuous symbol of American foreign policy and will potentially influence not only the immediate tactical situation, but the operational and strategic levels as well. His actions, therefore, will directly impact the outcome of the larger operation; and he will become ... the Strategic Corporal.68

Clearly, misconduct can have a real effect on operational success in the twenty-first century. Many defense strategists cite the collapse of discipline that led to the detainee abuse scandal at Abu Ghraib as one of the worst setbacks the U.S. armed forces suffered since 9/11, much because of the propaganda victory that it handed the insurgents. General David Petraeus has said that “Abu Ghraib and other situations like that are non-biodegradable. They don’t go away. The enemy continues to beat you with them like a stick.”69

There can be many explanations for erosion in discipline, but one aspect may be the military justice system itself, and the outcome of the 2005 Haditha incident in Iraq could be illustrative. This case arose from a situation where twenty-four innocent Iraqi civilians were killed by U.S. Marines in a botched response to an improvised explosive device attack on a convoy. Of the eight original suspects, six had charges dropped, one was tried and acquitted, and the last accused—Staff Sergeant Frank Wuterich—negotiated a plea agreement in 2012 that limited his punishment to a demotion but no jail time. Many military justice experts were at a loss to explain the apparent leniency in his case, as well as the apparent inability to convict any of the others allegedly involved.70

However, the complex evidentiary rules—almost identical to those applicable in the most staid federal courtroom in an American suburb—may have also played a role. The New York Times reported that beyond missteps by military prosecutors and a reluctance of decision makers to second-guess the actions of troops in combat, “collecting physical evidence and finding witnesses can be difficult
because the killings often occur in unstable and dangerous areas, and the cases often come to light only after time has passed.\textsuperscript{71} It is no surprise, therefore, that after reports of the killing of seventeen Afghan civilians in March 2012, CNN reported that “critics are questioning the military’s ability to conduct the transparent, speedy investigation demanded by Afghanistan in the case.”\textsuperscript{72}

Decades of “civilianizing” and “judicializing” of the military justice system may have altered the system beyond what the Constitution would require for military jurisprudence, and certainly far beyond the “rough justice” of Chief Justice Roberts’s belief. Indeed, as suggested above, the process today may be too cumbersome and complex for the battlefield environments where it is needed to function.\textsuperscript{73} Major Franklin Rosenblatt presents a disturbing picture of the current situation in a 2010 article, “Non-Deployable: The Court-Martial System in Combat from 2001–2009.”\textsuperscript{74} According to Rosenblatt, “After-action reports from deployed judge advocates show a nearly unanimous recognition that the full-bore application of military justice was impossible in the combat zone.”\textsuperscript{75}

Rosenblatt cites a catalog of reasons for the troubles in applying the UCMJ in remote areas, ranging from logistical difficulties to procedural shortcomings to attitudinal issues, and warns that “deployed courts-martial may someday become a relic of military history rather than a viable commander’s tool.”\textsuperscript{76} Saddling commanders in austere locations with adhering to many of the same intricacies of a domestic judicial system may be proving to be too much. Lieutenant Colonel Michael Stahlman, a Marine JAG, admits that “commanders often perceive the military justice system as a roadblock instead of an effective leadership tool.”\textsuperscript{77}

Whether UCMJ complexities and burdens are the cause or not, it appears that commanders may be avoiding taking the disciplinary action they should, and this can create a dangerous attitude among the troops. In fact, a new Army report suggests commanders are “opting out” of the system:

The rise in crime in contrast to the decline in disciplinary action (e.g., court martial, summary court martial, Article 15), retention of multiple felony offenders and the deliberate change in terms of reference
regarding criminal misconduct all point to a softening in the perception of criminality. Subtle changes in policy language (e.g., removing the term “criminal” from “serious criminal misconduct”), which may inadvertently shift leader perception of criminality, will not change the nature of the criminal act or alter its impact on victims, good order and discipline, and unit readiness.\footnote{78}

Still, some experts insist that the system can work, even in the field. In a recent article, Major E. John Gregory cites his own Army experiences in Iraq and argues that they demonstrate that

when a proper emphasis is placed on military justice in theater by both the command and military justice practitioners, the court-martial system is a fully deployable system of justice which is not overly burdensome, meets the command’s disciplinary needs, and is highly protective of an accused’s rights.\footnote{79}

Encouraging words for sure, but the trick is obtaining the “proper emphasis” under circumstances where there are multiple operational demands on a commander’s time and resources. The answer is not, however, to ship miscreants home, as some have suggested, but rather to examine the “civilianized” processes to determine which ones are truly constitutionally required—or prudent normatively—and streamline the system accordingly to make it compatible with the needs of discipline in the twenty-first century.

The ability to impose discipline, in situ, is vitally important to any military organization in combat, as otherwise misconduct can become a ticket out of a war zone. At the height of the Vietnam War in 1968, a court-martial was conducted in an underground bunker at Khe Sanh. As recorded by Gary Solis in his masterly Marines and Military Law in Vietnam: Trial by Fire, all the proceedings were conducted as the enemy poured intense artillery, rocket, and mortar fire onto the isolated outpost.\footnote{80} The court-martial acquitted the accused of smoking marijuana, but convicted him of sleeping on post and sentenced him to reduction in grade and forfeitures. The prosecutor aptly noted that the “sentence was appropriate” because the “accused was not sent back to the brig or otherwise allowed to escape the confines of Khe Sanh.”\footnote{81}
Interestingly, some nations—including especially heirs to the British military justice system—are increasingly civilianizing their systems even more than the United States has done, often with reference to resolving military disciplinary matters in civilian courts.\textsuperscript{82} Casting cases to civilian courts does not, however, necessarily provide the desired justice. Consider the case of former Marine sergeant Jose Luis Nazario.

Although retired military members may be subject to court-martial, military jurisdiction generally terminates at the end of an enlistment or when a military member is otherwise discharged without retirement.\textsuperscript{83} Thus, Nazario, who was discharged before allegations related to the killing of four civilians in Iraq were resolved, had to be tried in a civilian court. Following his acquittal in 2008, news reports related that “several jurors acknowledged that they also did not feel qualified to judge a Marine’s actions in the midst of a battle.”\textsuperscript{84} One juror said “she hoped the verdict would send a message to the troops in Iraq” to the effect that they would “realize that they shouldn’t be second-guessed, that we support them and know that they’re doing the right thing.”\textsuperscript{85}

Another challenge to the military justice system today relates to the handling of sexual assault allegations. In 2006, Congress, spurred primarily by heartrending but anecdotal claims of mishandled cases, and dissatisfied with the military’s efforts to address these alleged incidents, revised the sexual assault offense found in Article 120 of the UCMJ. The result was such a bloated and confusing statute that in 2011 CAAF found key provisions unconstitutional,\textsuperscript{86} necessitating a complete legislative replacement (which itself may be subject to challenge).\textsuperscript{87}

The military’s difficulty in dealing with sexual assault cases may seem to be a manifestation of the victimization of women in an organization overwhelmingly populated by males (women compose only 14.6 percent of the 1.4 million active-duty service members\textsuperscript{88}). The \textit{New York Times}, for example, claims that it “is even harder for military women to get away from abusers they work with or for; they can’t just quit their jobs or leave a combat zone.”\textsuperscript{89} This misperceives the issue. A 2010 Department of Defense study did show that a higher \textit{percentage} of women (4.4 percent) than men (0.9 percent)
reported "unwanted sexual contact." However, the translation of those percentages into actual numbers shows that considerably more men (approximately 11,288) perceived themselves as victims of "unwanted sexual contact" than did women (approximately 9,433).

The armed forces have made an extraordinary effort to crack down on sexual assaults, establishing a web of victim's resources, special policies and reports, training, and—significantly—an increased emphasis on prosecution. However, criticism—especially in Congress—continues unabated. Accordingly, further legislation is now before Congress, a proposal called the "STOP Act." This legislation has a number of features, including the establishment of a Sexual Assault Oversight and Response Council, separate from the military chain of command, who would, in turn, appoint a "director of military prosecution" with authority over sexual offenses in the armed forces.

This proposal to remove field commanders from acting in this particular class of offenses is controversial. Army major general Gary Patton, the newly appointed head of the military's Sexual Assault Prevention and Response Office, warns that "if you were to take the disciplinary component and put it into some external, centralized, whatever, body, independent, apart from the chain of the command, you've just removed the commander from the problem and tied the commander's hands." His predecessor, Air Force major general Mary Kay Hertog, agreed with having more senior commanders take the initial action in these cases but added,

Some have argued that allegations of sexual assault are best addressed outside the chain of command. I disagree.... [Keeping the] initial disposition of these cases within the military chain of command ... will ensure that the military itself remains responsible for addressing this critically important issue. Experience has shown time and again that strong internal leadership is effective in bringing about major change. The chain of command must ensure justice and be held to account for the consequences.

Furthermore, the STOP Act proposal seems to assume that the military's difficulties with sexual assault prosecution are somehow uniquely the result of command indifference (or worse). Indeed, in
its proposed “findings,” the STOP Act does cast aspersions on military officers by stating that the “great deference afforded command discretion raises serious concerns about conflicts of interest and the potential for abuse of power.” However, the American public—if not Congress—rates military officers second only to nurses as the profession having the highest honesty and ethics. *(Members of Congress were rated the lowest.)* Similarly, an April 2012 poll showed the U.S. public had the most confidence in military leaders, and the least in those of Congress. *Thus, whatever negative view Congress may have as to the potential for abuse by military commanders, it would not seem to be shared by the public.*

Moreover, the military’s challenges with sexual assault cases are hardly unique: the Department of Justice, while citing increasing civilian prosecutions, concedes that in the United States generally, “sexual assault cases have been underreported and had low prosecution rates.” In any event, reports in December 2011 indicate that “military commanders sent about 70 percent more cases to courts-martial that started as rape or aggravated sexual-assault allegations than they did in 2009.” Additionally, Reuters reported in August 2012 that military “commanders routinely lack sufficient evidence to prosecute [sexual assault] cases.”

Importantly, as in any justice system, it is a “fundamental right” of a service member to be subject to court-martial only where the evidence reasonably establishes that he or she has committed a triable offense. Clearly, prudence is necessary, especially when there are a growing number of cases where, but for DNA technology, persons wrongly convicted of sexual assault would continue to languish in jail. The National Registry of Exonerations compiled by University of Michigan Law School and Northwestern University recently reported, for example, that there have been more than two thousand wrongful convictions for serious crimes since 1989 (the year DNA exonerating evidence became readily available). Issues can also arise about misidentification and, occasionally, false reports. It is simply counterfactual to blame military commanders for the difficulties associated with sexual assault cases, as these same matters would, one would assume, similarly impact the special directorate the draft legislation proposes to establish.
In addition, referring cases to an office with an obvious agenda to increase prosecutions and, presumably, convictions, raises serious questions not just about impartiality, *qua* impartiality, but also regarding the special "enemy" of the military justice system: unlawful command influence.\textsuperscript{104} As a matter of law, improper influences on the military justice system can arise just as readily from politicians and others as from commanders formally part of the process.\textsuperscript{105} Reports are already emerging that "the politics of rape are tainting [the] military justice system," with one defense counsel claiming that "reality is they're charging more and more people with bogus cases just to show that they do take it seriously."\textsuperscript{106}

In fact, a McClatchy Newspaper analysis "found that the military is prosecuting a growing number of rape and sexual assault allegations, including highly contested cases that would be unlikely to go to trial in many civilian courts."\textsuperscript{107} Concerns have been raised, it is reported, "that the anti-rape campaign of advocacy groups and Congress is influencing" commanders to send undeserving cases to trial.\textsuperscript{108} According to Charles Feldmann, a former military and civilian prosecutor turned civilian defense attorney, a military officer is "not going to put his career at risk on an iffy rape case by not prosecuting it," because if he "dismisses a case and there's political backlash, he's going to take some real career heat over that dismissal."\textsuperscript{109}

Efforts, such as the STOP Act, to diminish the role of commanders in military justice matters need to be approached with great caution, as doing so upends thousands of years of military practice and tradition built on hard-won experience. Those countries that have taken similar steps in recent years have found themselves struggling with disciplinary processes that are out of sync with battlefield realities, as well as the overall needs of armed organizations responsible for the nation's defense.\textsuperscript{110} It should not be forgotten that, as the Supreme Court said in *Haig v. Agee*, "It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation."\textsuperscript{111}

The U.S. military justice system, despite many challenges, can, will—and must—continue to sustain the most powerful armed force the world has ever known. While its legitimacy, especially in an era of an all-volunteer military, depends upon the perception as well as the fact of fairness, it also needs to be effective and
efficient. Achieving that aim requires thoughtful prudence, well
grounded in the pragmatism generated by operational experience,
and tempered by the values and principles of a liberal democracy.
The importance of this responsibility cannot be overstated. As the
renowned Roman military thinker Vegetius sagely warned, “No
nation can be happy or secure that is remiss and negligent in the
discipline of its troops.”

Notes

bl/bl_text_xenophon_anabasis_3.htm.
unit/judgeadvocate/Documents/JAM/Mil_Justice_Materials/Resources/
MJFACTSHTS.html.
4 Codified in Title 10, U.S. Code § 801 et seq.
5 The UCMJ is established under Congress’s authority “to make Rules for the
Government and Regulation of the land and naval Forces,” as found in
Article I, Section 8, cl. 14 of the U.S. Constitution.
6 The Military Justice Act of 1968 was much in reaction to issues that arose
during the Vietnam War. See, generally, William Thomas Allison, Military
Justice in Vietnam: The Rule of Law in American War (Lawrence: University
7 See notes 74 to 82 below, and accompanying text.
8 See U.S. Secretary of Defense, Memorandum for the Secretaries of the
Military Departments, Chairman of the Joint Chiefs of Staff, and Chair,
Defense Legal Policy Board, Subject: Military Justice in Combat Zones, July
11 Captain John S. Cooke, “The United States Court of Military Appeals, 1975–77:
13 U.S. v. Denedo, 556 U.S. 904, 918 (2009) (Roberts, J., concurring in part and
dissenting in part).
14 See, generally, R. Chuck Mason, Military Justice: Courts-Martial, an
org/sgp/crs/natsec/R41739.pdf.
18 Article I, Section 8, cl. 14 of the U.S. Constitution.
21 10 U.S.C § 806.
22 10 U.S.C § 934, art. 134, UCMJ, provides as follows: “Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special, or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court.”
25 MCM.
26 Ibid., at Rules for Courts-Martial 916 (k)(1).
29 *In Re Grimley*, 147 U.S. 147, 153 (1890).
32 MCM, pt. IV, 14c(2) (a).
35 MCM, pt. IV, 12c.
39 10 U.S.C § 815.
40 David S. Cloud, “Discipline Recommended in Afghanistan Koran Burning,”
    world/nation/la-na-koran-burning-20120620,0,33470.story.
41 See, generally, Mason, Military Justice.
42 10 U.S.C § 825(d)(2).
43 U.S. v. Thomas, 22 M.J. 388, 393 (CMA 1986).
44 Mason, Military Justice.
45 Ex Parte Milligan, 71 U.S. 2 (1866).
47 Ex Parte Quirin, 317 U.S. 1 (1942).
48 In Re Yamashita, 327 U.S. 1 (1946).
49 Geoffrey S. Corn et al., The Law of Armed Conflict: An Operational Approach
    (2012), 535.
50 White House, President George W. Bush, “Detention, Treatment, and Trial of
    Certain Non-Citizens in the War against Terrorism,” November 13, 2001,
    html.
51 William Shawcross, Justice and the Enemy: Nuremberg, 9/11, and the Trial of
53 See, generally, Jennifer K. Elsea, Military Commission Act of 2009: Overview
54 See, for example, Jordan J. Paust, “Still Unlawful: The Obama Military
    Commissions, Supreme Court Holdings, and Deviant Dicta in the D.C.
55 See, for example, U.S. v. Al Bahlul, 820 F. Supp. 2d 1141 (CMCR 2011) (en banc).
56 Steve Vladeck, “Can the Military Court-Martial Civilian Contractors? 
    April 12, 2012, http://www.lawfareblog.com/2012/04/can-the-military-court-
    martial-civilian-contractors-reflections-on-the-oral-argument-in-united-states-v-ali/.
60 See, for example, Anna Multine, “Command Failure?” Christian Science
61 Mark Boal, “The Kill Team: How U.S. Soldiers in Afghanistan Murdered 
62 Cloud, "Discipline Recommended."


71 Ibid.


75 Ibid.

76 Ibid., 22.


81 Ibid.


85 Ibid.


94 Ibid. According to Rep. Speier, “H.R. 3435, the Sexual Assault Training Oversight and Prevention Act (STOP Act), has 125 co-sponsors. It would take these cases out of the normal chain of command and place the jurisdiction, still within the military, in the hands of an impartial office staffed by experts—both military and civilian.”


104 See U.S. v. Thomas, 22 M.J. 388, 393 (CMA 1986).

105 See, generally, Michael LaMarca, Did the President and Secretary of Defense Commit Unlawful Command Influence? The Upcoming Cases of Nidal Hasan, Bradley Manny, and Robert Bales, May 1, 2012 (unpublished manuscript; copy on file with the author).

106 Taylor and Adams, “Military’s Newly Aggressive Rape Prosecution.”

107 Ibid.

108 Ibid.

109 Ibid.

110 See, generally, Strickey, “Civilianization.”

United States of America

Submission to the
United Nations Human Rights Council
Universal Periodic Review

Eugene R. Fidell *(point of contact)*
Senior Research Scholar in Law and
Florence Rogatz Visiting Lecturer in Law
Yale Law School
127 Wall Street
New Haven, Connecticut 06511
(203) 432-4852
eugene.fidell@yale.edu

Elizabeth L. Hillman
Professor of Law, Provost and Academic Dean
University of California Hastings College of the Law
200 McAllister Street
San Francisco, California 94102
(415) 565-4682
hillmane@uchastings.edu

Nancy Duff Campbell
Co-President, National Women's Law Center
11 Dupont Circle, N.W., Suite 800
Washington, DC 20036
(202) 588-5180
campbell@nwlc.org

Amnesty International USA
5 Penn Plaza, 16th Floor
New York, NY 10001
(212) 633-4256
www.amnestyusa.org

The International Commission of Jurists
Case Postale 91, Rue des Bains 33
Ch 1211 Genève 8, Suisse
+41 22 979 3800
un@icj.org

September 2014
Summary

1. The United States is a party to the International Covenant on Civil and Political Rights ("ICCPR"). The ICCPR applies to the administration of justice through military courts. The United States relies extensively on courts-martial to maintain discipline and punish criminal conduct by its military personnel and certain civilians, but it has not domesticated the ICCPR and its military justice system is noncompliant on a host of critical issues. Although the UN Human Rights Committee ("the Committee") and other human rights bodies and mechanisms have raised questions about aspects of the military commissions conducted at Guantanamo Bay, Cuba, including as recently as March of this year, CCPR/C/USA/CO/4, ¶ 21; CCPR/C/USA/CO/3/Rev.1, ¶¶ 5, 14, 20, the Committee has not focused on compliance issues arising from the United States' far more numerous traditional courts-martial and non-judicial punishments.

2. The United States will be reviewed under the Universal Periodic Review (UPR) in April-May 2015, during the 20th session of the UPR Working Group. The UPR is concerned with, inter alia, "the extent to which States respect their obligations set out . . . in human rights treaties to which the State is party (human rights treaties ratified by the State concerned)." The UPR of the United States therefore provides a valuable opportunity to draw attention to United States noncompliance with its obligations under the ICCPR with respect to its military justice system. This submission identifies major compliance issues in that system and calls on reviewing States parties to make recommendations to the United States for remedial action.

Governing International and Domestic Sources of Law

3. Because the ICCPR is non-self-executing and has not been directly incorporated through specific United States legislation, it is not enforceable per se by United States courts even though its provisions bind the United States as a matter of international law. Unfortunately, the United States is not a party to the First Optional Protocol to the ICCPR. Although United States constitutional law has helped to bring civilian criminal trials into better compliance with applicable human rights standards (death penalty jurisprudence being the notable exception), domestic law has proved insufficient to bring the military justice system into substantial compliance with those standards.

4. Relevant applicable sources of international human rights law include the ICCPR, the Committee's General Comment ("GC") 32, as well as its case law and Conclusions and Recommendations following the examination of periodic reports. Useful additional resources include the Draft Principles Governing the Administration of Justice Through Military Tribunals, E/CN.4/2006/58 ("Decaux"), and the related Report of the Special Rapporteur on the Independence of Judges and Lawyers, A/68/285 ("Knavl").
5. Domestic sources of law include the United States Constitution, the statutory Uniform Code of Military Justice, 10 U.S.C. §§ 801 et seq. ("UCMJ"), and the Manual for Courts-Martial, United States (2012 ed., as amended in 2014) (an Executive Order promulgated by the President of the United States), regulations issued by the armed forces, and decisions of the federal courts, including the Supreme Court of the United States and the civilian United States Court of Appeals for the Armed Forces. Because the ICCPR applies not only to the federal government but to the 50 states, each of which maintains its own military forces, compliance issues may also implicate state constitutional, statutory, regulatory, and case law.

6. The United States military justice system’s noncompliance with contemporary international (as well as Canadian) norms was addressed by the Federal Court of Canada in Tindungan v. Minister of Citizenship & Immig., 2013 FC 115, available at http://www.canlii.org/en/ca/fct/doc/2013/2013fc115/2013fc115.html, in connection with a United States soldier’s claim for asylum in Canada. Aspects of the United States system’s noncompliance with the ICCPR are currently before the Committee in Rivera v. Canada, Communication No. 2196/2012.

7. Although reform measures are under consideration in the United States Congress, none of them would bring the country’s military justice system into full compliance with the ICCPR.

**Importance of United States Compliance with Respect to the Administration of Justice through Military Courts**

8. United States compliance with the ICCPR is important for several reasons. The country maintains a large standing military which it employs around the globe. Its military justice system affects hundreds of thousands of active, reserve and retired uniformed personnel as well as the thousands of civilian employees and contractors who serve with or accompany its forces in the field in war or contingency operations. In addition to the interests of persons who may be tried before it, the system also affects those civilians, foreign and domestic, who may be victims of crimes committed by military personnel. The administration of justice through military tribunals thus has both internal and external human rights implications.

9. The United States maintains an active program of assistance to other countries’ military justice systems through such activities as the Defense Institute of International Legal Studies. The United States military justice system therefore not only directly affects many individuals but also casts a long shadow over military justice worldwide. When such a country—which can and should be a role model—is noncompliant, it sends a profoundly undesirable message to other ICCPR States Parties as well as non-Parties.
Scope of this Submission

10. This submission addresses only the system for courts-martial and non-judicial punishment within the armed forces. The military commissions that were revived after the 9/11 attacks present other important human rights issues that have been the object of close scholarly and judicial scrutiny for over a decade. E.g., Hamdan v. Rumsfeld, 548 U.S. 557 (2006). They do not comply with the ICCPR in important respects. See David J. R. Frakt, Applying International Fair Trial Standards to the Military Commissions of Guantanamo, 37 So. Ill. U. L.J. 551 (2013); Jordan J. Paust, Still Unlawful: The Obama Military Commissions, Supreme Court Holdings, and Deviant Dicta in the D.C. Circuit, 45 Cornell Int’l L.J. 367, 378-80 (2012); Concluding Observations of the Human Rights Committee: UN Doc. CCPR/C/USA/CO/4 (2014) § 21; Joint special procedures report on the Situation of Detainees at Guantanamo Bay, UN Doc. E/CN.4/2006/120 (2006).

11. As noted above, issues of compliance also arise in the administration of military justice by state (as opposed to federal) military forces in the United States. This submission does not attempt to evaluate compliance by those 50 additional systems, except to note that in some respects, such as subject matter and personal jurisdiction, some of those systems may be more defensible than the federal system addressed below.

Major Compliance Issues

12. The following table notes major ICCPR compliance issues arising under the UCMJ with citations to the pertinent source(s) of law.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Domestic Law References</th>
<th>Human Rights References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military retirees and other civilians are subject to trial by courts-martial in the absence of “objective and serious reasons” and where regular civilian courts are available; there is no provision for civilians to serve on courts-martial</td>
<td>Arts. 2(a)(4)-(6), (10-(12), UCMJ</td>
<td>GC 32 § III ¶ 22 &amp; nn.36-37; Decaux ¶¶ 20-21; Knaul ¶¶ 102-04</td>
</tr>
<tr>
<td>Courts-martial are not limited to strictly military offenses, and can try persons accused of serious human rights</td>
<td>R.C.M. 203; Solorio v. United States, 483 U.S. 435 (1987)</td>
<td>Decaux ¶¶ 21, 29, 32-35; Knaul ¶¶ 98-100, 106</td>
</tr>
<tr>
<td>Violations</td>
<td>Art. 20, UCMJ; R.C.M. 1301; <em>Middendorf v. Henry</em>, 425 U.S. 25 (1976)</td>
<td>ICCPR art. 14(1); GC 32 § III ¶¶ 18-21</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Personnel may be ordered into correctional custody or confinement by non-judicial punishment imposed by commanders or one-officer summary court-martial, both of which are noncompliant</td>
<td>Arts. 15, 20, UCMJ</td>
<td>GC 32 § III ¶¶ 15 &amp; n.17, 18</td>
</tr>
<tr>
<td>Commanders pick court-martial members (jurors)</td>
<td>Art. 35(d)(2), UCMJ</td>
<td>ICCPR art. 14(1); GC 32 § III ¶ 19 &amp; n.31; Decaux ¶¶ 45-46; [1997] Findlay v. United Kingdom, 24 EHRR 221</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Even after recent legislative changes, comman-</td>
<td>Art. 60, UCMJ</td>
<td>ICCPR art. 14(1); GC 32 § III ¶ 19 &amp; n.31; Decaux ¶¶ 45-46 &amp; Principle No. 15(j)</td>
</tr>
<tr>
<td>ders can in some circumstances still overturn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or modify court-martial results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Military judges lack the protection of fixed</td>
<td>Art. 26(c), UCMJ;</td>
<td>ICCPR art. 14(1); GC 32 § III ¶ 19-20 &amp; nn.30-32; Knaul ¶¶ 93-96; CCPR/C/79/Add.95 (¶ 14) (judges irremovable only after 10 years) (Algeria); CCPR/C/79/Add.100 (¶ 8) (election by popular vote, 6-year terms) (Armenia); CCPR/C/79/Add.67 (¶ 14); cf. Inocal v. Turkey, Application No. 22678/93 (ECHR 9 June 1998) (¶ 68) (4-year terms with mere possibility of reappointment held not violate European Convention on Human Rights art. 6)</td>
</tr>
<tr>
<td>Many courts-martial (including all summary courts-martial) are not subject to direct appellate review by a court of law</td>
<td>Arts. 64, 66-67, 69, UCMJ; R.C.M. 1306</td>
<td>ICCPR art. 14(5); GC 32 § VII ¶ 45</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>There is no guarantee of a “duly reasoned” written judgment in courts-martial trials or first-level court-martial appeals; most intermediate military appellate decisions are utterly summary; denials of discretionary review by the United States Court of Appeals for the Armed Forces do not state reasons</td>
<td>ICCPR art. 14(5); GC 32 § VII ¶ 49 &amp; n.104; <em>Henry v. Jamaica</em>, Communication No. 230/87 (¶ 8.4) (“accused has right to written judgements, duly reasoned, for all instances of appeal,” including levels of appellate review beyond the one level required by the ICCPR)</td>
<td></td>
</tr>
<tr>
<td>The prosecution has a right to appellate review by the highest court of the military justice system in any case, while the accused must show “good cause” to obtain review; this is a denial of equality of arms</td>
<td>Art. 67(a)(2), -(a)(3), UCMJ; Eugene R. Fidell et al., <em>How “Robust” is Appellate Review of Courts-Martial?</em>, Balkinization, 8 May 2013, <a href="http://balkin.blogspot.com/2013/05/how-robust-is-appellate-review-of.html">http://balkin.blogspot.com/2013/05/how-robust-is-appellate-review-of.html</a></td>
<td>ICCPR art. 14(1); GC 32 § II ¶ 13 &amp; n.14; Knaul ¶ 109; <em>Dieter Wolf v. Panama</em>, Communication No. 1347/2005 (¶ 7.4)</td>
</tr>
<tr>
<td>The United States Court of Appeals for the Armed Forces, which is the sole civilian tribunal in the military justice system, is located for administrative purposes in the Department of Defense, is subject to a statutory political-balance requirement, and lacks power to review sentences for ap-</td>
<td>Arts. 67(c), 141, 142(b)(3), UCMJ; e.g., <em>United States v. Winckelmann</em>, 73 M.J. 11 (C.A.A.F. 2013); <em>United States v. Nerad</em>, 69 M.J. 138, 142 (C.A.A.F. 2010)</td>
<td>ICCPR arts. 14(1), (5); GC 32 § VII ¶ 48 &amp; nn.100-01; Knaul ¶ 110; <em>Uclés v. Spain</em>, Communication No. 1364/05 (¶ 11.3); <em>cf. Saidova v. Tajikistan</em>, Communication No. 964/2001, CCPR/C/81/D/964/2001 (2004) (¶ 6.5)</td>
</tr>
</tbody>
</table>
13. The deficiencies identified in the above table offend a variety of ICCPR provisions. The most prevalent theme is that American courts-martial lack the structural arrangements needed to ensure independence and impartiality. Excessive jurisdictional claims, such as the prosecution of offenses that have no connection to military duties, occur regularly. A recent blatant example is the court-martial of a U.S. Marine Corps staff noncommissioned officer for the murder of a civilian woman in Honolulu, Hawaii. He was sentenced to imprisonment for life. Regrettably, contemporary American constitutional jurisprudence no longer finds anything improper in such prosecutions.

Recommendations

14. Overall Recommendations

1. The United States should, in consultation with all relevant stakeholders, promptly formulate and implement a national action plan, with a concrete timeline and clear targets, to bring all aspects of its military justice system into compliance with the ICCPR.

2. The United States should become a party to the First Optional Protocol to the ICCPR.

3. When the United States ratified the ICCPR it included a declaration to the effect that the ICCPR would not be self-executing, in keeping with general principles of federal law. It should promptly enact legislation domesticating the ICCPR for both federal and state governments. It should promptly enact legislation and promulgate the regulatory changes needed to bring the military justice into full compliance.
15. Specific Recommendations

1. Non-judicial punishment powers exercised by military commanders should not include custodial sentences of any duration unless there is provision for prompt de novo review through a process that is ICCPR-compliant.

2. Where a soldier refuses non-judicial judicial punishment or a summary court-martial and the authorities decide to convene a general or special court-martial, the maximum punishment should not exceed what was permissible as non-judicial punishment or at a summary court-martial.

3. Under no circumstances should civilians or retired military personnel be subject to trial by court-martial.

4. Court-martial subject matter jurisdiction should be confined to military offenses and should exclude serious human rights violations.

5. Summary courts-martial should be abolished.

6. All courts-martial should be subject to appeal as of right with respect to both guilt and sentence.

7. The prosecution and defense should have equal access to appellate review.

8. The political balance requirement for the United States Court of Appeals for the Armed Forces should be repealed.

9. All courts-martial should be eligible for discretionary review by the Supreme Court of the United States, on an equal footing with civilian criminal cases.

10. All military judges should have nonrenewable fixed terms of office of at least 10 years' duration.

11. The power to decide how charges should be disposed of should be transferred from commanders to civilian prosecutors or military prosecutors who are independent of the chain of command except for minor disciplinary offenses.

12. Court-martial members (jurors) should be selected by a court-martial administrator independent of the chain of command rather than by military commanders.

13. Commanders should have no power to set aside or modify the findings and sentence adjudged by a court-martial.
Lawful Command Emphasis: Talk Offense, Not Offender; Talk Process, Not Results

Colonel James F. Garrett, Colonel Mark “Max” Maxwell, Lieutenant Colonel Matthew A. Calarco & Major Franklin D. Rosenblatt

Synopsis

Unlawful command influence (UCI) has rightfully been called the mortal enemy of military justice. This concern stems back to the injustices that occurred during both World War I and II. The reaction to these events was a law—the Uniform Code of Military Justice (UCMJ)—in 1950. A provision within the UCMJ provides that it is improper and unlawful for any person to attempt to influence the action of an appointing or reviewing authority or the action of any court-martial in reaching its verdict or pronouncing sentence. In modern practice, the most common but nebulous type of UCI is the appearance of UCI. Its appearance exists where an objective and disinterested observer who is fully informed of all the facts and circumstances would harbor a significant doubt about the fairness of the court-martial proceedings. Commanders who rely on a properly functioning military justice system in their quest for good order and discipline, and the Staff Judge Advocates (SJAs) who advise them, must remember three central tenants of military justice: commanders at every level must be free to act with independent discretion; the accused Soldier must be free to build his case without outside influences limiting the full ability to obtain evidence and witnesses with full commitment to the justice process; and members of the court-martial must be free to decide the case on the merits and, as necessary, a proper sentence based only on the evidence presented, law as instructed by the military judge, and arguments of counsel.

“Lawful command emphasis” means ensuring that these three legal tenants stay intact to ensure good order and discipline are preserved within the ranks. The balance then is between the commander’s constant participation in his unit’s life and the immutable rights and protections of the accused Soldier. The commander’s daily input in the unit’s direction plays a significant role in the tone and prioritization of the unit’s tasks to accomplish the military mission. As leaders, commanders are expected by their chain of command to prepare their units and its members to be ready to go into harm’s way. To stay within the law, commanders should always remember to talk about the offense but not the offender, and talk about the process, not the result. There will be times when commanders want to distribute information or a perspective that puts the unit’s mission in the best light possible. But judge advocates (JAs) have to give counsel so the commander understands the risk of saying something that would have a near-term positive impact, but could have a long-term detriment to both the accused and the very military justice system that allows commanders to hold Soldiers accountable.

A dialogue between the commander and his SJA helps identify the issues the commander believes need addressing.

A commander should identify and address perceived problems related to military justice. Staff Judge Advocates, however, must assist their commanders by drafting policies that are clear, have context, and avoid the appearance of UCI. Commanders want those who have violated the bonds of trust within the ranks to be held accountable. The UCMJ will maintain its relevancy by holding the individual transgressor accountable by ensuring that every accused receives a fair hearing and opportunity to present his case. This was the clear mandate of the reforms outlined by Congress in the UCMJ. The law provides commanders the tools to enforce accountability within the protections afforded an accused Soldier by the UCMJ, but simultaneously allows for commanders to discuss priorities related to good order and discipline within their ranks. When SJAs and commanders work as a team to do that properly, the result is another powerful tool: Lawful Command Emphasis.

Introduction

In the modern age, military justice must always be fair and transparent. In the words of the U.S. Army’s 22nd Chief of Staff, General George H. Decker, “it is essential that our excellent court-martial system generate public confidence in the basic fairness of the administration of military justice. No other single factor has greater tendency to destroy public confidence in the system than allegations of [unlawful] ‘command influence.’” Unlawful command influence is an existential threat to the military justice system, or according to the Court of Military Appeals—its “mortal enemy.”

† Judge Advocate, U.S. Army. Presently assigned as Strategic Initiatives Officer, Office of The Judge Advocate General, Washington, D.C.
‡ Judge Advocate, U.S. Army. Presently assigned as Chair, Criminal Law Department, The Judge Advocate General’s Legal Center & School, Charlottesville, Virginia.


2. United States v. Thomas, 22 M.J. 388, 393 (C.M.A. 1986). The U.S. Court of Military Appeals (CMA) was redesignated in 1994 as the U.S. Court of Appeals for the Armed Forces (CAAF).
Unlawful command influence is, in the words of U.S. Air Force Lieutenant Colonel Erik C. Coyne, "any action taken in an attempt to influence either an outcome or another into an inappropriate action."³ Unlawful command influence litigation frequently arises from unwitting statements by our civilian and military leaders discussing military justice. In the rigidly hierarchical military, the thinking goes: military members are naturally inclined to obey guidance from their superiors. When this guidance is perceived as penetrating the independent sphere of panel members and commanders, UCI concerns are triggered.

A prime example is President Obama’s 7 May 2013 press conference. The President, who is also the Commander-in-Chief of the armed forces, answered a question about the concerns over sexual assault in the military with tough but unscripted language:

The bottom line is: I have no tolerance for this. . . . I expect consequences. . . . I don’t just want more speeches or awareness programs or training, but ultimately folks look the other way. If we find out somebody’s engaging in this stuff, they’ve got to be held accountable: prosecuted, stripped of their positions, court-martialed, fired, dishonorably discharged. Period.⁴

The actual impact of these comments is not quantifiable. What is more readily apparent is that the comments entered into military motions and trial practice at lightning speed. Defense counsel argued that prosecutorial decisions were tainted by a mandate from the highest military official—the Commander-in-Chief—to prosecute all sexual assault allegations and issue the severest form of punitive discharge.⁵ Military trial judges granted many of these motions and fashioned varied remedies such as additional discovery, greater leeway for defense counsel to question members during voir dire, liberal grants of challenges for cause, and disallowance of punitive discharges.⁶ In response to these developments, several White House and Department of Defense officials emphasized that military officials should effectively disregard the President’s remarks and use their independent judgment when deciding cases.⁷

It is beyond the military expertise of the authors of this article to parse presidential political prerogatives.⁸ The fallout from the President’s comments, however, shows that military and civilian leaders have a strong self-interest in studying and understanding the role of command influence in military justice. The response to the legal fall-out described above led to one of the best, and most recent, examples of lawful command emphasis in the form of a memorandum from the Secretary of Defense clarifying the President’s remarks and views of the Administration.⁹ In the memorandum entitled, “Inegrity of the Military Justice Process,” the Secretary of Defense sent a message that was clear and forceful: “Central to military justice is the trust that those involved in the process base their decisions on their independent judgment. . . . Everyone who exercises discretionary authority in the military justice process must apply his independent judgment.”¹⁰ The Secretary told the entire Department of Defense, and the world for that matter, that there is no expectation for a certain result, regardless of the allegations. In other words, the Secretary is telling commanders to discuss process, not results, and discuss offenses, not offenders. If the President’s message had been delivered in the manner found in the Secretary of Defense memorandum, our trial courts would likely have avoided the necessity to ascend a mountain of litigation, which they continue to climb with no clear summit.

This article will grapple with the intersection of the current environment—especially when sexual assault is alleged—and doing the legally right thing. This article is both historical and tactical. In the end, understanding where a statutory provision comes from is important and helps


⁶ The military judge has "broad discretion in crafting a remedy to remove the taint of unlawful command influence." United States v. Douglas, 68 M.J. 349, 354 (C.A.A.F. 2010). For one example of a judge-crafted remedy in response to a UCI challenge concerning the President's comments, see


⁸ The topic of the president’s personal role in military justice matters deserves more attention in military legal scholarship than the limited coverage in this article. For example, contrast President Obama’s tough talk on sexual assault with President Bill Clinton’s refusal to respond to media questions about a court-martial acquittal of two Marine pilots who were accused of flying recklessly and severing a gondola cable in Italy in 1998, an incident that killed twenty civilians and ignited a diplomatic impasse with Italy. A detailed factual background about that case is found in United States v. Ashby, 68 M.J. 108 (C.A.A.F. 2009).

⁹ Memorandum from the Sec’y of Def to the Military Members of the Dep’t of Def., Integrity of the Military Justice Process (Aug. 6, 2013)

¹⁰ Id.
place it into context, but most commanders and JAs want the practical: what do I do? This article will discuss the history of the Uniform Code of Military Justice; the development of the concept of UCI; what constitutes UCI and how the courts have dealt with it; and a new term for consideration in our military lexicon: lawful command emphasis. Lawful command emphasis is, in short, the appropriate actions commanders or staff members can take within the military justice process to ensure good order and discipline is maintained within the ranks. The focus will be to explore the pitfalls of talking about offenders instead of offenses and the requirement to talk process and not results. The authors will conclude with some suggestions on how commanders and JAs can craft the command’s message so that it stays clear of UCI and focuses on lawful command emphasis. The UCMJ is strong, and it is incumbent that those entrusted to exercise this unique authority—principally commanders with the advice of JAs—do so judiciously and fairly.

Courts-Martial Jurisdiction

Most legal discussions in American jurisprudence will include the U.S. Constitution and the Supreme Court. The Supreme Court has zealously protected the federal judiciary’s constitutional power to adjudicate criminal matters, but the Court has carved out a narrow exception: military crimes. Trying military crimes in a non-Article III court—that is, outside the federal judiciary, specifically courts-martial—stems from Congress’s legislative powers of Section 8, Clause 14: “To makes Rules for the Government and Regulation of the land and naval Forces.”

The Court has interpreted the Constitution as granting Congress the authority to make rules for the government and regulation of the land and naval forces; this is known as the Land and Naval Forces Clause. Congress, in turn, enacted a military criminal code, which grants the Commander-in-Chief the authority to promulgate “[p]retrial, trial, and post-trial procedures, including modes of proof” for courts-martial. In other words, the adjudication of military crimes is outside the purview of Article III. As articulated by the Court, “[t]rial by court-martial is constitutionally permissible only for persons who can, on a fair appraisal, be regarded as falling within the authority given to Congress under Article I to regulate the ‘land and naval Forces’ . . . . The test for jurisdiction, it follows, is one of status, namely, whether the accused in the court-martial proceeding is a person who can be regarded as falling within the term ‘land and naval Forces.’” Since the inception of the republic, the scope of court-martial jurisdiction has been narrow, “which manifested itself in a very limited grant of authority to try offenses by court-martial.” This limited military jurisdiction continues to the present day and has been affirmed by the Court on many occasions.

The Evolution of the Court-Martial Process

Courts-martial practice in America is as old as the United States. The Continental Congress in 1775 enacted the country’s first Articles of War, which governed how the military should conduct itself during war. The articles enacted by the Continental Congress were modeled after, and virtually identical to, the British version, which traces its lineage to the Roman Empire. Court-martial authority vests commanders with the ability to try military personnel under their command who have committed a crime. Commanders exercised this authority on numerous occasions during the Revolutionary War. One of the most notorious courts-martial was the trial of Thomas Hickey, General Washington’s military aide. Hickey was court-martialed for mutiny, sedition, and trying to poison General Washington; thirteen officers found him guilty and sentenced him to be hanged. The primary goal of his court-martial and others was to deter future acts of mutiny, sedition, and treachery.

Between the Revolutionary War and World War I—over 140 years—the Articles of War saw few changes. It was not until 1857 that the Supreme Court took up the issue of the constitutional validity of courts-martial. In Dyses v. Hoover, the Court affirmed a Sailor’s court-martial conviction for desertion. The Land and Naval Forces Clause of Article I, among other constitutional provisions, “show that Congress had the power to provide for the trial and punishment of military and naval offenses in the manner then and now practiced by civilized nations . . . .” Nearly forty years later, the first procedural manual governing how courts-martial should be conducted for the land forces came into being in 1895. The 1895 Manual, however, was not

---

11 U.S. CONST. art. I, § 8, cl. 14. The authority to create military tribunals resides in Section 8, Clause 10 of Article I. “To define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations.” Id. art. I, § 8, cl. 10, see also Ex parte Quirin, 317 U.S. 1, 28 (1942) (holding that the Congress “has thus exercised its authority to define and punish offenses against the law of nations by sanctioning, within constitutional limitations, the jurisdiction of military commissions to try persons for [such] offenses”).


16 MILITARY LAWS OF THE UNITED STATES 702 n.1 (3d ed. 1898).


18 61 U.S. 65, 72 (1857).

19 MANUAL FOR COURTS-MARTIAL, UNITED STATES 3 (1895). The first manual was written by First Lieutenant Arthur Murray.
nearly as detailed as the modern-day Manual for Courts-Martial. The purpose of the manual, like today’s version, was to explain “the legal system that regulates the government of the military establishment.”

It was not until after World War I that Congress examined the military justice system in depth. In hearings held before Congress in 1919, the testimony raised concerns regarding “service members’ and society’s confidence in the justice and fairness of such a system.” The lightning rod for these concerns was Brigadier General Samuel T. Ansell, the Acting Army Judge Advocate General. In law review articles and testimony before Congress, General Ansell questioned the efficacy of a system where no independent legal authority could review the process and result of any court-martial, to include where a death sentence was imposed. As historian Colonel William Winthrop noted in his now-famous 1920 treatise on military law, “the court-martial being no part of the Judiciary of the nation, and no statute having placed it in legal relations therewith, its proceedings are not subject to being directly reviewed by any federal court . . . nor are its judgments or sentences subject to be appealed from such tribunal.”

Even uniformed lawyers, that is, JAs, had a limited role in the court-martial process. The only substantive role for JAs was to “prosecute in the name of the United States, but when the prisoner has made his plea, he shall so far consider himself counsel for the prisoner as to object to any leading question to any of the witnesses, and to any question to the prisoner, the answer to which might tend to criminate [sic] himself.”

Coupled with the lack of legal oversight, General Ansell’s most stinging rebuke of the state of military justice was the commander’s seemingly absolute unfettered authority: “[t]here is no legal standard to which court-martial procedure must conform and, therefore, there can be no error adjudged according a legal standard. In other words, military justice is administered not according to a standard of law at all, but under the authority of a commanding officer.” In the aftermath of World War I, General Ansell, who is referred to by some jurists as the “father of modern American military law,” was most concerned about command control or, by the current term, unlawful command influence.

In an effort to limit the commander’s expansive authority and in response to the voices of concern, Congress enacted the 1920 Articles of War, championed by General Ansell. The 1920 Articles of War made a number of changes to the military justice system, including strengthening the role of the JA in the court-martial process. Congress mandated (1) that the legal member of the court-martial should be a JA or if that was not possible, an officer “specially qualified to perform the duties;” (2) the prosecutor in a court-martial should perform a distinct role from being the command’s counsel; and (3) the accused could choose his own defense counsel. Viewed through today’s lens, these changes seem conservative, but for the first time, uniformed lawyers were now statutorily part of the court-martial process. The military justice system, however, remained intact: the commander exercised overarching control over the process with limited oversight and governance.

No substantive changes were made to the military justice system between the 1920 Articles of War and World War II. In December 1941, the American Army went to war with the 1920 Articles of War. During the course of World War II, about 1.7 million courts-martial were convened, over 100 capital executions were carried out, and over 45,000 servicemen were imprisoned.

At the end of the war, numerous veterans groups raised genuine concerns about the fairness of the military justice system. For example, “[n]ot infrequently the [commanding] general reprimanded the members of a court for an acquittal

29 Articles of War (1920).
30 Id. art. 8.
31 Id. art. 14.
32 Id.
33 Bills to Improve the Administration of Justice in the Armed Services: Hearing Before Subcomm. on Const. Rs. of the S. Comm. of the Judiciary and a Special Subcomm. of the S. Comm. on Armed Services, 89TH Cong. 713, 714 (1966) [hereinafter Joint Hearings], available at http://www.loc.gov/tfdr/Military_Law/pdf/MJhearing-1966.pdf (re fermenting a statement submitted by Professor Arthur E. Sutherland that consisted of a law-review article that was written by Rear Admiral Robert J. White).
or an insufficient sentence.\textsuperscript{34} As one commentator noted, "[t]he emotions suppressed during the long, tense period of global warfare were now released by peace, and erupted into a tornado-like explosion of violent feelings, abusive criticism of the military, and aggressive pressures on Congress for fundamental reforms in the court-martial system."\textsuperscript{35} With over 16 million servicemembers in the ranks during the war, the concerns were held by many who fought and then reintegrated into American society. As validation of these concerns about fairness, the Secretary of War, even before the Japanese surrendered in 1945, appointed a Clemency Board to review all general court-martial in which the servicemember was adjudged confinement. The Board reduced or remitted the confinement in 85\% of the cases.\textsuperscript{36} The overarching concern voiced by numerous lobbies to Congress was "the denial to the courts of independence of action in many instances by the commanding officers who appointed the courts and reviewed their judgments, and who conceived it the duty of the command to interfere for disciplinary purposes."\textsuperscript{37}

The Development of the Concept of Unlawful Command Influence

Subject: Inadequacy of Court-Martial Sentences
To: Colonel Clad T. Gunn, President of the general court-martial appointed by paragraph 3, Special Orders No. 104, this headquarters 16 August 1944

... I am completely at a loss to understand the reasons for the sentences in the case in reference. The same court but recently imposed three sentences of death in similarly serious cases ... . As officers of the United States Army I would have expected a far clearer recognition of duty and the dictates of justice from the members of the court ... . Unfortunately, the provisions of Article of War 19 and 31 prevent me from ascertaining which of the members of the court were responsible for

the adoption of life sentences rather than death sentences. However, those members who were guilty of such gross failure to vote for adequate punishments will themselves recognize the application of the foregoing reprimand.

Troy H. Middleton
Major General, U.S. Army
Commanding

Shortly after the cession of hostilities in World War II in March 1946, the Secretary of War, Robert P. Patterson, addressed the "command control" concern by appointing the War Department Advisory Committee on Military Justice, known as the Vanderbilt Committee because of its chair, Arthur T. Vanderbilt. The Committee's scope was to "study the administration of military justice within the Army and the Army's courts-martial system, and to make recommendations to the Secretary of War as to changes in existing laws, regulations, and practices ... ."\textsuperscript{39} The principle recommendation of the Vanderbilt Committee was the "checking of command control."\textsuperscript{40} The Committee recommended that the law "provide that it is improper and unlawful for any person to attempt to influence the action of an appointing or reviewing authority or the action of any court-martial ... in reaching its verdict or pronouncing sentence ... ." It also recommended the elimination of any "reprimand of the court or its members in any form."\textsuperscript{41}

In the aftermath of the Vanderbilt Committee's report, Congressman Charles H. Eston of Ohio held hearings in 1947 on the fairness of the military justice system. These hearings held by the U.S. House Sub-Committee on Military Justice, of which Eston was the chairman, resulted in proposed legislation, known as the Eston Act.\textsuperscript{42} The Eston Act, supported by the Department of War, prohibited unlawfully influencing the action of a court-martial. The legislation, which passed both chambers of Congress and was signed into law by President Truman, stated in large measure, the modern-day prohibition of unlawful command influence:


\textsuperscript{35} Joint Hearings, supra note 32, at 714 (statement submitted by Professor Sutherland).

\textsuperscript{36} REPORT OF THE DEPARTMENT OF WAR ADVISORY CLEMENCY BOARD (1946).

\textsuperscript{37} DEPT OF WAR ADVISORY COMM. ON MILITARY JUSTICE, REPORT OF THE WAR DEPARTMENT ADVISORY COMMITTEE ON MILITARY JUSTICE 3 (1946) [hereinafter VANDERBILT COMMITTEE], available at http://www.loc.gov/frd/Military_Law/pdf/report-war-dept-advisory-committee.pdf; see also Morris, supra note 17, at 125 (noting also that there were concerns about unlawful command influence and the protections afforded to service members during the investigative stage).


\textsuperscript{39} VANDERBILT COMMITTEE, supra note 37, at 1.

\textsuperscript{40} Farmer & Wels, supra note 34, at 266 (citing the Vanderbilt Committee Report).

\textsuperscript{41} VANDERBILT COMMITTEE, supra note 37, at 8.

No authority appointing a general, special, or summary court-martial nor any other commanding officer, shall censure, reprimand, or admonish such court, or any member thereof, with respect to the findings or sentence adjudged by the court, or with respect to any other exercise, by such court or any member thereof, of its or his judicial responsibility. No person subject to military law shall attempt to coerce or unlawfully influence the action of a court-martial or any military court or commission, or any member thereof, in reaching the findings or sentence in any case, or the action of an appointing or reviewing or confirming authority with respect to his judicial acts.

Although a step in the right direction, some advocates believed this legislation did not go far enough: "the reforms were illusory."44 In response to this criticism, Secretary James V. Forrestal of the newly created Department of Defense, which replaced the Departments of War and Navy, appointed Harvard Law School Professor Edmund M. Morgan to chair a committee on military justice along with the undersecretaries of each Service. Unlike the Vanderbilt Committee, this body was to prepare a "uniform code of military justice which would be applicable alike to all three Services, and which could be submitted to the 81st Congress as the recommendation of the National Military establishment."45 The result was the creation of the 1950 Uniform Code of Military Justice. The UCMJ revolutionized the practice and review of courts-martial. In creating the modern-day UCMJ, signed into law by President Truman in 1950, Professor Morgan wrote of his committee's work, "(w)e were convinced that a Code of Military Justice cannot ignore the military circumstances under which it must operate, but we were equally determined that it must be designated to administer justice. We, therefore, aimed at providing functions for command and appropriate procedures for the administration of justice. We have done our best to strike a fair balance."46

Congress established a comprehensive system of how, when, and why a court-martial could be convened. The UCMJ established roles for JAs and set their qualifications: JAs participating in a court-martial "must be certified as competent to perform such duties by the Judge Advocate General of the armed force of which he is a member."47 Furthermore, a three-member civilian appellate court was established, the Court of Military Appeals,48 to review courts-martial appeals from the various services.

Congress made the court-martial system a creature of statute, thereby giving itself unprecedented oversight authority. As part of the new statutory framework, Congress gave the President the authority to establish a court-martial's procedures and modes of proof.49 The President's Executive Orders implementing the UCMJ comprised the Manual for Courts-Martial (MCM); these presidential rules were subject to appellate review by the Court of Military Appeals and, later, the Supreme Court.

What did not change, however, was the Elston Act mandating the prohibition of unlawful command influence. The Morgan Committee adopted this language in full and thereby incorporated the Act's language verbatim into the new UCMJ, Article 37—Unlawfully Influencing Action of Court. With minor changes,50 this provision has remained intact since its inception in 1948. The only substantive change to the modern-day Article 37 of the UCMJ occurred with the 1968 Military Justice Act. This Act, along with expanding the powers of military judges, added language to Article 37(b) that made it illegal to "consider or evaluate the performance of duty of any . . . member of a court-martial" when preparing the servicemember's fitness or efficiency report for promotion or assignment.51

Striking a Fair Balance

As Professor Morgan aptly articulated over sixty years ago, "[T]here are many schools of thought on military justice, ranging all the way from those who sponsor complete military control, to those who support a complete absence of military participation. I do not believe either of

---

44 Farmer & Wels, supra note 34, at 273 (citing 34 A.B.A. J. 702-03 (1948).
48 UCMJ art. 67 (1950). It is now the modern-day U.S. Court of Appeals for the Armed Forces.
49 The CMA's appeals flowed from each military department's Board of Review. This board, now the Court of Criminal Appeals, reviewed each conviction for both errors of law, but still sufficiency of the facts. Id. art 66.
50 Id. art. 36(a).
51 The word "shall" was replaced with "may" in 1956.
these extremes represents the proper solution.”

The balance then is between the commander’s constant participation in his unit’s mission and tasks and the immutable rights and protections of the servicemember who is accused of a crime. The preamble to the MCM foreshadows this balance: “The purpose of military law is to promote justice, to assist in maintaining good order and discipline in the armed forces, to promote efficiency and effectiveness in the military establishment, and thereby to strengthen the national security of the United States.”

The commander has daily input in the direction that his unit takes, and obviously plays a significant role in the tone and prioritization of the unit’s tasks to accomplish the military mission. The commander, after all, is the leader and is expected to prepare the unit and its members to be ready to go into harm’s way.

As for the civilian who becomes a servicemember, the Vanderbilt Committee succinctly observed, “[t]he civilian must realize that in entering the army he becomes a member of a closely knit community whose safety and effectiveness are dependent upon absolute obedience to the high command; and that for his own protection, as well as for the safety of his country, army justice must be swift and sure and stern.” The individual servicemember becomes part of something bigger, not only in accomplishing the unit mission, but in possessing the legal obligation to sacrifice his life, if required, in its accomplishment. There is simply no civilian equivalent to this concept.

Fundamental to obtaining the obedience required to maintain the unit’s safety and effectiveness is discipline. It is the commander who is held accountable and whose obligation it is to instill, maintain, and enforce good order and discipline within the ranks. The commander is the fulcrum of discipline and justice. The Vanderbilt Committee also pointed out that “[n]othing can be worse for [Soldiers’] morale than the belief that the game is not being played according to the rules in the book, the written rules contained in . . . the Manual of Courts-Martial.” Soldiers must believe the system is fair, and that it is administered accordingly. Discipline, in other words, has its limits; this was the stark lesson learned from the unfairness Soldiers perceived during World Wars I and II. Clearly, “discipline will be better and morale will be higher if service personnel receive fair treatment.”

Even commentators from the 19th Century “recognized that courts-martial were under the obligation to render justice in accordance with the fundamental principle of law and without partiality, favor, or affection.”

Unlawful Command Influence

Since the passage of the UCMJ, UCI has been analyzed by the courts in two ways. One way is to discuss UCI as accusatory or adjudicative. Accusatory UCI springs from command influence that invades the independent discretion of other justice actors in the preferral, forwarding, or referral of charges. Adjudicative UCI, on the other hand, occurs when command influence interferes with witnesses, judges, members, or counsel.

The other narrative is to talk about UCI and the impact it has on the military justice system in terms of actual or apparent UCI. Actual UCI is the “actual manipulation of any given trial.” For the most part, this type of UCI is rare and, if found, will normally result in the dismissal of the entire case.

The most nebulous type of UCI is the appearance of unlawful command influence. As defined by the courts, the appearance of UCI exists “where an objective, disinterested observer, fully informed of all of the facts and circumstances, would harbor a significant doubt about the fairness of the [court-martial] proceeding.” The commander must strike a balance between “the commander’s responsibility for discipline . . . [and the] ‘subtle pressures that can be brought to bear by command in military society.’”

The Mechanics of Case Progression Without UCI

Commanders who rely on a properly functioning military justice system in their quest for good order and discipline, and the SJAs who advise them, must jealously guard three central tenants of military justice that come under attack in the presence of UCI.

53 House UCMJ Hearings, supra note 46, at 506.
55 VANDERBILT COMMITTEE REPORT, supra note 37, at 5.
56 Id. at 6.
57 CONST. RTS. REPORT, supra note 1, at 17.
58 Farmer & Wels, supra note 34, at 277 (citing WINTHROP, MILITARY LAW AND PRECEDENTS 61–62 (1886)).
60 Id.
61 Id.
63 See United States v. Gore, 60 M.J. 178 (C.A.A.F. 2004) (the convening authority told a defense witness not to testify at sentencing).
64 United States v. Lewis, 63 M.J. 405, 415 (C.A.A.F. 2006).
(1) Commanders at every level must be free to act with independent discretion.  

(2) The accused must be free to build his case without outside influences impacting a full ability to obtain evidence and witnesses with full commitment to the justice process.  

(3) Members of the court-martial must be free to decide the case on the merits and, as necessary, a proper sentence based only on the evidence presented, law as instructed by the military judge, and arguments of counsel.  

No doubt, Article 37 is the cornerstone of protection against UCI in military justice, but it is only the first in a line of currently existing procedures and protections found in statute, executive order, and case law. The preamble to the MCM not only highlights the necessities of good order and discipline, but also reminds us that the purpose of military law is “to promote efficiency and effectiveness in the military establishment” in an effort to strengthen the security of the Nation. While all commanders value efficiency, few value efficiency above thorough investigation and analysis, which will lead to the best disposition decisions possible.

Commanders and SJAs who emphasize process in combating the day’s most notable detractors from good order and discipline, and are not focused on a particular offender or result, increase the probability of good decisions free of UCI exponentially. This begins with those levels of command closest to the Soldiers, who deserve a healthy and orderly command climate. These “immediate commander[s]” as defined by Rule for Courts-Martial (RCM) 306, ordinarily have the ability and responsibility to conduct a preliminary inquiry into suspected offenses within their units. They then have the discretion to dispose of offenses by members of their command at the lowest possible level unless otherwise withheld.

While the initial disposition decision refers to whether to prefer charges, take some other form of action, or do nothing at all, once charges have been preferred against a Soldier, the command must next decide how to dispose of the charges. The military’s system of justice was built to give commanders at the lowest possible level discretion to dispose of charges. As described above, the military has long valued the necessity for military justice to be portable, fair, and swift. In making decisions to act on or forward charges with recommendations, commanders and SJAs are again reminded that each commander, regardless of level of command, must exercise independent discretion.

Command Influence and Potential Pitfalls

Commanders may and should discuss military justice process, views, and their unit’s most pressing needs in the areas of health, welfare, and good order and discipline with their subordinates. As long as a commander neither directs a particular action regarding an ongoing case or type of case, nor impacts the participation of witnesses, counsel, court-martial members, or judges, discussions that foster good order and discipline or instruct on the fair administration of justice are not UCI. Most commanders know this and would never consider purposefully influencing independent command discretion or the court-martial process. But UCI most frequently occurs in a much less conspicuous manner. The comments of our Commander-in-Chief about sexual assault, as already discussed, provide but one example of how an off-the-cuff response can lead to unintended consequences. Answering unanticipated questions without reflection, addressing unit formations, staff calls, safety and briefings, and discussing views on disposition in forums like a Sexual Assault Review Board provide some of the most fertile ground from which UCI will grow for the commander-SJA team who do not cultivate frequent conversations about delivering a proper command message.

Commanders and SJAs who routinely discuss their shared understanding of the potential for a command message to impact case progression in order to identify and avoid potential UCI pitfalls foster a healthy military justice practice. While the SJA’s role focuses on more technical aspects of legal requirements, a SJA improves the commander’s awareness and vigilance through discussion of...
these aspects. Simultaneously, while a SJA does not bear the burden of command, discussions with commanders about climate, discipline, and a commander’s pre-existing beliefs regarding justice assist in identifying potential UCI issues before they become problematic.

Failing to discuss the message, and as a result to identify potential UCI in command remarks, can result in the perception, if not the reality, of the message inextricably invoking the court-martial process. The resulting relief granted by a trial or appellate court could be extreme, to include dismissal of charges with prejudice. The system simply works best and avoids unnecessary consequences caused by UCI if the SJA and commander have an open, frank, and ongoing dialogue about cases, the system, and the command message.

This advice holds true for how commanders and JAs should manage UCI concerns during high-profile incidents. In an age of digital media and instant communications, gaffes become instantly known and quickly irretrievable. At the same time, we expect our senior leaders to be able to talk about issues directly, without being vague or requiring lawyers to vet every comment. Beyond considerations already mentioned, such as emphasizing training and education, it may help to think about UCI in a new light. Apparent UCI is not the “mortal enemy” of military justice that actual UCI is, but commanders and all JAs should take every measure to ensure the dictates of the law are adhered to zealously.

Court Analysis of UCI

Given every commander’s reliance on their legal advisors to guide them through potential UCI minefields, every JA in such a role should make it a priority to understand the legal framework of UCI analysis. The defense must first raise the issue of UCI at trial, as articulated in the case of United States v. Biagase. “The threshold for raising the issue at trial is low, but more than mere allegation or speculation.” The facts provided to raise a UCI claim must also demonstrate that, if true, “the alleged unlawful command influence has a logical connection to the court-martial, in terms of its potential to cause unfairness in the proceedings.”

The Court in Biagase went on to clarify past inconsistencies in case law, clearly articulating that the government’s burden in overcoming a properly raised claim of UCI is beyond a reasonable doubt.

The government may carry its burden (1) by disproving the predicate facts on which the allegation of unlawful command influence is based; (2) by persuading the military judge or the appellate court that the facts do not constitute unlawful command influence; (3) if at trial, by producing evidence proving that the unlawful command influence will not affect the proceedings; or (4), if on appeal, by persuading the appellate court that the unlawful command influence had no prejudicial impact on the court-martial.

With this case law in mind, it is imperative that commanders and JAs receive education and training on the prevention of UCI. This education and training is in the self-interest of all military justice players, especially leaders who wield the most influence in the military. This so-called “shield” of UCI prevention has the same goal as the ancient English adage, “Justice should not only be done but should be seen to be done.”

Many brigade commanders and most general officers receive specific training at The Judge Advocate General’s Legal Center and School (TJAGLCS) in Charlottesville, Virginia, regarding UCI. In the recent past, issues that arise in sexual assault cases—the current UCI lightning rod—are also covered. In this environment, commanders learn about, and freely discuss, critical areas where the pursuit of good order and discipline must patiently and unwaveringly adhere to a military justice process designed to protect against UCI. Judge advocates learn about UCI at their advanced course and ways to eliminate it from our system of justice.

The “sword” of preventing UCI, on the other hand, is wielded by defense counsel in identifying and raising issues

---

78 See e.g., United States v. Stoneman, 57 M.J. 35 (C.A.A.F. 2010) (discussing a case in which the accused’s brigade commander sent an e-mail to unit leadership promising to “declare war” on leaders who failed to lead by example).


80 But see United States v. Ayers, 54 M.J. 85, 94-95 (2000) (noting that the court “has recognized that the appearance of unlawful command influence is as devastating to the military justice system as the actual manipulation of any given trial”) (internal quotation marks omitted).


82 Id. (citing United States v. Johnston, 39 M.J. 242, 244 (C.M.A. 1994)).

83 Id. (citing United States v. Allen, 33 M.J. 209, 212 (C.M.A. 1991)).

84 Id. at 130-51.

85 Id. at 151.

86 See Fred L. Borch, Legal Education for Commanders: The History of the General Officer Legal Orientation and Senior Officer Legal Orientation Courses, ARMY LAW., Mar. 2014, at 68.

87 Id.
of encroachments on the impartiality of the court-martial process. This focus is increasingly on apparent UCI. The current dormancy of actual UCI is a positive development, but defense counsel must be ever vigilant to ensure this mortal enemy does not rear its head. Finally, defense counsel must never subscribe to the notion that challenging an entire system is too radical or that probing the decisions of high-level commanders is a departure from the traditional customs of the military bar. Instead, defense counsel who are unencumbered in their zealfulness represent the most ironclad guarantee of court-martial impartiality and justice.

The Sinclair and Wilkerson Cases

In light of President Obama's comments, two military cases grabbed the American public's interest: *United States v. Sinclair* and *United States v. Wilkerson*. Both cases occurred in the midst of a public tempest over the debate of sexual assault in the military and the role of commanders in courts-martial. The salacious facts and the senior ranks of the accused helped make both cases among the most publicized courts-martial in modern times, in particular *Sinclair*.

Brigadier General Jeffrey Sinclair pleaded to and was found guilty of maltreatment of subordinates, adultery, and solicitation, among other crimes. In *Sinclair*, UCI issues were heavily litigated over the course of three motions sessions. The defense challenged the information sharing and coordination among military officials in the pre-preferral stage, the tough talk by military and civilian leaders on the problem of sexual assault, the effect of extensive media attention on the case, the potential bias of prospective general officer panel members, the influence of an outside lawyer on the prosecution, and the effect of contemporaneous sexual assault prevention initiatives on the court-martial. Unlawful command influence served as a catch-all for other issues in the case, such as prosecutorial ethics and whether the convening authority displayed an inflexible disposition when he decided to reject a plea agreement based solely on the victim's desire that he reject it. Whether these issues amounted to apparent UCI is open for debate, but given its broad definition, the UCI doctrine proved that it was up to the task in *Sinclair*. After the court-martial, there was consternation over the sentence (as should be expected in such a closely watched criminal trial) but no lingering controversy over whether the military justice system had the right tools at its disposal to shield against improper interference. The scheme of burdens from *Biagiase* empowered the court-martial parties to robustly explore all UCI possibilities. *Sinclair* served as an emphatic rebuttal to the most cynical criticism of military justice that it is more concerned with politically influenced show-trials than truth seeking.

Interestingly, much public discourse about the *Sinclair* trial talked about "undue" command influence rather than the correct term "unlawful" command influence. This is telling. "Undue influence" borrows a term of equity from contract law and probate law. "Undue" sounds more benign than the sinister connotations of "unlawful": a harm to be corrected, but short of a mortal enemy. Perhaps the mistaken label of "undue" reflects a broader undertcurrent that UCI issues now skew more towards apparent UCI than actual. Unlawful command influence practice, it seems, is increasingly concerned with rooting out issues that can be perceived as harmful influence rather than thwarting affirmatively illegal meddling and obstruction. This is a welcome, positive trend.

The *Wilkerson* case, on the other hand, offers an important lesson about UCI from the perspective of favorable actions toward the accused. *United States v. Wilkerson* drew national attention when the convening authority, Air Force Lieutenant General Craig Franklin, dismissed charges of sexual assault and conduct unbecoming an officer against Lieutenant Colonel James Wilkerson after a panel convicted him and sentenced him to dismissal and one year of confinement.

Lieutenant General Franklin's post-trial decision sparked debate about military justice reform, which this article will not retreat. Construed more narrowly, the *Wilkerson* case is a helpful aid in diagnosing when a convening authority has an "other than an official interest" in a case. This tenet of UCI asks whether "a reasonable person would impute to [the convening authority] a personal feeling or interest in the outcome." Anyone with an "other than an official" interest is an accuser, and accusers are ineligible from convening

---


89 Since this sentence fell below requirements for production of a trial transcript and submission for appellate review, study of the UCI aspects in this court-martial (and there were many) is far more difficult than with a published appellate opinion. In researching the case for this article, the authors are grateful to Lieutenant Colonel Robert Stelle for providing helpful information about the three UCI motions submitted by the defense, the three government responses, and the military judge's written ruling on the first motion. Lieutenant Colonel Stelle was a trial counsel on the case.

90 The accused was convicted of maltreatment and sentenced to a reprimand and to forfeit $5,000 per month for four months. Oppel, supra note 88.

91 See, e.g., Ruth Marcus, *Break the Chain of Command on Military Sex Assault Cases*, WASH. POST, Mar. 18, 2014 (describing developments in the case of "whether there had been 'undue command influence' in pursuing the Sinclair prosecution").


93 UCMJ art. 1(9); MCM, supra note 54, R.C.M. 504(c)(1).
general or special courts-martial. Following this, an accuser who carries out convening authority duties is engaged in unlawful command influence.

Published military appellate opinions about convening authorities with "other than an official interest" focus on those who display animus towards an accused. Wilkerson demonstrates how the opposite response, favoritism, can be just as problematic. The Wilkerson case includes a treasure trove of internal documents released in response to public and political attention on the case. These documents helped illuminate the convening authority’s manner of deliberation in ways that normally are not available to the public, and caused many to question his impartiality.

Wilkerson will never become UCI case law because the convening authority disapproved the findings of guilty and sentence and dismissed the charges. But the case is a useful lesson in how perceptions matter: if an accused’s privilege or personal connections to judicial officials garner him more favorable treatment than he would otherwise enjoy, the integrity of the military justice system suffers, just as it suffers when a convening authority displays a personal hostility towards the accused. In either case, an accuser is improperly serving as a convening authority. The rule is simple: quasi-judicial officials, like Lieutenant General Franklin, must be impartial or recuse themselves.

Focus on Lawful Command Emphasis

A review of relevant cases is replete with examples of UCI, holding true the notion that the law is made from bad cases. Yet, commanders who properly address disciplinary

issues enjoy the protection of their command responsibilities from the courts. Following the tragic death of multiple civilians riding a gondola when a Marine Prowler made contact with the cable, as outlined in the case of United States v. Ashby, the 2d Marine Aircraft Wing Commander addressed the officers in the Prowler community through a series of speeches. The commander implied that the incident was caused because the crew was not following rules by flying too low. He admonished the Prowler community as a whole for violating rules on low-level flights and discussed the possibility of punishment for violating flight rules. He never specifically addressed any disciplinary proceedings against the mishap aircrew, what would be an appropriate punishment in the case, or whether fellow aviators should testify in the case.

The Ashby court considered that “[b]ecause of the highly publicized international nature of the incident, it is understandable that many senior military officials became publicly involved in the aftermath and investigation of the accident.” However, there was “no direct evidence that the actions of any of those officials improperly influenced the court-martial.” The appellate court evaluated the facts for actual UCI and “the appearance of unlawful command influence where ‘an objective, disinterested observer, fully informed of all the facts and circumstances, would harbor a significant doubt about the fairness of the proceedings.’” and found no UCI that impacted the court-martial process. The court supported the commanders involved in the investigation who spoke about the cause of the incident, eventually failing to find “that the senior military officials’ interest in the investigation was anything other than proper, official, and lawfully directed at completing a quality and thorough investigation.”

Further support for a commander’s ability to lawfully influence the discipline and climate among our ranks, even with regard to sexual assault, can be found in United States v. Wylie. In Wylie, the Navy-Marine Corps Court of

---

94 UCMJ art. 22(b) (general courts-martial), art. 23(b) (special courts-martial).
96 The Wilkerson FOIA Release, UNITED STATES AIR FORCE FREEDOM OF INFORMATION ACT READING ROOM, http://www.foia.af.mil/reading/the.wilkerson/foxcase.asp (last visited July 25, 2014). The releases show that both the convening authority and the accused were officers in the same tight-knit F-16 pilot community. In his clemency submission, the accused emphasized this common background with the convening authority and noted that they flew a combat mission together in Iraq. While deliberating, Lieutenant General Franklin received e-mails from a close military advisor that the accused’s “integrity is airtight” and “character is unshakeable,” and another e-mail from a retired group of F-16 pilots decrying the trial as an unfair assault on the fighter pilot community. In a memorandum justifying why he dismissed the charges, Lieutenant General Franklin said that part of his reasonable doubt came from the accused’s selection for promotion to full Colonel, service as a wing inspector general, and description as a doting father and husband. The convening authority seemed aware of how his actions would be perceived as favoritism, and addressed this in his written statement by emphasizing that he did not personally remember the accused. However, after dismissing the charges he wrote in an internal e-mail stating, “I intend to get him back to a flying assignment as soon as possible . . . . Certainly after [the accused] and [the accused’s] wife have had a chance to discuss, I would like to know what he wants to do next . . . . Please make sure Colonel Wilkerson knows he can contact me . . . about the way ahead for his next assignment.”
98 Id.
99 Id.
100 Id (citing United States v. Lewis, 63 M.J. 405, 415 (C.A.A.F. 2006)).
101 Id. at 129.
102 Id.
103 Id.
104 Id. at 128.
105 United States v. Wylie, No. 201200088, 2012 WL 5995983 (N-M. Ct. Crim. App. Nov. 30, 2012), review denied, 72 M.J. 164 (C.A.A.F. 2013). It is important to note that this was an unpublished case from a sister-service court and is in no way binding within the Army. Still, it provides a good example of command commentary that survived appellate scrutiny on what is currently the most sensitive topic.
Criminal Appeals considered a two-page message from the Commander of the Pacific Fleet titled, "Leadership against Sexual Assault." Among other comments, the message stated,

Despite on-going training and prevention efforts, sexual assault continues to be a persistent problem in the Navy that demands our attention. Two-thirds of all sexual assaults are blue-on-blue, to include seniors sexually assaulting juniors. It would be unwise for [us] to underestimate the impact that sexual assault has within the Navy. It begins with leaders who . . . react forcefully and consistently when sexual misconduct occurs.

The court specifically called the message "an instance of lawful command influence." This message is an excellent example of lawful command emphasis.

Commanders may easily, and legally, influence the progression of a case or investigation without influencing a subordinate commander at all through the use of a withholding policy. Among the most notable examples of a withholding policy is the 20 April 2012 Secretary of Defense mandate that all sexual assault cases are withheld to the first O-6, special court-martial convening authority for initial disposition. Commanders and SIAs should review this memorandum not only for its impact on dispositions in sexual assault cases, but also for its form and construction. The most notable aspect of this memorandum is the lack of reference to how any commander should dispose of a case beyond the process. Instead, the Secretary goes only so far as to support the process, while emphasizing the responsibility for reviewing all matters, conducting independent reviews as necessary, encouraging subordinate commanders to make recommendations, and only then determining an appropriate disposition.

But with these UCI parameters in place, how can commanders set priorities and a tone for their unit on a daily basis without crossing into unlawful command influence? Commanders can talk about offenses, but should not talk about offenders. Commanders can emphasize, for example, that sexual assault is "a criminal offense that has no place in the Army. It is incompatible with Army values and is punishable" under the law. These actions are not an influence on a particular case, but an emphasis on the commander’s priorities. Lawful command emphasis allows the commander to prioritize those tasks so that he can accomplish the mission. To stay within the law, commanders should remember to talk about the offense, but not the offender, and talk about the process, not the result.

**Talk Offense, Not Offenders**

Commanders and their legal advisors should focus on the offense and how that offense harms the military’s mission and the bonds of trust within the military that make mission success possible. Therefore, commanders and their staff should not refer to an alleged offender in a derogatory manner. Intemperate comments can impact the alleged offender’s right to a fair trial. For example, if commanders or staff members make intemperate comments, alleged offenders might not be able to muster witnesses willing to testify in their defense. If commanders or primary staff members (those who are under the commander’s mantle of authority, to include the SJA or even the accused’s first-line supervisor) refer to the accused as a “terrorist” or “scumbag,” others, including potential panel members, might presume the accused is guilty. At a minimum, those types of comments will have a chilling effect on the fairness of the judicial proceedings and be “a corruption of the truth-seeking function of the trial process.”

Instead, talk the offense. The phrase “sexual assault is a criminal offense that has no place in the Army” is a perfectly valid and acceptable statement for any commander to make about sexual assault. Sexual assault is not the only criminal offense that has seized the public’s narrative and made the daily news feed—some that might come to mind are hazel, driving under the influence of alcohol, sexual harassment, domestic violence, and discrimination. Each of these is a

106  Id. at *2.
107  Id.
108  Id. at *3.
109  Memorandum from Sec’y of Defense to Sec’ys of the Military Departments et al., subject: Withholding Initial Disposition Authority Under the Uniform Code of Military Justice in Certain Sexual Assault Cases (20 Apr. 2012).
110  Id.
111  Id.
112  Id.
113  Memorandum from the Chief of Staff, XVIII Airborne Corps and Fort Bragg, subject: [Policy] (9 Sept. 2008) (on file with the authors).
114  The concept of “talk offense, not offender, talk process, not results” was outlined in 2006 by then-Lieutenant Colonel Patricia Ham, Chair of the Criminal Law Department at The Judge Advocate General’s Legal Center and School. *See Patricia A. Ham, Still Waters Run Deep? The Year in Unlawful Command Influence, Army Law*., June 2006, at 53.
115  Id. at 66.
crime under the UCMJ, federal law, or state law. Stating that "sexual harassment in any form will not be condoned within our ranks" is a comment about the offense, not the offender. 195 For example, a commander can always explain that every sexual assault in the Army deteriorates a unit's ability to be prepared for the mission, using words to the effect of, "there is no place for behavior that has this kind of impact at a time with as varied a mission-set as we have, requiring 100% mission focus."

Furthermore, commanders should not single out an alleged offender; that is, a commander should not call a particular Soldier a "druggie" for testing positive on a urinalysis examination. That commander would be veering into waters of assigning guilt before the judicial proceedings commence, which could impact the Soldier's due process rights. Likewise, it is important for a commander to make a distinction between the crime and the person accused of the crime. So while the commander can say, "There is no place for sexual assault within the Army," the commander should not go on to say, "or for those who commit this crime." Even if an accused is found guilty by court-martial, the sentence might not include a discharge, meaning the accused is allowed to stay in the military.

As already discussed, commanders must always advance the narrative that their subordinates use independent judgment. The Commanding General of 1st Infantry Division and Fort Riley articulated this adroitly for the entire Division:

Independent Judgment: I expect everyone involved in the military justice system to exercise their own independent judgment and make decisions based upon the individual facts and merits of a case. Decisions are not to be made based upon personal interests, a desire for career advancement, or an effort to please others in the chain of command. Senior officials must never pressure a subordinate to take a particular action or make a certain recommendation in any action. 120

This language tracks both the sentiment and the verbiage crafted by the Secretary of Defense's memorandum on the integrity of the military justice system several days earlier. It reminds commanders, leaders, and all JAs that each case must be resolved on its own facts. One should not presume a conclusion without knowledge of the facts.

119 Id. at 438.

121 Memorandum from the Commanding General, 1st Infantry Division and Fort Riley, subject: Danger 6 Sends 13-4, Integrity of the Military Justice System (8 Aug. 2013) (on file with the authors).

Proactive Measures on Offense

There are numerous proactive ways commanders can talk offense and not focus on the offender: policy memorandums, required unit training, and check-lists. Commanders often put out policy guidance to make those in their commands aware of the commanders' priorities. Several years ago, alcohol abuse was an issue within the ranks. Today, alcohol-related incidents still happen, but with a focus on eliminating alcohol abuse from the ranks, there has been a down-turn in these types of incidents. As the Commander of the 4th Infantry Division and Fort Carson phrased it, "[a]lcohol is a drug... by both military and civilian personnel is inconsistent with Army values, standards of performance, discipline, and the readiness necessary to accomplish the Army's mission." 121 His policy memorandum goes on to set parameters of when alcohol can be present at unit functions, for example: "[u]nits . . . will not conduct fundraisers using alcohol." 122 The commander also requires that certain training be conducted to prevent an alcohol-related incident: leaders "will ensure that all Soldiers and Civilians are briefed prior to any holiday, training holiday, and . . . extended leave about the dangers of alcohol misuse and abuse." 123

The goal is to give members of the command awareness and then the tools to help those who are affected: "[l]eaders should make available suitable programs to help reduce or eliminate alcohol-related incidents and to promote responsible social behavior." Programs like the Army Substance Abuse Program and the Family Advocacy Program are available to all Soldiers, which should be made clear in the policy memorandum. Also, if adverse action must be taken against a Soldier because of involvement in alcohol-related misconduct, the memorandum should make clear that "[c]ommanders are expected to continue to exercise discretion in recommending" the appropriate disposition. 124 Although an excellent articulation, this sentiment could be further bolstered and driven further from any possible UCI allegations by inserting the word "independent" before discretion.

With the national narrative focused on sexual assault, commanders should consider putting out a policy memorandum on sexual assault. Such memoranda should make it clear that sexual assault is a crime, and should

121 Policy Letter, Headquarters, 4th Infantry Division (Mechanized) and Fort Carson, subject: Command Alcohol Policy 1 (13 Feb. 2012) [hereinafter Carson Alcohol Policy] (on file with the authors).
122 Id.; see also Policy Letter, Headquarters, XVIII Airborne Corps and Fort Bragg, subject: Mandatory Initiation of Administrative Separation for Drugs and Alcohol Related Offenses 2 (26 Mar. 2012) (on file with the authors).

123 Carson Alcohol Policy, supra note 121.
124 Id.
outline the unit’s training responsibilities for the prevention of sexual assault. The memorandum should also include information as to how a victim should report a sexual assault and what resources are available to the victim. As one command succinctly stated, “[l]eaders at all levels must take swift and decisive action in preventing, identifying, reporting, and—after consulting with legal authorities—disposing of all incidents of sexual assault.” The XVIII Airborne Corps’ policy on the response to incidents of sexual assault gives subordinate commanders a sexual assault victim assistance checklist and the telephone numbers of care providers and local authorities. This same policy outlines the unit’s annual training requirements. The commander is trying to be proactive and set a tone that sexual assault or harassment is not acceptable behavior. With specific regard to sexual assault policies, programs that begin with Soldiers at the lowest rank and grow upward tend to be most effective and least likely to create UCI concerns. Plus, it allows commanders to teach and empower Soldiers to take care of each other when the chain of command is not present and inculcate a culture where sexual assault is not acceptable behavior.

Regardless of the subject matter, commanders are trying to “develop a command climate in which service members feel confident that they can openly address incidents of sexual assault [and harassment, hazing, or domestic violence] with their chain of command.” In the policy memorandum, as in the oral and written comments of a commander, the focus should be on the conduct that should not be condoned—these crimes interfere with the unit’s mission and degrade the unit’s combat effectiveness and readiness. The memorandum should simply avoid discussion of any alleged perpetrator of sexual assault, hazing, or domestic violence and refrain from commenting on what should happen to any Soldiers who are accused of such conduct presently or in the future.

125 Policy Letter, Headquarters, Fort Campbell, subject: Fort Campbell Policy on Sexual Assault (30 Nov. 2011) (on file with the authors).
126 Policy Letter, CG-01, Headquarters, 4th Infantry Division (Mechanized) and Fort Carson, subject: Sexual Harassment/Assault Response and Prevention (SHARP) Program (n.d.) (on file with the authors) (policy is undated).
127 The authors recommend staying away from the terminology “will not be tolerated” given developed case law that takes a dim view of the “zero tolerance” policy. See United States v. Simpson, 58 M.J. 368, 376 (C.A.A.F. 2003) (finding no unlawful command influence in the use of “zero tolerance” regarding Army policy about drug use, but emphasized the court’s conclusion was case-specific and warned that “zero tolerance” has improperly affected past courts-martial).

**Talk Process, Not Results**

We live in an age of instantaneous information and social media commentary. There is a great drive to comment on what is happening instantaneously—the current pending case, the de jure outrage—and the perception is that there is a demand to know the facts as we know them this very second. This feeding of the news cycle is a reality of our current environment, and with instantaneous communication platforms, the demand for comment or information grows more intense. In the context of the UCMJ, Colonel Erik Coyne correctly couches high-interest cases as “[b]alancing the need for information with the demands of justice.” Commentary that calls into question the fairness of the military justice system by discussing results is corrosive. All military courts should impartially and judiciously decide the merits of a case; this is foundational and paramount. To do otherwise is to cast into doubt the instant case that is, or potentially will be, before a court-martial. More seriously, it undermines the system. It gradually leads to doubt about the fairness of the UCMJ.

Colonel Patricia Ham, former Chair of the Criminal Law Department at The Judge Advocate General’s Legal Center and School, gave two excellent examples of talking process, not results. The first related to the allegation that in November 2004 in Iraq, a Marine corporal shot an unarmed man in a Fallujah mosque. The situation captured the public’s attention, in part, because the episode was captured by a journalist, Kevin Sites, on camera. Instead of making conclusions or telegraphing a certain disciplinary result, General George V. Casey, the commander in Iraq at the time, stated, “[T]he shooting is being investigated, and justice will be done .... This whole operation was about the rule of law, and justice will be done.” General Casey, when asked about the details of what the military knew and potential culpability, was not making conclusions but discussing the process. Since there was film of the actions, there was an appetite in certain corridors of the press to bring this Marine to justice for killing a civilian, but General Casey and the Marine Corps leadership investigated the facts and concluded that the Marine’s actions were consistent with the rules of engagement and the law of armed conflict.

128 Coyne, supra note 3, at 16.
129 See also Ham, supra note 114.
130 Id. at 67.
131 New York Times Rewrites Fallujah History, GLOBAL POL’Y FORUM (Nov. 16, 2004), https://www.globalpolicy.org/component/content/article /168/36645.html (“If part of that ‘information war’ means convincing Americans that civilians are not victims of the Fallujah invasion, the Times has signed up on the side of the Pentagon.”).
The other example given by Colonel Ham relates to the November 2005 Haditha Dam massacre where twenty-four Iraqi civilians were killed allegedly by U.S. Marines. General Peter Pace, the Chairman of the Joint Chiefs of Staff at the time, when asked about what the military would do with the implicated Marines, said, “We will find out what happened, and we’ll make it public . . . . [T]o speculate right now wouldn’t do anybody any good.” Even more than the Fallujah mosque incident, the Haditha Dam massacre seeped into the public’s narrative. But the criminal process had not occurred at that point, and the rights of the accused would not allow the military’s leadership to talk about conclusions of culpability.

Both examples are related to requests for information about an ongoing investigation regarding potential war crimes. It is certain that both of these senior officers had information that would have put the military in a better light at the time. But both officers took a strategic pause and did not offer commentary that could have had a near-term positive impact, but could have caused long-term detriment to both the individuals involved and our military justice system.

Comments by the Commandant of the Marine Corps and the Secretary of the Army

The above comments can be juxtaposed with what two senior leaders in the military establishment recently said about matters related to sexual assault in the military. One example shows the unintended consequences of talking results and the other shows the intended benefits of talking process. The first are the comments by the Commandant of the Marine Corps, General James F. Amos, during his Heritage Brief, and the second are the comments by the Secretary of the Army, the Honorable John McHugh, about the court-martial of Brigadier General Jeffrey Sinclair.

In the spring of 2012, the Marine Corps’ Commandant, General James F. Amos, toured Marine Corps installations worldwide. During his talks with Marines, known as the Heritage Brief, he discussed his priorities as the Commandant, his responsibility for the Corps’ “spiritual health,” and those issues that impacted this health. During this address, he discussed the problem of sexual assault within the Marine Corps as follows:

[W]e had 348 sexual assaults in 2011 and you go—males in here, I know exactly what you are thinking, well . . . it’s not true; it is buyer’s remorse; they got a little

The Commandant was talking squarely about results and not about the process. As the senior Marine, he was informing Marines that a vast majority of sexual assault allegations are “legitimate,” and once found guilty of this disgraceful and heinous act, the Marine needs to be removed from the ranks. In other words, believe the victim of sexual assault and eliminate the perpetrator.

The Commandant’s remarks landed squarely in the middle of the court-martial of Staff Sergeant Howell. Howell was accused of rape, among other violations of the UCMJ, and was found guilty by a panel of Marines and given eighteen years of confinement and a dishonorable discharge. Howell raised the appearance of UCI, in part, on the Commandant’s remarks given at Parris Island where Howell was pending trial by general court-martial for sexual assault. The Navy-Marine Corps Court of Criminal Appeals agreed and set aside the findings of guilt and the sentence. The Howell court held that “a disinterested observer, knowing that potential court-martial members heard this very personal appeal in April from the [Commandant] to ‘fix’ the sexual assault problem, would harbor significant doubts about the fairness of a sexual assault trial held shortly thereafter in June.”


136 Id. at *5 (emphasis added).

137 Id. at *1–2.

138 Id. at *17. The Court notes in a footnote that “on the date of the Heritage Brief at Parris Island, the appellant was pending trial by general court-martial for sexual assault offenses. The panel for his specific court-martial had been identified, and eight panel members were sitting in the
The lack of curative instructions to the panel members who heard the Commandant speak and the military judge’s flawed rulings, along with his intertempere comments during the trial, made this case unanimous in its result. But Senior Judge Ward, in his concurring opinion, noted that “[m]uch of the Heritage Brief in my mind reflects lawful command influence. Reasonable minds can disagree as to attendant meanings from certain remarks. In many ways, the [Commandant’s] remarks in regard to sexual assault reflect a broader, ongoing debate that extends well beyond our military.”

As outlined in these pages, there are numerous steps a commander can take to ensure lawful command emphasis. What is perplexing about Senior Judge Ward’s comment about sexual assault reflecting a broad, ongoing debate is that those other commentators to this debate are not the Commandant of the U.S. Marine Corps—the senior military officer in the Marine Corps. Like a commander, when he speaks, his subordinates listen. In the end, with position comes responsibility, and one of those responsibilities is adherence to Article 37, UCMJ. In sum, the tactical imperative of eradicating sexual assaults from our ranks cannot trump the strategic necessity of preserving our time-tested code of military justice. One of its pillars for more than sixty-five years is Article 37, UCMJ.

On the other side of the spectrum concerning comments by senior leadership is the Sinclair case. As already discussed, the Army court-martialed Brigadier General Jeffrey Sinclair for maltreatment of subordinates, among other crimes. After the trial but before the General Court-Martial Convening Authority (GCMCA) took action on General Sinclair’s case—in which the GCMCA would review the record of trial and consider General Sinclair’s clemency matters—the Secretary of the Army was asked about General Sinclair’s sentence while testifying before the U.S. House of Representatives. He was asked in the context of a less than cordial audience; one Member asserted that Sinclair was “given a slap on the wrist,” thereby suggesting that military justice “does not work.” Instead of defending the result or casting it into doubt, the Secretary adroitly talked about the process.

As the final decision-maker in matters of this kind, I’m really constrained in what I can say. Unlike in the civilian sector, when a jury comes in, and the case is closed, this case is not closed. They’re under the uniform code of military justice: a continuing process of certification of the record providing both the victim as well as [Sinclair] an opportunity to respond to the content of that record . . . . What I can say is that as in the civilian sector, we do not have control over, nor do we try to influence the sentencing of the judge. The Army was faced with the prospect of prosecuting this particular individual, and it did that, and it also prosecuted in a way that obtained a conviction. Those are the things we—we do control . . . . So, we do take the steps necessary to hold soldiers accountable, but we cannot, and nor would the civilian sector, be able to make the determinations of a sentencing judge.

Then a Member of Congress asked whether Sinclair would be able to retire at his current grade. The Secretary, again, talked about the process and did not telegraph what would occur.

Under the processes for the military, when a soldier goes for retirement, the secretary of the department has the authority to order a grade determination board, and that grade determination board makes recommendations as to the grade at retirement for that officer . . . . [U]nder the military procedures, at retirement, the service secretary of any of the military departments can order a grade determination board to make recommendations on grade at retirement.

When asked if he was going to conduct a grade determination board, the Secretary answered: “I’m not at liberty to make comment on what I may or may not do, particularly given that the case is still technically open under the UCMJ.” The Secretary did not make a comment that would impact General Sinclair’s opportunity to have his clemency be fully and fairly considered by the GCMCA—a right afforded every accused. Secretary McHugh’s responses provide a good example of a right way for leaders to talk about military justice.

---

139 Id. at *23 (Ward, J., concurring).
141 Id.
142 Id. at 63.
143 Id.
Crafting Your Message

While this article cannot identify every potential UCI pitfall or look into a crystal ball to predict lawful command emphasis that will always survive scrutiny, it can offer a method that helps accomplish both tasks based on lessons learned from senior leaders. The best first step is simply a conversation between the commander and the SJA identifying the issue the commander wants to address. A commander may and should identify and address perceived problems related to military justice. Staff Judge Advocates must assist in drafting policies and statements that are clear, have context, and avoid UCI.

Both the commander and SJA should consider the content and complexity. Ask, "Can this commander address this issue and have the intended impact on the intended audience?" Most of the time, critical analysis and carefully crafted language will result in a positive answer to those questions. On other occasions, the commander-SJA team will determine the commander must exercise restraint on the issue to ensure independent discretion and fairness.

If the commander decides to address the issue, consideration of the intended audience is critical, as is the commander's intent regarding further promulgation. Some messages are simply too complex and nuanced for transmission to a large audience. A commander must be able to clearly and directly communicate command emphasis to an audience, orally or in writing, with some predictability regarding the manner in which listeners or readers at varying ranks will receive the message. To the extent the commander-SJA team senses the message may become murky for some, they should reevaluate the intended audience and message.

An often cited example, and the one used during General Officer Legal Orientations at TJAGLCS, comes from United States v. Treakle. In Treakle, a commanding general was frustrated with subordinate commanders who recommended referral of cases to levels of courts-martial empowered to adjudge a punitive discharge, but then testified in favor of retaining the Soldier. Potential for UCI existed within both aspects of this general's frustration. If he directed a lesser course of action, he would unlawfully influence the independent discretion of his subordinate commanders. If he directed subordinates not to testify to retain Soldiers for whom they recommended a discharge, he would unlawfully influence their testimony. Was there room for a nuanced message to the right audience that only addressed a method of doing military justice business using a systematic, consistent approach?

The commanding general in Treakle discussed the issue with his SJA. The SJA prepared talking points that, in part, warned against conveying a message that might discourage testimony. While the general used the talking points, he spoke somewhat extemporaneously to several different large audiences, often leaving out the cautionary note supplied by his SJA. Subordinates at various levels of command who attended different meetings later conveyed very different understandings of the comments.

The general could have discussed the necessity for thorough investigations and critical analysis using all the factors listed in RCM 306, and the importance of making independent recommendations and having the courage to stand behind them. Instead, he conveyed a complex message orally on several occasions to various audiences where he often strayed from the points prepared by the SJA and with a tone and tenor that confused his subordinates. While his SJA was there for some of those meetings, he was more frequently absent and never took steps to provide course correction until it was too late. The message, audience, forum, and legal presence were all wrong, resulting in unintended UCI instead of lawful command emphasis.

Even after a commander-SJA team determines proper lawful command emphasis to the right audience, in the correct context, should it be delivered orally or in writing? Commanders tend to appreciate the closer interpersonal aspects of in-person communications. Written policies offer

140 United States v. Treakle, 18 M.J. 646, 653 (C.M.A. 1984) (discussing comments by a commanding general seeking to correct a perceived military justice problem that were interpreted very differently by members of the unit who heard the comments at different meetings and in different contexts).

141 Id. at 649 (discussing a SJA who provided a point paper with cautionary warnings meant to safeguard against UCI).

142 Id. at 653.

143 Id. at 654.

144 See CRIMINAL LAW DEP'T., THE JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., U.S. ARMY, GENERAL OFFICER LEGAL ORIENTATION—UNLAWFUL COMMAND INFLUENCE (quoting Treakle, 18 M.J. at 646).

145 TreaKle, 18 M.J. at 650.

146 Id. at 654.

147 Id. at 650–52.

148 MCM, supra note 54, R.C.M. 306(b) discussion. Some of the factors include "the nature of and circumstances surrounding the offense and the extent of the harm caused by the offense, including the offense's effect on morale, health, safety, welfare, and discipline; . . . the views of the victim as to disposition; . . . and the character and military service of the accused." Id.

149 TreaKle, 18 M.J. at 654.

150 Id. at 649–50.
the opportunity for precise language and consistency in the way the message is received. In deciding which is best, commanders should consider their ability to predict the manner in which subordinates will receive the message and the resulting impact. Part of the impact may be responding to a UCI motion. Accordingly, when SJAs discuss delivery of the message, they must provide counsel on how both delivery and reception of the message should be preserved.

After the lawful command emphasis is delivered, commanders and JAs must follow up to ensure the message received was consistent with the commander’s intent. As an organization, the military frequently requires subordinates to provide “back-briefs” or use other methods to ensure proper understanding of an intent or operation. It is a method that every level of Soldier has experienced and understands. When exercising lawful command emphasis, both legal and command personnel should ask what subordinates gleaned from the command policy or message. Only then can the team truly assess the success of the message or the potential need for clarifying guidance.

Conclusion

The UCMJ is unique and must comport with the fundamental concepts of American justice. The balance between justice and discipline is not antithetical, however. It is complementary. All commanders and those under the mantle of command authority must make the fair and impartial functioning of the military justice system their mission. It truly is where tactics and strategy meet.

Commanders want transgressors in their units to be held accountable, which is understandable and necessary. The commander-SJA approach must ensure the strategic vibrancy of the UCMJ. The joint focus must be discipline—holding offenders accountable—and ensuring that every accused receives a fair hearing with the full opportunity to present his case. That is the goal of Article 37. Lawful command emphasis provides the commander-SJA team with the means to protect the integrity of Article 37 and the UCMJ while simultaneously addressing indiscipline within the formation. Properly applied, lawful command emphasis allows a commander to lead a stronger, mission-ready unit built on Soldier trust and trust in our military justice system.

156 Id. at 654.
The military should make everyone in the service follow California’s ‘yes means yes’ laws

By Rachel E. VanLandingham October 15 2014  THE WASHINGTON POST
Rachel E. VanLandingham teaches criminal law at Southwestern Law School in Los Angeles. She is a retired Air Force Judge Advocate and Vice President of the National Institute of Military Justice.

The U.S. military are among the most respected members of society. Yet in the bedroom, we expect much less of them than we do of the 18-year-olds who grace California’s university campuses.

According to a law signed last month, college students in California must secure “affirmative, conscious, and voluntary” consent from their partner before sex. This measure acknowledges that American universities have a rampant sexual assault problem; almost 20 percent of undergraduate women experience an attempted or actual sexual assault in college.

With almost half of its active-duty ranks under age 25, the U.S. military has been grappling with similarly unacceptable rates of what it calls “unwanted sexual contact,” primarily among its college-age members.

Part of the problem is written into the Uniform Code of Military Justice (UCMJ). Right now, in the military, silence may in fact equal consent. According to Article 120, the “totality of the circumstances” must be considered when sexual assault is reported. Silence and lack of resistance equal consent, unless a victim’s silence or passivity can be attributed to intentional acts by the defendant.
That is, a young service member who freezes because they are shocked at being groped or penetrated, or goes limp because they are afraid their drill instructor will flunk them out of basic training (though he hasn’t said so), can be construed as consenting to such unwanted contact.

Furthermore, even if a jury doesn’t buy that this passivity actually equals consent, the statute allows the defense to argue that they reasonably mistook the victim’s silence as consent.

California ensures that such a mistake can never be construed as reasonable: “[l]ack of protest or resistance does not mean consent, nor does silence mean consent.” Period.

The military needs to jettison its “silence may sometimes represent consent” definition in favor of a clear affirmative consent standard like California’s. It also needs the California law’s reminder that “[i]t is the responsibility of each person involved in the sexual activity to ensure that he or she has the affirmative consent of the other or others to engage in the sexual activity.”

Such clarifications are critically needed in the military environment to counteract the often powerful dynamics of rank, loyalty and teamwork which contribute to an inherently coercive atmosphere; an atmosphere in which silence should never be a default for consent to sex.

These changes (which need to be approved by Congress) will reverberate well beyond the courtroom. They will help change attitudes via education. The military actually uses the UCMJ’s statutory definition of consent — typically word for awkward word — to train and educate today’s young service members as to what is acceptable behavior regarding sex. The deeply disturbing prevalence of sexual assault on our military bases and college campuses demands that expectations regarding sexual behavior shouldn’t be left to popular music and the media.
We owe our young men and women in uniform at least as much clarity as college students in California, and to hold them to at least the same reasonable and modern standard. Accountability of offenders is one method of deterrence; prevention through education is even better.
MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEFS OF THE MILITARY SERVICES
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT

SUBJECT: Comprehensive Review of the Uniform Code of Military Justice

As proposed by the Chairman of the Joint Chiefs of Staff and the other members of the Joint Chiefs, I direct the General Counsel to conduct a comprehensive review of the Uniform Code of Military Justice (UCMJ) and the military justice system with support from military justice experts provided by the Services.

Such a comprehensive review is appropriate given the many amendments to the UCMJ since the Military Justice Act of 1983 and to the Manual for Courts-Martial (MCM) since 1984. The review should include an analysis of not only the UCMJ, but also its implementation through the MCM and Service regulations. The review should consider any report and recommendations issued by the Response Systems Panel. I direct that a report including a recommendation for any appropriate amendments to the UCMJ be submitted within 12 months and that a second report recommending any appropriate amendments to the MCM be submitted within 18 months. The General Counsel will submit an Issue Nomination to the Director, Cost Assessment and Program Evaluation, describing the additional resources necessary for this review.

[Signature]
Panel VII:

Cybersecurity – Will We Ever Be Secure?

Moderator:
Jill D. Rhodes
RESOLVED, That the American Bar Association urges the Executive and Legislative branches to consider the following guiding principles throughout the decision-making process when making U.S. policy determinations to improve cybersecurity for the U.S. public and private sectors:

Principle 1: Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks.

Principle 2: Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks.

Principle 3: Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements.

Principle 4: Privacy and civil liberties must remain a priority when developing cybersecurity law and policy.

Principle 5: Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.
EXECUTIVE SUMMARY

1. Summary of the Resolution

Sophisticated cybersecurity threats are increasingly targeting citizen information as well as critical economic and national security assets. Consequently, the cybersecurity of our digital infrastructure is a national priority for leaders in both public and private sectors. In order to effectively engage in the ongoing national dialogue regarding cybersecurity, the Resolution establishes American Bar Association guiding principles for the Executive and Legislative branches to consider when making U.S. public policy determinations to improve cybersecurity.

2. Summary of the Issue that the Resolution Addresses

Growing cybersecurity attacks against U.S. public and private sector entities threaten the delivery of essential citizen services, security of corporate data, including intellectual property and trade secrets, U.S. government assets and data, and personally identifiable information of citizens. As cybersecurity attacks have evolved, public and private sector leaders have been challenged to further more than decade-old policy foundations to effectively confront cybersecurity threats. With cybersecurity threats equally targeting the public and private sectors, legislation and policy must drive new and unprecedented levels of public-private collaboration across a large stakeholder group including all levels of government, corporations, the legal community, academia and citizenry.

Currently, Congress is considering several legislative solutions and the Administration is developing an Executive Order to improve the nation’s cybersecurity preparedness. In this environment, the American Bar Association requires a policy position to weigh in on pressing cybersecurity issues.

3. Please Explain How the Proposed Policy Position will address the issue

The Resolution is designed to equip the American Bar Association with widely-supported guiding principles that will enable the Association to weigh in on cybersecurity legislation and policy in the short term. Over the long term, the guiding principles will provide a framework to drive the Association’s continued focus on cybersecurity.

4. Summary of Minority Views

The Resolution is designed to encompass varying views on cybersecurity and present a framework to accommodate all stakeholders. Therefore, there are no known minority views at this time.
REPORT

The American Bar Association recognizes the increasingly critical need for action in response to growing cybersecurity attacks against U.S. public and private sector entities that threaten the delivery of essential citizen services, security of corporate data, including intellectual property and trade secrets, U.S. government assets and data, and personally identifiable information of citizens. Widespread use of the Internet and information technology during the past decade has created unprecedented opportunities. New and innovative uses of the Internet and information technology have improved the delivery of essential goods and services, increased the quality of life, offer new ways to connect with citizens, and paved the way for economic growth across the globe. However, along with exciting new functionality, use of the Internet and information technology may introduce opportunities for criminals, terrorists, and nation states to undermine the delivery of these extraordinary capabilities and create national and economic security risks.

In this environment, the cybersecurity of our digital infrastructure is a national priority for leaders in both public and private sectors. The American Bar Association has a central role to play in promoting cybersecurity. The American Bar Association should provide the leadership and expertise for lawyers to gain, and remain, competent in cybersecurity and to protect client information from cybersecurity breaches. In addition, the American Bar Association should lead a new national dialogue on cybersecurity amongst the legal profession, as lawyers are actively counseling government, private corporations, and the non-profit communities. Legal scholars are similarly positioned in academia to lead discussions on evolving cybersecurity challenges and, more profoundly, to offer legal and policy solutions to resolve complex new challenges. Finally, the American Bar Association should promote policy principles that advance our national agenda toward greater security and privacy protections, at home and abroad.

This report provides an overview of cyber threats, shared risks, and new roles and responsibilities for leaders in the government, corporations, legal profession, academia, and citizenry. The report concludes with five initial principles to guide the private sector and the executive and legislative branches of government in developing cybersecurity policies and working with leaders in both the public and private sectors.
Cyber Threat Environment

Sophisticated cybersecurity threats are increasingly targeting both citizen information and critical economic and national security assets. Global threats from criminals, terrorists, and nation states pose significant risks to critical infrastructure, government and corporate data, personally identifiable information, and intellectual property creating concerns in the areas of consumer protection, privacy and critical infrastructure protection. \(^1\) Cyber crimes are not just a threat to information systems, but also, in the hands of an anarchist, a terrorist or a hostile group or nation to tangible assets, communications necessary for a functioning society, political processes such as elections, and human life.

Both government and the private sector have demonstrated a concern for cybersecurity threats, risks, and their potential consequences, as demonstrated by significant government and private sector investments in cybersecurity infrastructure. However, resource commitments alone have not led to a comprehensive mitigation of cybersecurity vulnerabilities. Rather, the nation is facing risks that demand new ways of thinking and expertise to address them.

Shared Risks

Cybersecurity threats equally target both the public and private sectors. Public and private sectors also share common vulnerabilities, such as reliance on the global Internet and use of modern technologies to reach customers and citizens across the globe. As a result, cybersecurity presents both shared risks and shared responsibilities requiring the public and private sectors to address risks separately and in partnership.

National leaders have treated cybersecurity and collaboration as a national priority and a shared public-private responsibility for well over a decade. Presidential Decision Directive 63, signed in 1998, formalized public-private partnerships as a key part of the nation’s first cybersecurity policy. \(^2\) Since then, successive Administrations have uniformly adopted a collaborative approach for managing cybersecurity. Similarly,

---


leaders in the private sector and academia have also recognized the value of public-private collaboration as a strategic priority. Multiple findings from the nation’s leading academic institutions, think tanks, and trade associations call for new levels of collaboration around shared cybersecurity risks.

**New Roles, New Responsibilities**

The nation requires new and unprecedented levels of public-private collaboration. Effective frameworks will demand a rethinking of current roles and responsibilities across affected stakeholders in several areas.

- The U.S. government must protect citizen data as well as unclassified and classified systems. In addition, the U.S. government needs to leverage its resources across civilian, law enforcement, defense, intelligence, and diplomatic components to share threat information and collaborate with the private sector.

- Private sector companies that store or process citizen data, or own and operate critical infrastructures, should continue to promote effective, company-specific security measures, as well as participate with the government in collaborative efforts to address shared cybersecurity threats.

- Lawyers have a deep responsibility (i) to protect client information and to develop, and maintain secure systems, (ii) to play an active role in the creation and implementation of public-private frameworks, and (iii) to represent clients that may have fallen victim to cybercrime.

- Academia should continue to participate in a national dialogue on law, policy, and technological innovations. Legal scholars, law school administrators, and others in the legal community should foster an environment in which law students can undertake future leadership roles and responsibilities relating to cybersecurity.

- Consumers and citizens also have unique roles and responsibilities, and they need improved resources to help them counter and prevent cybersecurity risks.

**National Policy Principles**

Cybersecurity is a complex issue that requires a holistic approach to address current and future risks. The American Bar Association should play a leadership role in preparing lawyers to contribute to this multidisciplinary discussion and also be prepared to contribute to the national dialogue on cybersecurity. Toward those ends, the American Bar Association should adopt the following initial principles to guide its leadership role in the cybersecurity debate:

**Principle 1**: Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks.
Comment: Advancing cybersecurity at home and abroad will require solutions that address both public and private sector risks. Frameworks must be developed to define new roles and responsibilities for all of the participants who are necessary to secure cybersecurity. These include governments at all levels, corporations, nonprofit organizations, non-governmental organizations (NGOs), lawyers, academics, and citizens. These diverse groups must be molded into workable frameworks that facilitate cooperation and effectively confront cybersecurity threats. New partnership frameworks to address more virulent cyber threats need to be analyzed and existing, effective partnership frameworks should have continued support and participation.

**Principle 2:** Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks.

Comment: In light of the global nature of shared cybersecurity threats, advanced forms of information sharing and collaboration are needed. Information on threats is necessary, but it is not nearly sufficient to counter the risks. Public and private sectors need to share not only information on threats, but also knowledge on how to manage cybersecurity threats, including effective tools, practices, and risk frameworks. The public and private sectors should engage in a continuing dialogue to better enable them to constantly share information on new capabilities, risks, and developments and how to react to them, while still maintaining privacy and civil liberty protections.

**Principle 3:** Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements.

Comment: Effective public-private frameworks for information sharing and collaboration will require the modernization of law and policy. At a minimum, the public and private sectors should review and consider measures that remove impediments to greater public-private collaboration and the sharing of capabilities. The ability to track and trace cybercriminal activity and legal issues pertaining to liability, antitrust, and the protection of government and corporate information remain legal challenges that should continue to be reviewed and considered. The legal, engineering, computer, and scientific academies should support rigorous review of legal doctrines and application of those doctrines, and offer innovative solutions for helping to create an effective legal and policy environment for the coming decade.

**Principle 4:** Privacy and civil liberties must remain a priority when developing cybersecurity law and policy.

Comment: Privacy and civil liberties must remain bedrock principles as the nation grapples with complex cyber threats and global attacks. Lawmakers have both a responsibility to foster new forms of collaboration, but also to protect and maximize privacy and civil liberties as part of these solutions. Since cybersecurity programs will traffic in digital information that could contain sensitive personal information or reflect constitutionally protected activity, it is crucial that these principles are fundamentally
built into cyber programs from the start, and that cyber programs be conducted with reasonable accountability. Furthermore, the legal profession has a unique role to play in educating lawmakers and the public as to the choices that are available, the impact of those choices, and the challenges associated with balancing cybersecurity needs against privacy and civil liberties rights.

**Principle 5:** Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.

**Comment:** New public-private frameworks for cybersecurity will require a trained and supportive workforce to implement and maintain them. The nation requires a focus on developing cybersecurity expertise within all levels of the government and private sector and within the general population. The ABA should have a critical role in educating and encouraging lawyers, law firms, and citizens about the need to act to minimize cyber security risks. The weakest link may be the individual’s home computer that has been infected and is serving a proxy role in cybercriminal activity. Lawyers must dedicate themselves to continually developing the competencies necessary to effectively secure client and firm data and systems and participate in cybersecurity initiatives with the government, corporations, the legal profession, academia, and citizens.
RESOLVED, That the American Bar Association condemns unauthorized, illegal governmental, organizational and individual intrusions into the computer systems and networks utilized by lawyers and law firms;

FURTHER RESOLVED, That the American Bar Association urges federal, state, local, territorial, and tribal governmental bodies to examine, and if necessary, amend or supplement, existing laws to promote deterrence and provide appropriate sanctions for unauthorized, illegal intrusions into the computer networks utilized by lawyers and law firms;

FURTHER RESOLVED, That the American Bar Association urges the United States government to work with other nations and organizations in both the public and private sectors to develop legal mechanisms, norms and policies to deter, prevent, and punish unauthorized, illegal intrusions into the computer systems and networks utilized by lawyers and law firms;

FURTHER RESOLVED, That while the American Bar Association supports governmental actions, policies, practices and procedures to combat these unauthorized, illegal intrusions into the computer systems and networks utilized by lawyers and law firms, the ABA opposes governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, the confidential lawyer-client relationship, or traditional state court and bar regulation and oversight of lawyers and the legal profession; and

FURTHER RESOLVED, That the American Bar Association urges lawyers and law firms to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice, and also comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity.
EXECUTIVE SUMMARY

1. Summary of the Resolution

This Resolution condemns unauthorized, illegal intrusions by governments, organizations, and individuals into the computer systems and networks utilized by lawyers and law firms; urges federal, state, and other governmental bodies to examine and, if necessary, amend existing laws to fight such intrusions; urges the United States government to work with other nations and organizations in both the public and private sectors to deter, prevent, and punish such intrusions; supports governmental measures to combat such intrusions while opposing governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, the confidential lawyer-client relationship, or traditional state court regulation of lawyers; urges lawyers and law firms to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice; and urges lawyers and law firms to comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity.

2. Summary of the Issue that the Resolution Addresses

As American businesses and government agencies become increasingly reliant upon network communications, they grow more vulnerable to information security attacks. These attacks increasingly target both citizen information and national security assets. Criminals, terrorists, and nation states all see potential gains from attacking information systems. These threats to highly sensitive information trigger concerns from the national security community, privacy advocates, and industry leaders alike, and seriously threaten client confidentiality.

3. Please Explain How the Proposed Policy Position will Address the Issue

By adopting the proposed Resolution, the ABA will be able to play a leading role in urging the United States government and other governmental bodies to examine, and if necessary, amend or supplement existing laws in order to discourage, prevent, and punish malicious intrusions into lawyer and law firm computer systems and networks, but only in a fashion that protects client confidentiality, the attorney-client privilege, the larger confidential lawyer-client relationship, and traditional state court regulation and oversight of lawyers and the legal profession.

4. Summary of Minority Views

The Cybersecurity Legal Task Force is unaware of any minority views.
I. Introduction

This Report explains the American Bar Association’s ("ABA") resolution regarding the growing problem of intrusions into the computer systems and networks utilized by lawyers and law firms. It notes the alarming rise of attacks on these electronic systems and networks and the recent rise of nation states as significant actors in hacking activities over the past decade. The Report also condemns these unauthorized, illegal intrusions and urges governmental bodies at all levels—federal, state, local, territorial, and tribal—to examine, and if necessary, amend or supplement existing laws to deter and punish these intrusions but only in a manner that respects and protects client confidentiality, the broader confidential lawyer-client relationship, and traditional state court regulation and oversight of lawyers and the legal profession. Further, the Report notes the different measures available to combat hacking, including diplomatic and law enforcement tools, legislation, and regulatory measures. This Report also underscores the importance of protecting confidential client information, the attorney-client privilege, and other core legal principles. Finally, the Report describes the ethical rules and professional obligations of lawyers and law firms implicated by information security breaches. This includes the lawyer’s obligation to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice. It also includes the lawyer’s obligation to comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity. Overall, the Resolution builds upon the several ABA Resolutions passed by the House of Delegates and Board of Governors relating to information security and client confidentiality.

Moreover, it is the expectation of the Task Force that there will be additional resolutions on cyber dealing with the issues of privacy, legal and illegal intrusions, and government responsibilities. This resolution does not address U.S. government activities authorized by law in the national security realm.

II. Background

A. Increasing Cyber Attacks on Lawyers and Law Firms

As American businesses and government agencies become increasingly reliant upon electronic communications, they grow more vulnerable to information security attacks. Such attacks are increasingly sophisticated and target critical infrastructure and national security assets as well as personal information. Criminals, terrorists, and nation states all see potential gains from attacking information systems. These threats to highly sensitive information trigger concerns from the national security community, privacy advocates, and industry leaders alike.
The Director of the National Security Agency estimates that the United States loses $250 billion each year due to cyber-espionage and other malicious attacks on information systems. \(^1\) Confidentiality, integrity, and availability are the three cornerstone goals that every data security program is designed to achieve. Malicious attacks exploiting security vulnerabilities take a number of forms. A common attack affecting “availability” and information access is a “distributed denial of service” ("DDoS") attack, whereby servers are overwhelmed when malicious attackers flood the bandwidth or other resources of the targeted system with external communications requests. Attacks on “integrity” cause improper modification of information by inserting, deleting, or changing existing data. In an attack affecting “confidentiality,” an eavesdropper can gain access to sensitive data whenever it leaves a secure area or is transmitted in an unsecure fashion (i.e., unencrypted).

New and increasingly elaborate methods are being developed for accessing confidential information. By using “phishing” or “spear phishing” attacks, intruders attempt to acquire information, such as login credentials. Masquerading as a trustworthy entity in an electronic communication, they entice users to open an e-mail attachment or click on a link to a website containing malicious software that will infect a network’s computers and report sensitive information back to the intruders. \(^2\) These programs often remain undetected for months. \(^3\)

Attacks on confidential information held in private systems and networks can pose a direct threat to the economic and national security interests of the United States as well as the security of individuals and companies. Data collected by government agencies and by private information security experts over the past half-decade indicate a serious rise in state-sponsored hacking activities. \(^4\) “Attribution” techniques—which allow investigators to detect where cyber attacks originate—have improved, and information security experts have linked many recent attacks on private organizations to state-sponsored actors. \(^5\) A 2013 National Intelligence Estimate identified state-sponsored hacking as a chief threat to the country’s economic competitiveness. \(^6\) The report represents the consensus view of the United States intelligence community and describes a wide range of sectors that have been the focus of hacking over the past five years, including the financial, information technology, aerospace, and automotive sectors. \(^7\)

---


3. Id.


5. MANDIANT APT1, supra note 2; See also JAMES R. CLAPPER, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 2-3 (Mar. 12, 2013) (“State and non-state actors increasingly exploit the Internet to achieve strategic objectives.”).


7. Id.
As security experts in aggressively targeted sectors have ramped up security efforts, the information security firm Mandiant reports that state-sponsored hackers have broadened their sights to include outside vendors and the business partners of high-value targets. Mandiant’s comprehensive report on information security in the private sector points to an increase in attacks on the computer systems and networks of firms engaging in outsourced tasks, such as information technology, human resources, financial, and legal services.

Because law firms work with thousands of clients across numerous industry sectors, cyber intruders see law firms as lucrative storehouses of sensitive information. Companies seek counsel when they are engaged in deeply sensitive and highly expensive matters, which tend to generate information that is potentially of great value to third parties. Financial details concerning a merger or acquisition can give any interested outside entity an advantage in future negotiations. Similarly, lawyers have access to details about an organization’s inner workings in the midst of litigation. Such information enables competitors to assess the financial stability of an organization and gain other tactical information. Furthermore, a firm’s litigation strategy is often outlined in various intra-firm communications. These documents provide significant advantage to opposing parties or interested third parties when computer systems or networks are successfully breached.

Law enforcement authorities in the United States, Canada, and the UK have all noted the rise in threats to law firm information systems. In November 2011, the Federal Bureau of Investigation (“FBI”) convened 200 large law firms in New York City to urge them to review their cybersecurity policies. In 2012, the Director General of the British MI-5 informed the 300 largest companies in the UK that their information was as likely to be stolen from the computers of their attorneys and international consultants as from their own. The FBI does not track individual breaches or keep statistics on the types of businesses attacked, but a 2012 Mandiant report estimated that 80% of the 100 largest United States law firms were subject to successful data breaches by malicious intruders in 2011 alone.

B. A Threat to Attorney-Client Confidentiality

Consistent with its commitment to client protection, the ABA is committed to defending the confidentiality of lawyer-client communications against these new threats. Protecting confidences is imperative for both ethical and practical reasons. Preservation of client confidentiality is widely recognized as fundamental to the ability of lawyers to successfully represent their clients’ interests. Clients must be secure in their ability to share confidential information with their lawyers, and the preservation of the confidentiality of lawyer-client communications is crucial to public confidence in the legal system. The legal profession, the

---

9 Id.
legal system, and foreign and domestic actors should not ignore this important facet of the attorney-client relationship.

The involvement of nation states in targeting confidential legal information is particularly troubling. Basic principles of due process and even human rights may be violated when confidential communications are breached by such intrusions. As protectors of the rule of law and the integrity of those who practice law, the ABA and the United States legal community condemn such intrusions and the organizations and nations engaged in this conduct.

III. A Strong United States and International Response

Widespread intrusions into the computer systems and networks of law firms deeply threaten clients, the legal profession and our system of justice. The United States has acknowledged that private actors and foreign governments disregard this essential aspect of legal representation when they systemically steal information, threaten access to information, or improperly modify information to the disadvantage of clients. The ABA urges the United States government and international community to speak out against these intrusions and to counter them with decisive action. In addition, the ABA urges not just the federal government, but state, local, territorial, and tribal governmental bodies as well, to examine, and if necessary, amend or supplement, any existing laws as may be necessary to deter and punish those who launch these unauthorized, illegal intrusions into the computer systems and networks of lawyers and law firms.

A. Importance of Protecting Client Confidences

Preserving the confidentiality of the attorney-client relationship is a bedrock principle of the American Bar Association. However, widespread security breaches expose client confidences and erode trust. This in turn jeopardizes the ability of lawyers to carry out their critical role in the legal system. The obligation of lawyers to maintain confidentiality, a fiduciary duty of the highest order, is expressed in the common law, the applicable rules of professional conduct, the attorney-client privilege and the work product doctrine.

1. Confidentiality, the Attorney-Client Privilege and the Work Product Doctrine

The fiduciary duty of confidentiality of an agent, particularly a lawyer, vis-à-vis the lawyer’s client, has historical roots in the common law. It remains a common law duty, but today it is also codified in the rules of professional conduct of every jurisdiction in the United States, in essentially the same form as one finds it in the ABA Model Rules of Professional Conduct (“Model Rules”). The duty of confidentiality, which applies to any voluntary act by a lawyer, is extremely broad in its Model Rule incarnation, protecting all information relating to the representation, even if that information has been otherwise disclosed in public documents. The Model Rules provide narrow exceptions that permit, but do not require, lawyer disclosure of confidential client information. Such exceptions include but are not limited to when the lawyer

reasonably believes disclosure is necessary to prevent reasonably certain death or serious bodily harm, to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial financial injury to another and for which the client has used or is using the lawyer’s services, to consult with another lawyer about the lawyer’s compliance with the Rules, and to comply with other law or a court order.\textsuperscript{13}

The attorney-client privilege is the oldest common law privilege for confidential communications, dating to 16\textsuperscript{th} century England. It is a privilege whose underlying purpose is to enable persons to seek and lawyers to provide candid legal advice through unfettered communication between lawyer and client without fear that those communications will be disclosed to others. The availability of the privilege is considered indispensable to effective lawyer advocacy on behalf of clients in every representation, both before tribunals and elsewhere. In a landmark case regarding attorney-client privilege, the Supreme Court noted “full and frank communication between attorneys and their clients” also “promote[s] broader public interests in the observance of law and administration of justice.”\textsuperscript{14}

Attorney-client communications are generally only privileged if the communication was for the purpose of enabling the client to secure legal assistance and was made outside the presence of third parties. Some exceptions to the privilege include communications unrelated to the representation, non-legal advice, and advice in furtherance of an illegal activity.\textsuperscript{15} The privilege is also lost if the client knowingly waives the privilege on informed consent.\textsuperscript{16} However, the attorney-client privilege cannot be lost simply because a government agency or other third party claims they need to know the client’s communications with a lawyer. If this exception were adopted, clients could not know whether their communications would be privileged in advance. As a result, clients would likely withhold crucial facts from their lawyers and fail to receive the advice they need to conform their conduct to the law.

The work product doctrine protects the work product of an attorney developed in anticipation of litigation.\textsuperscript{17} Like the attorney-client privilege, the doctrine is rooted in ensuring effective legal representation by preventing the exposure of certain lawyer work product material to adversaries. However, the doctrine’s main purpose is to allow the lawyer to thoroughly prepare for litigation. Thus, while not all attorney-client privileged communications are work product (because they do not occur in anticipation of litigation), work product is in a certain sense broader because it covers communications with non-clients as well as clients, if undertaken in anticipation of litigation. Another key difference is that both the attorney and client may claim ownership of the work product while the attorney-client privilege belongs solely to the client.\textsuperscript{18}

2. Confidentiality Obligations in Cyberspace

\textsuperscript{13} See MODEL RULES OF PROF’L CONDUCT R. 1.6(b) (2013).


\textsuperscript{15} See Clark v. U.S., 289 U.S. 1, 15 (1933); U.S. v. Bob, 106 F.2d 37, 40 (2d Cir. 1939).


\textsuperscript{18} Id., at 490.
Recent technological advances create new and unique legal challenges. The American Bar Association is already providing leadership and guidance on protecting client information from cybersecurity breaches and balancing important policy goals. Lawyers have a responsibility to develop and maintain systems that will effectively secure client information and firm computer networks. Lawyers must also dedicate themselves to staying competent in cybersecurity to better represent clients who are victims of cybercrimes.

The legal profession has historically provided leadership and played an essential role in preserving legal rights and, ultimately, the rule of law. The complexity and severity of cybersecurity threats only make the legal profession's involvement more necessary. In August 2005, the ABA House of Delegates unanimously approved Resolution 111, which broadly addressed attorney-client principles. The resolution reaffirmed the preservation of the attorney-client privilege and work product doctrine as central to maintaining the confidential lawyer-client relationship. The key public benefits can be summarized as follows:

1. Promoting voluntary legal compliance.
2. Encouraging client candor.
3. Ensuring effective client advocacy.
4. Ensuring access to justice.
5. Promoting efficiency in the American adversarial legal system.

The principles of the attorney-client privilege and work product doctrine must be protected in the context of cyber intrusions. However, lawyers must also develop policies that strike the right balance between client-attorney confidentiality and necessary access to protected information. The client information implicated in a law firm cyber intrusion may be relevant in attempting to determine the perpetrator who exposed the privileged information in the first place. Reconciling these competing objectives will require thoughtful debate and patience from the legal community.

B. Potential Government Actions to Reduce Cyber Intrusions

The United States government has an obligation to help protect the computer systems and networks of American companies and citizens from unlawful intrusion. In order to combat the new and significant threats of cyber attacks, the government should evaluate a full spectrum of law enforcement, military, diplomatic, intelligence, and economic measures to pressure cyber-espionage actors into stopping their attacks. This Report notes a number of tools that United States authorities may consider, including increased investigations to hold hackers accountable, high-profile diplomatic actions, economic sanctions, and use of visa authority.

1. Renewed Focus on Investigations

Government criminal and civil investigations should use law enforcement and intelligence authorities to penetrate hacker networks. Litigants and lawyers who participate in or abet cyber intrusions should also be sanctioned and prosecuted. Such conduct by lawyers should also be

19 See e.g., MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. & R. 1.6(c) (2013) (as adopted in August 2012).
subject to review by lawyer disciplinary authorities. The United States Department of Justice ("DOJ") prosecutes cyber-espionage primarily through the National Security Division and the Criminal Division’s Computer Crime and Intellectual Property Section. DOJ should prioritize and devote more resources to cybercrime, including attacks on law firms. For example, DOJ’s National Security Division may begin indicting suspected state-sponsored hackers, in part as a deterrent strategy. Although nation states are not likely to turn over their citizens to the United States for criminal prosecution, the specific legal action makes it more difficult for a hacker’s state-sponsor to deny a problem exists. The action would give the United States additional leverage in diplomatic negotiations. The indictments would also have the benefit of discouraging suspected hackers from traveling freely because foreign governments could easily turn them over to United States law enforcement.

The United States could reemphasize mutual international assistance for investigatory powers under the Convention on Cybercrime. In 2001, the Convention of the Council of Europe codified international best practices for legal frameworks protecting against cybercrime. The United States has both signed and ratified the Convention. Article 25 states “parties should afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data.” As a practical matter, this principle of active cooperation remains extremely relevant to the world of cyber-espionage.

Cyber intrusion investigations would also greatly benefit from domestic public-private cooperation. Since private companies are frequent victims of cybercrimes, they often possess the motivation and creativity to bolster the government’s efforts. In particular, the private sector could supplement the government’s relative lack of financial resources. This may include using a private investigator in place of a government investigator. A compromised company can also volunteer information on the cyber intruder’s nature, goals, tactics, and potential vulnerabilities.

Diplomatic Responses

The United States should lead a multinational coalition of countries that have been major targets of cyber attacks to discourage such attacks, including those against lawyers and law

---

24 Satola, supra note 23, at 1772-73.
25 CONVENTION ON CYBERCRIME, supra note 22.
firms.\textsuperscript{27} Using a collaborative approach through bilateral and multilateral diplomacy, the U.S. should encourage development of an international code of conduct to combat cyber intrusions. At his January 2013 nomination hearing, Secretary of State John Kerry mentioned the need to “engage in cyber diplomacy and cyber negotiations and try to establish rules of the road that help us to be able to cope” with the challenges of foreign hackers.\textsuperscript{28}

When cooperation is not feasible, the United States should take a firmer diplomatic tone with nation states implicated in attacks on the computer systems and networks of American law firms. “The international community cannot tolerate such activity from any country,” said National Security Advisor Thomas Donilon regarding cyber intrusions in March 2013 remarks to the Asia Society.\textsuperscript{29} With proper attribution, the international community could bring negative publicity to state-sponsored hackers. This in turn could persuade specific countries and private companies to raise complaints with the offending nation state. Along those lines, the United States government should continue to press cyber-espionage actors at the highest levels of diplomacy. All state-sponsors of cyber attacks should recognize the urgency of the problem and acknowledge the need to prevent widespread cybercrimes. The United States can encourage these nation states to conduct their own investigations, prioritize domestic anti-hacking enforcement, and expose the individuals responsible for specific intrusions.

3. Other Government Sanctions and Tools

The United States government could also consider serious measures such as economic sanctions or asset forfeitures against those involved in cyber intrusions, or the strategic use of visa authority vis-à-vis foreign nationals. The Treasury Department’s Office of Foreign Assets Control (“OFAC”) administers sanctions against targeted foreign actors.\textsuperscript{30} OFAC accomplishes key national security goals by imposing controls on transactions and freezing assets under United States jurisdiction.\textsuperscript{31} OFAC’s legal authority derives from presidential national emergency powers and specific legislation.\textsuperscript{32} Many of the sanctions are based on United Nations resolutions and other international mandates. The Computer Fraud and Abuse Act (“CFAA”) also authorizes the criminal forfeiture of any personal property or interest in personal property derived from illegal


\textsuperscript{28} Testimony of John Kerry, \textit{Hearing on the Nomination of John Kerry to be Secretary of State}, Senate Foreign Relations Committee 112\textsuperscript{th} Congress (Jan. 24, 2013).


\textsuperscript{31} Id.

\textsuperscript{32} See 50 U.S.C. § 1702 (a)(1)(B), (C) (2012) (granting authority to the President to declare an economic emergency and then impose sanctions).
activity. Additionally, the Obama administration has proposed amending the CFAA to include a civil forfeiture provision.

Visas too could be used either as a carrot or a stick. At the Attorney General’s discretion, DOJ can issue S-5 criminal informant visas to foreign nationals possessing “critical reliable information concerning a criminal organization.” Meanwhile, the Department of Homeland Security has the authority to adopt a policy of denying or canceling visas to individuals involved in cyber-espionage, including researchers.

C. Protecting Client Confidentiality During Investigations

Confidential client information should be protected during any cyber intrusion investigation, consistent with ethics rules and to prevent the erosion of the attorney-client privilege and work product doctrine. Assisting such government investigations is important, but law enforcement should seek ways to conduct investigations without breaching confidentiality. If private investigators are going through compromised computer systems and networks instead of government investigators, they too must take steps to avoid disclosing the client’s information. Guidelines should also ensure client confidences are not used in unrelated investigations, unless the privilege or work product protection is waived by the client’s consent. Privileged and confidential client information from law firm systems and networks should not be permitted to be used in prosecutions or civil enforcement cases against the client and third parties. This protection should also extend to government agency inquiries related to intelligence or national security.

Government efforts to combat cyber attacks should comport with ABA’s long-standing commitment to the principle of attorney-client confidentiality. Both parties suffer when the foundation of the attorney-client relationship is threatened. The exposure of information to government agencies or private parties creates a chilling effect on client-attorney communication and reduces client candor. Such exposure also discourages voluntary legal compliance and information-sharing in cybercrime investigations. This is especially problematic as companies conducting internal investigations increasingly rely on law firms’ attorney-client privilege.

IV. Ethical and Professional Obligations for Computer Security

The wealth of confidential data maintained in lawyers’ computers and information systems faces substantial and very real security risks. It is critical for all lawyers to understand and

address these risks to ensure they comply with their legal, ethical, and regulatory obligations to safeguard client data. The ABA Model Rules of Professional Conduct provide guidance to lawyers regarding their ethical obligations about preventing the unauthorized disclosure of and unauthorized access to confidential client information and responding to a breach should it occur. This Resolution, in the final Further Resolved clause, reminds lawyers and law firms of the importance of reviewing and complying with applicable ethics rules and also other law that governs their conduct in the cybersecurity context.

A. Protection of Information Systems

There are two main duties implicated in the protection of confidential client information from inadvertent disclosure or unauthorized access: (1) the duty of competence under Model Rule 1.1, and (2) the duty of confidentiality under Model Rule 1.6.

1. Duty of Competence: Model Rule 1.1

Model Rule 1.1 provides that a lawyer shall provide “competent representation” to a client. This requires “the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” In August 2012, the House of Delegates adopted amendments to the Comments to Model Rule 1.1 at the recommendation of the ABA Commission on Ethics 20/20 to highlight the importance of technology to legal practice. Comment [8] to Model Rule 1.1 now states that a lawyer “should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . .” The amendment does not impose new obligations on lawyers. Rather, it is intended to highlight the growing significance of technology to legal practice and emphasize a lawyer’s responsibility to stay informed.

The duty is not necessarily for lawyers to become technological experts, but to ensure that they understand the impact of technology on the activities of a client or law firm. Technical proficiency implicates not only adequate protection of confidential information, but providing adequate advice to clients on technological matters including protection of the client’s own data.

The Report of ABA Ethics 20/20 Commission explaining the amendment noted that a lawyer should understand the basic features of relevant technology, such as how to create an electronic document and how to use email, in order to ensure clients receive competent and

---

39 Jon M. Garon, Technology Requires Reboot of Professionalism and Ethics for Practitioners, 16 J. INTERNET L. 3 (2012).
41 Garon, supra note 39.
42 CURATO, supra note 38.
efficient legal services. Some suggest that the level of knowledge a lawyer should obtain will depend on factors such as the types and sensitivity of data collected by the lawyer or law office in each particular area of practice.

Attorneys have an obligation to safeguard information relating to clients. This may include approaching information security as a process, understanding the limitations in attorneys' competence, obtaining appropriate assistance, continuing security training and awareness, and reviewing technology, threats, and available security options as they evolve over time. Flexibility is required to allow obligations to grow and develop alongside technological advancement.

Many law firms and lawyers already rely on IT to assist them in relevant technology and training. Lawyers who do not do so already may want to consult with technological experts to ensure that they are adequately keeping pace with rapidly changing technology and related security threats. Additionally, law firms might benefit by increasing the number of nonlawyers devoted to safeguarding information and training attorneys in how to prevent accidental disclosure or unauthorized access.

2. Duty of Confidentiality: Model Rule 1.6

A lawyer has an ethical duty to take reasonable measures to protect a client’s confidential information from unauthorized access and disclosure. Under Model Rule 1.6, lawyers must take "reasonable precautions" to safeguard "information relating to the representation of a client."

The ABA amended Model Rule 1.6 in August 2012 to require that this duty extend to client information in computers and information systems. New paragraph (c), states, "[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." However, an inadvertent disclosure or breach alone does not constitute a violation of the rule if reasonable precautions have been taken. Notably, the new black letter Rule and Comment did not change any ethical obligations. It simply made the prevailing understanding of the obligations explicit and clear in light of new technology.

Defining the "reasonable precautions" lawyers must take to protect data poses a challenge. The specific administrative, technical, or physical safeguards required for a client's information will vary from situation to situation. Additionally, what is "reasonable" will change as technology

---

47 Id.
48 MODEL RULES OF PROF'L CONDUCT R. 1.6 (2013).
49 MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2013).
changes. Comment [18] provides guidance as to what is “reasonable” by identifying some of the factors that would dictate heightened security and require greater precaution. These standards include the:

1. Sensitivity of the information
2. Likelihood of disclosure if additional safeguards are not used
3. Cost of using additional safeguards
4. Difficulty of using the safeguards
5. Extent to which the safeguards adversely affect the ability to represent the client (e.g., by making a device or important piece of software excessively difficult to use).

Lawyers may develop greater clarity and specificity with individual clients through contractual agreements and waivers. Indeed, Comment [18] states that a client may require the lawyer to use special security measures beyond the requirements of Rule 1.6, or may waive certain security measures that would otherwise be required by the Rule. Comment [19] includes a similar provision. These provisions should be utilized to avoid uncertainty. Significantly, many state bar ethics opinions have indicated that lawyers and law firms should obtain informed consent from the client prior to utilizing any cloud computing or third-party online hosts of confidential client information. Accordingly, these types of agreements may already be relatively common practice for many lawyers and law firms.

Confidentiality also implicates Model Rule 5.3, which provides that lawyers with managerial authority in a law firm must take steps to ensure that all firm employees, including nonlawyers, handle data and use technology in a manner that reasonably safeguards client information. Further, Comment [3] to Rule 5.3 extends the obligation beyond firm staff to vendors and other nonlawyers outside the firm. Many incidences of hacking occur through offsite vendors or the personal computers of employees. In response, lawyers and law firms could develop internal policies and training as part of the “reasonable” precautions utilized to safeguard confidential information and prevent liability.

---

50 CURATO, supra note 38, at 14.
52 CURATO, supra note 38, at 15.
54 CURATO, supra note 38, at 14.
Lawyers should keep informed of state and federal laws governing information security. Comment [18] to Model Rule 1.6 notes that whether a lawyer is required to take additional steps to comply with other laws that govern data privacy is beyond the scope of the Rule. However, there is a burgeoning body of privacy and breach notification laws that apply to lawyers, as well as those who store or transmit electronic information. Lawyers should familiarize themselves and comply with these laws.

B. Legal and Ethical Duties Triggered by a Security Breach

With respect to client communications, when there is a breach of confidentiality, a lawyer may have a duty to disclose that breach under the Model Rules. The ethical obligations of lawyers to disclose breaches to a client are set forth in Model Rule 1.4. Model Rule 1.4 generally discusses a lawyer's duty to communicate with his or her client. Rule 1.4(a) requires keeping the client "reasonably informed about the status of the matter."\textsuperscript{55} Rule 1.4(b) states that a "lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."\textsuperscript{56} Though not explicitly stated, these provisions indicate that in certain circumstances lawyers might have an ethical obligation to provide notice to a client when confidential information relating to the client is compromised.

The general standard for Rule 1.4 is that a lawyer must keep clients informed about material developments. Therefore, lawyers must tell clients that a breach occurred when it is material to their case. However, the scope of the duty to inform remains under review. For example, in 2009, the Illinois State Bar Association took the position that a lawyer may be obligated to disclose a breach to its client "if it is likely to affect the position of the client or the outcome of the client's case."\textsuperscript{57} However, other state bars have either specifically declined to issue direct opinions or have issued opinions that have no clear standard.\textsuperscript{58}

Some of the ambiguity associated with determining when a material breach has occurred can be mitigated by provisions in Rule 1.4 that require obtaining "informed consent."\textsuperscript{59} As part of good practice, a lawyer may want to inform clients of the technology and security practices they utilize so that clients can make informed decisions. Lawyers may also want to provide specialized instructions to clients regarding how a breach or possible breach of confidential information will be handled.\textsuperscript{60} By obtaining informed consent in advance, lawyers and law firms can craft specific terms regarding what constitutes a material breach and when clients will be informed of a breach. Notably, certain legal and regulatory requirements may be stricter than the ethical rules. Thus, it is important that lawyers ensure that consent agreements are in accordance with state and federal laws.


\textsuperscript{56} Id.

\textsuperscript{57} BARKETT, supra note 53.

\textsuperscript{58} Id., at 14.

\textsuperscript{59} MODEL RULES OF PROF'L CONDUCT R. 1.4 (2013).

\textsuperscript{60} Trope & Hughes, supra note 55, at 229 (2011).
Beyond their ethical duties, lawyers may be subject to legal or regulatory requirements for breach notification. 51 Forty six (46) states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws that require any business in possession of certain sensitive personal information about a covered individual to disclose a breach of that information to the person(s) affected. The first federal data breach notification law covers health care. 62 Furthermore, a breach may affect entities and individuals who are not clients. This means that lawyers’ legal obligations may not be limited to information relating to their clients.

V. Conclusion

Information security represents an increasingly important issue for the legal profession. Sophisticated hacking activities on private computer systems and networks, including on those utilized by lawyers and law firms, have increased dramatically over the last decade. These information security breaches expose clients, their lawyers, and society at large to significant economic losses. Further, these breaches undermine the legal profession as a whole by threatening client confidentiality, the attorney-client privilege, and the broader confidential lawyer-client relationship. As the national representative of the legal profession, the ABA should play a leading role in urging the United States and other governmental bodies to discourage, prevent, and punish malicious intrusions into lawyer and law firm computer systems and networks, but only in a fashion that protects these core legal principles and traditional state court regulation and oversight of lawyers and the legal profession. The ethical rules have long imposed certain professional obligations on lawyers and law firms to protect confidential information from breaches, but as technology advances, the legal profession must adapt to meet the demands of clients and ensure that cornerstones of the profession, such as confidentiality, remain intact.

Respectfully submitted,

Judith Miller and Harvey Rishikof
Co-Chairs, Cybersecurity Legal Task Force
August 2013

---

51 LUCY THOMSON, DATA BREACH AND ENCRYPTION HANDBOOK (ABA 2011).
RESOLVED, That the American Bar Association amends the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality as follows (insertions underlined, deletions struck through):

(a) the black letter and Comments to Model Rule 1.0 (Terminology);
(b) the Comments to Model Rule 1.1 (Competence);
(c) the Comments to Model Rule 1.4 (Communication);
(d) the black letter and Comments to Model Rule 1.6 (Confidentiality of Information); and
(e) the black letter and Comments to Model Rule 4.4 (Respect for Rights of Third Parties).

Rule 1.0 Terminology

(a) “Belief” or “believes” denotes that the person involved actually supposed the fact in question to be true. A person’s belief may be inferred from circumstances.
(b) “Confirmed in writing,” when used in reference to the informed consent of a person, denotes informed consent that is given in writing by the person or a writing that a lawyer promptly transmits to the person confirming an oral informed consent. See paragraph (e) for the definition of “informed consent.” If it is not feasible to obtain or transmit the writing at the time the person gives informed consent, then the lawyer must obtain or transmit it within a reasonable time thereafter.
(c) “Firm” or “law firm” denotes a lawyer or 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.
(d) “Fraud” or “fraudulent” denotes conduct that is fraudulent under the substantive or procedural law of the applicable jurisdiction and has a purpose to deceive.
(e) “Informed consent” denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about
the material risks of and reasonably available alternatives to the proposed course of
conduct.

(f) “Knowingly,” “known,” or “knows” denotes actual knowledge of the fact in
question. A person’s knowledge may be inferred from circumstances.

(g) “Partner” denotes a member of a partnership, a shareholder in a law firm
organized as a professional corporation, or a member of an association authorized to
practice law.

(h) “Reasonable” or “reasonably” when used in relation to conduct by a lawyer
denotes the conduct of a reasonably prudent and competent lawyer.

(i) “Reasonable belief” or “reasonably believes” when used in reference to a
lawyer denotes that the lawyer believes the matter in question and that the circumstances
are such that the belief is reasonable.

(j) “Reasonably should know” when used in reference to a lawyer denotes that a
lawyer of reasonable prudence and competence would ascertain the matter in question.

(k) “Screened” denotes the isolation of a lawyer from any participation in a matter
through the timely imposition of procedures within a firm that are reasonably adequate
under the circumstances to protect information that the isolated lawyer is obligated to
protect under these Rules or other law.

(l) “Substantial” when used in reference to degree or extent denotes a material
matter of clear and weighty importance.

(m) “Tribunal” denotes a court, an arbitrator in a binding arbitration proceeding
or a legislative body, administrative agency or other body acting in an adjudicative
capacity. A legislative body, administrative agency or other body acts in an adjudicative
capacity when a neutral official, after the presentation of evidence or legal argument by a
party or parties, will render a binding legal judgment directly affecting a party’s interests
in a particular matter.

(n) “Writing” or “written” denotes a tangible or electronic record of a
communication or representation, including handwriting, typewriting, printing,
photostating, photography, audio or videorecording, and e-mail electronic
communications. A “signed” writing includes an electronic sound, symbol or process
attached to or logically associated with a writing and executed or adopted by a person with
the intent and sign the writing.

Comment

... Screened

... [9] The purpose of screening is to assure the affected parties that confidential information
known by the personally disqualified lawyer remains protected. The personally disqualified
lawyer should acknowledge the obligation not to communicate with any of the other lawyers in
the firm with respect to the matter. Similarly, other lawyers in the firm who are working on the
matter should be informed that the screening is in place and that they may not communicate with
the personally disqualified lawyer with respect to the matter. Additional screening measures that
are appropriate for the particular matter will depend on the circumstances. To implement,
reinforce and remind all affected lawyers of the presence of the screening, it may be appropriate
for the firm to undertake such procedures as a written undertaking by the screened lawyer to
105A Revised

avoid any communication with other firm personnel and any contact with any firm files or other
materials, information, including information in electronic form, relating to the matter, written
notice and instructions to all other firm personnel forbidding any communication with the
screened lawyer relating to the matter, denial of access by the screened lawyer to firm files or
other materials, information, including information in electronic form, relating to the matter, and
periodic reminders of the screen to the screened lawyer and all other firm personnel.

... 

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

... 

Maintaining Competence

[6] 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 1.4 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

... 

Communicating with Client

[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.
236

Client telephone calls should be promptly returned or acknowledged. A lawyer should promptly respond to or acknowledge client communications.

...  

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; or

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

(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

...  

Acting Competently to Preserve Confidentiality

[16] Paragraph (c) requires a lawyer must 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 or entities 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, confidential 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].

[17] 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.

...  

Rule 4.4 Respect for Rights of Third Persons

(a) In representing a client, a lawyer shall not use means that have no substantial
purpose other than to embarrass, delay, or burden a third person, or use methods of
obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document or electronically stored information relating
to the representation of the lawyer’s client and knows or reasonably should know that the
document or electronically stored information was inadvertently sent shall promptly notify the sender.

Comment

...  

[2] Paragraph (b) recognizes that lawyers sometimes receive a document or
electronically stored information that was mistakenly sent or produced by opposing parties
or their lawyers. A document or electronically stored information is inadvertently sent when it is
accidentally transmitted, such as when an email or letter is misaddressed or a document or
electronically stored information is accidentally included with information that was intentionally
transmitted. If a lawyer knows or reasonably should know that such a document or electronically
stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the
sender in order to permit that person to take protective measures. Whether the lawyer is
required to take additional steps, such as returning the document or electronically stored
information or original document, is a matter of law beyond the scope of these Rules, as is the
question of whether the privileged status of a document or electronically stored information has
been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a
document or electronically stored information that the lawyer knows or reasonably should know
may have been wrongfully inappropriately obtained by the sending person. For purposes of this
Rule, "document or electronically stored information" includes, in addition to paper documents,
e-mail and other forms of electronically stored information, including embedded data (commonly
referred to as "metadata"), that is e-mail or other electronic modes of transmission subject to
being read or put into readable form. Metadata in electronic documents creates an obligation
under this Rule only if the receiving lawyer knows or reasonably should know that the metadata
was inadvertently sent to the receiving lawyer.

[3] Some lawyers may choose to return a document or electronically stored information
unread, for example, when the lawyer learns before receiving it the document that it was
inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do
so, the decision to voluntarily return such a document or electronically stored information is a
matter of professional judgment ordinarily reserved to the lawyer. See Rules 1.2 and 1.4.
RESOLUTION

RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.
EXECUTIVE SUMMARY

1. **Summary of the Resolution**

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the U.S. It encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. This Resolution and Report are intended to educate organizations and heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers’ rules of professional conduct.

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical.

2. **Summary of the Issue that the Resolution Addresses**

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the U.S. The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. The consequences of a cyber incident or data breach can have a disturbing impact on the victim, whether a business, organization, government entity, or an individual. It is thus appropriate to encourage all organizations—whether private or public—to develop, implement and maintain an appropriate cybersecurity program. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization or entity had undertaken proper cybersecurity planning and implemented appropriate security safeguards.

2. **Please Explain How the Proposed Policy Position Will Address the Issue**

Through this Resolution, the ABA highlights the importance of cybersecurity plans for private and public sector organizations as a matter of sound governance and risk management. This Resolution and Report will educate organizations, heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers’ rules of professional conduct.

4. **Summary of Minority Views**

This Resolution and report have been revised in response to input received from several ABA entities. No minority views have come to our attention with respect to the revised report.
I. INTRODUCTION

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the United States (U.S.). It encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. This Resolution and Report are intended to educate organizations and heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers' rules of professional conduct.

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical.

II. CYBERSECURITY THREATS -- BACKGROUND

The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. Cyber-criminals exploit weaknesses in software and operating platforms, the domain name system, and mobile and web-based applications. They conduct successful social engineering through phishing attacks, social media, email, and various applications. Malware can quickly morph, change security controls, lurk in systems undetected, download other malware, and exfiltrate data undetected.

An organization-wide cybersecurity program with defined controls based on risk categorizations reflecting the operational impact and magnitude of harm of a cyber incident can mitigate risk to a considerable degree. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper security planning and implemented appropriate security safeguards.

In today's digital world, threats to data and information systems are found almost everywhere a computer, server, smart phone, thumb drive, or other electronic device is operating (including the cloud). Many organizations provide access to their networks to business partners and entrust their data and business functions to outsourcing and cloud providers, creating additional risks. The proliferation of mobile devices and wireless technologies that enable mobile commerce and a continually expanding array of applications—more than 1.5 million—also present vulnerable points in the flow of sensitive data in computer networks.

Security is only as strong as its weakest link. Failed security has resulted in thousands of data breaches that have led to the loss or compromise of millions of personally identifiable records, as well as the theft of classified information, valuable intellectual property and trade secrets, and the
compromise of critical infrastructure.\(^1\) The consequences of a cyber incident or data breach can have a disturbing impact on the victim, whether a business, organization, government entity, or an individual.

The protection of one of the most valuable and vulnerable assets of all organizations—its information—is not only vitally important, but it also avoids the high costs associated with cybercrime, including forensic investigations and data breach notification; the loss of confidential, classified, and proprietary data; reputational damage; loss of public confidence; and in the case of business, drops in stock price, and loss of market share and trust. Breaches also have resulted in the disclosure of closely-held government information, and businesses have faced regulatory fines and investigations, civil damage actions, administrative proceedings, and criminal indictments. The first- and third-party losses associated with security incidents are rising, and cybersecurity is now one of the top risks organizations must manage.

**Sensitive Data At Risk**

There are many types of sensitive data that are targeted by cyber-criminals or subject to unauthorized access, use, disclosure, or sabotage by insiders. They include personally identifiable information (PII), personal health information (PHI), and financial records, confidential and proprietary business data, intellectual property and trade secrets, research data, privileged legal documents, and classified information (including sensitive national security information). There is a vibrant market for these data, and all organizations—regardless of size—should consider themselves at risk.

The sensitive personal data being amassed by companies and governments is staggering. Inexpensive storage has enabled companies to collect and store large amounts of data and retain it far longer than they would have if it were in paper. “Big data,” the term applied to the collection of massive amounts of data that can be correlated, analyzed, and parsed for targeted advertising and strategic business purposes, creates rich targets for cyber-criminals. PII that can be used for fraud is being collected and often stored by organizations unprotected, putting many Americans at risk.\(^2\) On its website, the Internal Revenue Service (IRS) indicates that it “has seen a significant increase in refund fraud that involves identity thieves who file false claims for refunds by stealing and using someone’s Social Security number.”\(^3\)

Another aspect of the problem is illustrated by the dependence of American society on electronic transactions and e-commerce, which has fueled data breaches in all industry sectors. Failed security has resulted in massive data breaches of millions of personally identifiable records.\(^4\) The recent data breaches of leading retail companies and credit bureaus have caught the attention of the public, politicians, and law enforcement. The success of these breaches, however, has also

---


created a “me too” among cyber-criminals eager to capture their own trove of data. Risks will increase with the “Internet of Things,” as the Internet becomes the backbone for appliances, gadgets, and operational aspects of daily life. Many of the most personal aspects of people’s lives will be documented and transmitted over the Internet, subject to interception or theft.

Protecting the Nation’s Critical Infrastructure

The national and economic security of the United States depends on the reliable functioning of critical infrastructure: cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers.  


Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, issued in February 2013, advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. Comprehensive cybersecurity programs are essential for critical infrastructure organizations, and following appropriate security frameworks and standards is central to achieving a strong cybersecurity posture and resilience. The electric sector, for example, voluntarily agreed to comply with cybersecurity requirements promulgated by the North American Electric Reliability Corporation and the Federal Energy Regulatory Commission (NERC/FERC).

The National Institute of Standards and Technology (NIST) recently published the Framework for Improving Critical Infrastructure Cybersecurity, and mapped the Framework to other accepted security frameworks and standards.

Law Firms Are Targets of Cyber Attacks

The threat of cyber attacks against law firms is growing. Lawyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices. There are many reasons for hackers to target the information being held by law firms. They collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery.

The data and information kept by law firms are largely protected by the attorney-client privilege and/or the work product doctrine, as well as by various legal ethics requirements. Thus, lawyers and law firms should implement an appropriate cybersecurity program to protect confidential and sensitive information.

Both large and small law firms have been the target of hacker attacks in the U.S. as well as abroad. The FBI has issued warnings to firms and held a meeting in early 2012 with approximately 200 law firms in New York City to discuss the risk of breaches and theft of client data. A cybersecurity firm that helps organizations secure their networks against threats and resolve computer security incidents estimated that 80 major law firms were breached in 2011 alone.

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (2013) provides threat information, practical guidance and strategies to lawyers and law firms of all sizes, and explores the relationship and legal obligations between lawyers and clients when a cyber-attack occurs. Amendments to the ABA Model Rules of Professional Conduct (Model Rules) adopted in 2012 provide that a lawyer’s duty of competence includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology (Comment [8] to Model Rule 1.1). Further, to enhance the protection of client confidential information, Model Rule 1.6 (Confidentiality) provides that 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.” The touchstone regarding lawyers’ obligations under Model Rules 1.1 and 1.6 is reasonableness. What is reasonable depends on the circumstances. With regard to data security, the Comments to Model Rule 1.6 provide lawyers with a nonexclusive list of factors designed to help them assess the reasonableness of their actions.

III. CYBERSECURITY PROGRAM—FRAMEWORKS AND STANDARDS

There are a number of accepted frameworks and standards that can serve as a reference for developing, implementing, and maintaining an appropriately-tailored cybersecurity program. Some of these well-known frameworks and standards include:

- Information Technology Infrastructure Library (ITIL), http://itil-officialsite.com

---


- International Society of Automation (ISA), http://www.isa.org
- ISACA, COBIT, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
- U.S. Nuclear Regulatory Commission, nrc-stp.orl.gov/slo/regguide571.pdf

These references are generally consistent, and a number of the provisions in the various security frameworks and standards map to one another. Thus, it is less important which framework or standard an organization might choose to follow and more important that it undertakes the key activities of a cybersecurity program.

A cybersecurity program is comprised of a series of activities. These activities include, for example: governance by boards of directors and/or senior management; development of security strategies, plans, policies and procedures; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training.

Due to the nature of the threat environment, certain activities in a cybersecurity program are ongoing. Continuous monitoring and log analysis are designed to provide data that can provide early detection of threats. To maintain a proactive security posture, potential threats should be investigated and targeted attacks detected in advance or addressed as they occur. The objective is to address cybersecurity threats and risks in a timely, disciplined, and structured fashion.

Privacy compliance requirements should be incorporated into the cybersecurity program. In addition, an effective cybersecurity program requires trained personnel to evaluate the security impact of actual and proposed changes to the system, assess security controls, correlate and analyze security-related information, and provide actionable communication of the security status across all levels of the organization.

Administrative, technical, organizational and physical controls help ensure the confidentiality, availability, and integrity of digital assets. Such controls should be carefully determined,
implemented, and enforced. NIST has published extensive guidance on the selection of controls for government systems, which can also be useful for private sector organizations.\(^\text{10}\)

Many organizations are undertaking some of the required cybersecurity activities, but not others, and some activities may be performed without all the critical inputs. In such cases, the resulting cybersecurity program could have gaps and deficiencies and associated risks that may adversely affect the organization’s operations, financial bottom line, and compliance. To help protect against massive data breaches or loss of confidential/proprietary data, organizations—whether private or public—should continually work to assess and improve their security posture, in light of the most recent guidance and recommendations on cybersecurity programs.

**Small Organizations**

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical. Small organizations, including small law firms and solo practitioners, can prioritize key cybersecurity activities and tailor them to address the specific risks that have been identified. For example, NIST has provided guidance on information security for small businesses.\(^\text{11}\) Similarly, the U.S. Department of Health and Human Services (HHS) has accorded flexibility in its HIPAA Security Series guidance for the needs of small covered entities.\(^\text{12}\)

**IV. RISK-BASED ASSESSMENT—AN ACCEPTED BUSINESS PROCESS**

Organizational risk can include many types of risk (e.g., management, investment, financial, legal liability, safety, logistics, supply chain, and security risk). Security risks related to the operation and use of information systems is just one of many types of organizational risk. This Resolution focuses on one aspect of a comprehensive enterprise risk management program—operational and IT/cybersecurity risk.

Risk assessments inform decision-makers and support the risk management process by identifying: (i) relevant threats to the organization or threats directed through third party entities; (ii) vulnerabilities both internal and external to the organization; (iii) the impact (i.e., harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a categorization of risk according to the degree of risk and magnitude of harm to the organization flowing from the threat or vulnerability if it occurred.

---


Cybersecurity is based on a systematic assessment of risks that are present in a particular operating environment. Ensuring the confidentiality, integrity, and availability of digital assets is fundamental to their protection. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed.

Risk assessments are the basis for the selection of appropriate security controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level. The principal goal of the organization’s risk management process should be to protect the organization and its ability to perform its mission, not just to protect its IT assets.

Risk assessment is not new to most businesses. It is a fundamental business process that many have been following since at least 1977 when Congress enacted the requirement in the Foreign Corrupt Practices Act of 1977 (FCPA), 15 U.S.C. §§ 78dd-1, et seq., that public companies have internal controls. Nearly all rely on the COSO Framework to comply with the internal control reporting requirements under the FCPA and the Sarbanes-Oxley Act of 2002, PL 107-204, 116 Stat 745. The framework, issued in 1992 and updated in 2013, is designed to assist companies in structuring and evaluating controls that address a broad range of risks. It is geared to the achievement of three important objectives—operations (operational and financial reporting goals, and safeguarding assets from loss, the objective of an effective cybersecurity program), reporting (financial and non-financial), and compliance (with laws and regulations).

Risk assessments for publicly-traded companies are addressed in the Securities and Exchange Commission (SEC) guidance on *Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents.*

Examples of cybersecurity risk management frameworks and standards include:

- **ISO/IEC 27005:2011: Information Security Risk Management.** It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the implementation of information security based on a risk management approach.

- **ISO/IEC 31000:2009: Risk Management—Principles and Guidelines.** This document is intended to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

- *Managing Information Security Risk, Organization, Mission, and Information System View,*

---

13 The Committee on Sponsoring Organizations of the Treadway Commission ("COSO"), an initiative of several groups with an interest in effective internal control, available at http://www.coso.org.
NIST Spec Pub 800-39 (March 2011)\textsuperscript{17} and Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Spec Pub 800-37 Rev. 1 (February 2010).\textsuperscript{18} These publications provide guidance for developing an integrated, organization-wide process for managing risk that includes the activities of security categorization; security control selection, implementation, and assessment; information system authorization; and security control monitoring.

- **Critical Sectors—DHS Infrastructure Risk Management Approach.**\textsuperscript{19} This guidance provides a useful approach to critical infrastructure risk management utilizing a risk management framework enunciated by DHS. It is designed to be applied to all threats and hazards, including cyber incidents, natural disasters, man-made safety hazards, and acts of terrorism, although different information and methodologies may be used to understand each. Risk information allows partners, from facility owners and operators to federal agencies, to prioritize their risk management efforts.

- **DOE Electricity Subsector Cybersecurity Risk Management Process (RPM).**\textsuperscript{20} The electricity subsector increasingly relies on digital technology to reduce costs, increase efficiency, and maintain reliability during the generation, transmission, and distribution of electric power. Managing cybersecurity risk is critical to achieving their strategic goals and objectives, including reliability, resiliency, security, and safety. Issued by the Department of Energy in conjunction with NIST and NERC, this guidance is designed to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks.

V. **CYBERSECURITY PROGRAM—CYBER RESPONSE PLANS**

Incident response is the practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference. Fully developed and tested incident response plans and business continuity/disaster recovery (BC/DR) plans are components of a cybersecurity program. Organizations should be prepared if a cyber attack or data breach occurs or if an event interrupts their operations. Response plans, policies, and procedures should be able to accommodate the full array of threats, not just data breaches.

Incident response plans involve stakeholders across an organization, including IT, security, legal, finance, operational units, human resources, and procurement. The individuals should be identified and their roles and responsibilities defined. Communication with and coordination among stakeholders is an important aspect of an incident response plan. This includes the identification of who within an organization should be responsible for communicating with

employees, customers, and other key groups (e.g., investors). It would also include plans for appropriate external communications, such as with first responders, forensic investigation experts, Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers (ISACs), regulators, communications providers, and outside counsel.

If litigation is anticipated, adequate documentation and evidentiary procedures for incident response can be very important. This advance planning can help to ensure that valuable tracking and tracing data and evidence of what happened within a system are preserved and secured and chain of custody is documented.

For many organizations, adequate incident response planning is a compliance requirement. For example, those organizations subject to the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), or state data breach laws.

Resources are available to assist organizations in understanding the key components of incident response. NIST, for example, has published an excellent guide, the *Computer Security Incident Handling Guide*, and Carnegie Mellon has issued the *Handbook for Computer Security Incident Response Teams*.

*Business Continuity Management*—The other critical cyber response plan for a cybersecurity program is a business continuity/disaster recovery plan. Although they are commonly lumped together as BC/DR, there are separate processes for business continuity and disaster recovery. A cybersecurity incident that is initially handled under an incident response plan may cause a business interruption that requires implementation of business continuity procedures. Thus, each plan should be drafted and tested for such circumstances to ensure a smooth and efficient response and continuity of operations.

Certain critical infrastructure sectors have BC/DR requirements. NERC, for example, has requirements for BC/DR in its required standards, and it conducts ongoing work regarding continuity of operations and resiliency of electricity grids. These activities help these companies stay abreast of threats and develop, implement, and maintain sophisticated BC/DR plans.

VI. **INFORMATION SHARING**

Sharing threat information regarding cyber incidents with others, such as law enforcement, community emergency response teams (CERTs), information sharing and analysis centers

---


(ISACs), business partners, and public sector cyber officials who could benefit from the knowledge, helps advance cyber defenses and resiliency in other organizations. An attack on any organization may impact others, or it may be targeted at a particular activity or business process, such as point-of-sale systems or control processes. The sharing of threat information can substantially improve the ability of other organizations to respond to a similar attack. It also expands the knowledge base about threats and effective mitigation measures.

Many organizations have not thought through what external assistance they might need when responding to incidents. Establishing relationships with external organizations—such as FBI InfraGard, ISACs, CERTs, and industry cyber groups—regarding cyber threats can be an important defensive measure for any organization. Such organizations are usually open to receiving information in an anonymized or sanitized fashion, if desired, by the entity providing the information.

It is important that organizations identify what data they might share, determine with whom they would share it and in what form, and consider any legal ramifications associated with the data or sharing it with third parties. Although some have raised concerns that antitrust constraints may arise with information sharing, the U.S. Department of Justice (DOJ) has indicated a willingness to provide letters of exception, if requested, to enable cyber information sharing. On April 14, 2014, DOJ joined with the Federal Trade Commission (FTC) and issued a joint “Antitrust Policy Statement on Sharing of Cybersecurity Information,” which clarifies the issue:

Through this Statement, the Department of Justice’s Antitrust Division (the “Division”) and the Federal Trade Commission (the “Commission” or “FTC”) (collectively, the “Agencies”) explain their analytical framework for information sharing and make it clear that they do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing.

VII. EXISTING ABA POLICY

In recent years, the ABA House of Delegates and Board of Governors have adopted several policies regarding cybersecurity and lawyers’ use of technology, and the proposed Resolution is consistent with those existing ABA policies. These ABA policies include the following:

Resolution 118, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco (August 2013)

This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firms, urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions, and makes other related recommendations. The complete Resolution and Report are available at:

24 Lawyers, law firms, and organizations and entities authorized to provide legal services should take into consideration any ethical constraints that may apply to client records, and any legal restrictions applicable to records under seal, grand jury information, classified information, etc.
http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf

* * *

Policy Adopted by the ABA Board of Governors (November 2012)

The ABA’s Board of Governors approved a policy in November 2012 comprised of five cybersecurity principles developed by the ABA Cybersecurity Legal Task Force. The complete Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf

* * *


Resolution 105A amends the black letter and Comments to Model Rule 1.0 (Terminology), the Comments to Model Rule 1.1 (Competence) and Model Rule 1.4 (Communication), and the black letter and Comments to Model Rule 1.6 (Confidentiality of Information) and Model Rule 4.4 (Respect for Rights of Third Parties) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality. Resolution 105B amends the black letter and Comments to Model Rules 1.18 and 7.3, and the Comments to Model Rules 7.1, 7.2 and 5.5 of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and client development.

Resolution 105C amends the Comments to Model Rule 1.1 (Competence) and Model Rule 5.5 (Unauthorized Practice of Law; Multijurisdictional Practice of Law), and the title and Comments to Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding the ethical implications of retaining lawyers and nonlawyers outside the firm to work on client matters (i.e., outsourcing).

The Resolutions and related Reports are available at:

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105a.doc

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_105b.authcheckdam.pdf

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105c.doc
VIII. CONCLUSION

This Resolution is intended to call attention to the importance of appropriate cybersecurity programs for all organizations. These issues are linked directly to our Nation’s economic and national security. The principles and concepts discussed in this Resolution and Report can help organizations, including law firms, understand and address cybersecurity threats and risks.

Respectfully Submitted,

Judith Miller
Harvey Rishikof
Co-Chairs, ABA Cybersecurity Legal Task Force

August 2014
FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE

Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011

October 2011
# Table of Contents

Executive Summary........................................................................................................... i
Scope Note ......................................................................................................................... iii
US Technologies and Trade Secrets at Risk in Cyberspace................................................ 1
   The Appeal of Collecting in Cyberspace................................................................. 1
      Security and attribution................................................................................... 1
      Faster and cheaper......................................................................................... 2
      Extra-territoriality......................................................................................... 2
   Large but Uncertain Costs.................................................................................. 3
Pervasive Threat from Intelligence Adversaries and Partners............................................ 4
   China: Persistent Collector.................................................................................. 5
   Russia: Extensive, Sophisticated Operations..................................................... 5
   US Partners: Leveraging Access......................................................................... 6
Outlook......................................................................................................................... 6
   Near Certainties................................................................................................. 6
      Evolving cyber environment......................................................................... 6
      Little change in principal threats................................................................. 7
      Technologies likely to be of greatest interest............................................... 8
   Business information......................................................................................... 9
Possible Game Changers.......................................................................................... 10
   Emergence of new state threats...................................................................... 10
   Growing role of non-state and non-corporate actors.................................... 10
Annex A
Intelligence Community and Private Sector Measures to Counter Economic Espionage and Manage Collection in Cyberspace ................................................................. A-1

Annex B
West and East Accuse China and Russia of Economic Espionage .................................................. B-1

List of Text Boxes
Non-Cyber Methods of Economic Espionage .................................................................................. 2
The Cost of Economic Espionage to One Company ....................................................................... 3
A Possible Proxy Measure of the Costs of Economic Espionage to the United States .............. 4

List of Charts
Recent Insider Thefts of Corporate Trade Secrets with a Link to China ........................................ 4
Russian Leaders Link Intelligence Operations and Economic Interests ...................................... 6
Projected Growth in Number of IT Devices Connected to Networks and the Internet, 2003-2020 ..... 7
Rising Prices Increase Value of Commodity Information to Foreign Collectors ............................. 9
Executive Summary

Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation’s prosperity and security. Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect.

US Technologies and Trade Secrets at Risk in Cyberspace

Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cyber tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the economic espionage threat, and the Intelligence Community (IC) judges the use of such tools is already a larger threat than more traditional espionage methods.

Economic espionage inflicts costs on companies that range from loss of unique intellectual property to outlays for remediation, but no reliable estimates of the monetary value of these costs exist. Many companies are unaware when their sensitive data is pilfered, and those that find out are often reluctant to report the loss, fearing potential damage to their reputation with investors, customers, and employees. Moreover, victims of trade secret theft use different methods to estimate their losses; some base estimates on the actual costs of developing the stolen information, while others project the loss of future revenues and profits.

Pervasive Threat from Adversaries and Partners

Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.

- Chinese actors are the world’s most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC cannot confirm who was responsible.
- Russia’s intelligence services are conducting a range of activities to collect economic information and technology from US targets.
- Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities.

Outlook

Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment.

- Over the next several years, the proliferation of portable devices that connect to the Internet and other networks will continue to create new opportunities for malicious actors to conduct espionage. The trend in both commercial and government organizations toward the pooling of information processing and storage will present even greater challenges to preserving the security and integrity of sensitive information.
The US workforce will experience a cultural shift that places greater value on access to information and less emphasis on privacy or data protection. At the same time, deepening globalization of economic activities will make national boundaries less of a deterrent to economic espionage than ever.

We judge that the governments of China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace.

The relative threat to sensitive US economic information and technologies from a number of countries may change in response to international economic and political developments. One or more fast-growing regional powers may judge that changes in its economic and political interests merit the risk of aggressive cyber and other espionage against US technologies and economic information.

Although foreign collectors will remain interested in all aspects of US economic activity and technology, we judge that the greatest interest may be in the following areas:

- Information and communications technology (ICT), which forms the backbone of nearly every other technology.
- Business information that pertains to supplies of scarce natural resources or that provides foreign actors an edge in negotiations with US businesses or the US Government.
- Military technologies, particularly marine systems, unmanned aerial vehicles (UAVs), and other aerospace/aeronautic technologies.
- Civilian and dual-use technologies in sectors likely to experience fast growth, such as clean energy and health care/pharmaceuticals.

Cyberspace provides relatively small-scale actors an opportunity to become players in economic espionage. Under-resourced governments or corporations could build relationships with hackers to develop customized malware or remote-access exploits to steal sensitive US economic or technology information, just as certain FIS have already done.

- Similarly, political or social activists may use the tools of economic espionage against US companies, agencies, or other entities, with disgruntled insiders leaking information about corporate trade secrets or critical US technology to “hacktivist” groups like WikiLeaks.
Scope Note

This assessment is submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359, as amended, which requires that the President biennially submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the 14th Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2008 and draws primarily on data from 2009-2011.

New Focus and Additional Resources Used for This Year's Report

This report differs from previous editions in three important ways. The first and most significant is the focus. This report gives special attention to foreign collectors' exploitation of cyberspace, while not excluding other established tactics and methods used in foreign economic collection and industrial espionage. This reflects the fact that nearly all business records, research results, and other sensitive economic or technology-related information now exist primarily in digital form. Cyberspace makes it possible for foreign collectors to gather enormous quantities of information quickly and with little risk, whether via remote exploitation of victims' computer networks, downloads of data to external media devices, or e-mail messages transmitting sensitive information.

The second difference from prior reports is that, in addition to researching the large body of intelligence reporting and analysis on economic espionage produced by the Intelligence Community, the Department of Defense (DoD), and other US Government agencies, the drafters of this report consulted new sources of government information.

Third, the Office of the National Counterintelligence Executive (ONCIX) mobilized significant resources from outside the IC during the course of this study. This included outreach to the private sector and, in particular, sponsorship of a conference in November 2010 on cyber-enabled economic espionage at which 26 US Government agencies and 21 private-sector organizations were represented. ONCIX also contracted with outside experts to conduct studies of the academic literature on the cost of economic espionage and the role of the cyber "underground economy."

Definitions of Key Terms

For the purposes of this report, key terms were defined according to both legal and analytic criteria.

The legal criteria derive from the language in the Economic Espionage Act (EEA) of 1996 (18 USC §§ 1831-1839). The EEA is concerned in particular with economic espionage and foreign activities to acquire US trade secrets. In this context, trade secrets are all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored or unstored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, if the owner (the person or entity in whom or in which rightful legal or equitable title to, or license in, is reposed) has taken reasonable measures to keep such information secret and the information derives independent economic value, actual, or potential from not being generally known to, and not being readily ascertainable through, proper means by the public. Activities to acquire these secrets include the following criminal offenses:

- Economic espionage occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality or agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1831).
• **Industrial espionage**, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmitting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1832).

The following definitions reflect the experience of IC cyber, counterintelligence, and economic analysts:

• **Cyberspace** is the interdependent network of information technology (IT) infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

• **Sensitive** is defined as information or technology (a) that has been classified or controlled by a US Government organization or restricted in a proprietary manner by a US corporation or other institution, or (b) that has or may reasonably be expected to have military, intelligence, or other uses with implications for US national security, or (c) that may enhance the economic competitiveness of US firms in global markets.

**Contributors**

ONCIX compiled this report using inputs and reporting from many US Government agencies and departments, including the Air Force Office of Special Investigations (AFOSI), Army Counterintelligence Center (ACIC), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Defense Security Service (DSS), Department of Energy (DoE), Department of Health and Human Services (HHS), Department of State (DoS), Federal Bureau of Investigation (FBI), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Naval Criminal Investigative Service (NCIS).
Foreign Spies Stealing US Economic Secrets in Cyberspace

US Technologies and Trade Secrets at Risk in Cyberspace

The pace of foreign economic collection and industrial espionage activities against major US corporations and US Government agencies is accelerating. FIS, corporations, and private individuals increased their efforts in 2009-2011 to steal proprietary technologies, which cost millions of dollars to develop and represented tens or hundreds of millions of dollars in potential profits. The computer networks of a broad array of US Government agencies, private companies, universities, and other institutions—all holding large volumes of sensitive economic information—were targeted by cyber espionage; much of this activity appears to have originated in China.

Increasingly, economic collection and industrial espionage occur in cyberspace, reflecting dramatic technological, economic, and social changes that have taken place in recent years in the ways that economic, scientific, and other sensitive information is created, used, and stored. Today, nearly all business records, research results, and other sensitive economic data are digitized and accessible on networks worldwide. Cyber collection can take many forms, including: simple visits to a US company’s website for the collection of openly available information; a corporate insider’s downloading of proprietary information onto a thumb drive at the behest of a foreign rival; or intrusions launched by FIS or other actors against the computer networks of a private company, federal agency, or an individual.

The Appeal of Collecting in Cyberspace

Cyberspace is a unique complement to the espionage environment because it provides foreign collectors with relative anonymity, facilitates the transfer of a vast amount of information, and makes it more difficult for victims and governments to assign blame by masking geographic locations.

Security and attribution. Collectors operating in a cyber environment can collect economic information with less risk of detection. This is particularly true for remote computer network exploitation (CNE). Foreign collectors take advantage of the fact that it is difficult to detect and to attribute responsibility for these operations.

There is increasing similarity between the tools, tactics, and techniques used by various actors, which reduces the reliability of using these factors to identify those responsible for computer network intrusions.

- The proliferation of malicious software (malware) presents opportunities for intelligence services and other actors to launch operations with limited resources and without developing unique tools that can be associated with them.
- Hacker websites are prevalent across the Internet, and tool sharing is common, causing intrusions by unrelated actors to exhibit similar technical characteristics.
- FIS and other foreign entities have used independent hackers at times to augment their capabilities and act as proxies for intrusions, thereby providing plausible deniability.
- Many actors route operations through computers in third countries or physically operate from third countries to obscure the origin of their activity.

Another factor adding to the challenge of attribution is the diverging perspectives of the actual targets of economic espionage in cyberspace.

- At a conference sponsored by ONCIX in November 2010, US private industry representatives said they saw little difference between cybercrime—for example, identity theft or the misappropriation of intellectual property such as the counterfeiting of commercial video or audio recordings—and the collection of economic or technology information by intelligence services or other foreign entities. Private sector organizations are often less concerned with attribution and focus instead on damage control and prevention; moreover, few companies have the ability to identify cyber intruders.
• US Government law enforcement and intelligence agencies, on the other hand, seek to establish attribution as part of their mission to counter F15 and other clandestine information collectors. They, unlike companies, also have the intelligence collection authorities and capabilities needed to break multiple layers of cover and to establish attribution where possible.

Cyberspace also offers greater security to the perpetrator in cases involving insiders. Although audits or similar security measures may flag illicit information downloads from a corporate network, a malicious actor can quickly and safely transfer a data set once it is copied. A physical meeting is unnecessary between the corrupted insider and the persons or organizations the information is being collected for, reducing the risk of detection.

**Faster and cheaper.** Cyberspace makes possible the near instantaneous transfer of enormous quantities of economic and other information. Until fairly recently, economic espionage often required that insiders pass large volumes of documents to their handlers in physical form—a lengthy process of collection, collation, transportation, and exploitation.

• Dongfan Chung was an engineer with Rockwell and Boeing who worked on the B-1 bomber, space shuttle, and other projects and was sentenced in early 2010 to 15 years in prison for economic espionage on behalf of the Chinese aviation industry. At the time of his arrest, 250,000 pages of sensitive documents were found in his house. This is suggestive of the volume of information Chung could have passed to his handlers between 1979 and 2006.\(^8\) The logistics of handling the physical volume of these documents—which would fill nearly four 4-drawer filing cabinets—would have required considerable attention from Chung and his handlers. With current technology, all the data in the documents hidden in Chung's house would fit onto one inexpensive CD.\(^9\)

**Extra-territoriality.** In addition to the problem of attribution, it often is difficult to establish the geographic location of an act of economic espionage that takes place in cyberspace. Uncertainty about the physical location of the act provides cover for the perpetrators and complicates efforts by US Government law enforcement or intelligence agencies to respond.

**Non-Cyber Methods of Economic Espionage**

Although this assessment focuses on the use of cyber tools and the cyber environment in foreign efforts to collect sensitive US economic information and technologies, a variety of other methods also remain in use.

**Requests for Information (RFI).** Foreign collectors make unsolicited direct and indirect requests for information via personal contacts, telephone, e-mail, fax, and other forms of communication and often seek classified, sensitive, or export-controlled information.

**Solicitation or Marketing of Services.** Foreign companies seek entrance into US firms and other targeted institutions by pursuing business relationships that provide access to sensitive or classified information, technologies, or projects.

**Conferences, Conventions, and Trade Shows.** These public venues offer opportunities for foreign adversaries to gain access to US information and experts in dual-use and sensitive technologies.

**Official Foreign Visitors and Exploitation of Joint Research.** Foreign government organizations, including intelligence services, use official visits to US Government and cleared defense contractor facilities, as well as joint research projects between foreign and US entities, to target and collect information.

**Foreign Targeting of US Visitors Overseas.** Whether traveling for business or personal reasons, US travelers overseas—businesspeople, US Government employees, and contractors—are routinely targeted by foreign collectors, especially if they are assessed...
as having access to some sensitive information. Some US allies engage in this practice, as do less friendly powers such as Russia and China. Targeting takes many forms: exploitation of electronic media and devices, surreptitious entry into hotel rooms, aggressive surveillance, and attempts to set up sexual or romantic entanglements.

**Open Source Information.** Foreign collectors are aware that much US economic and technological information is available in professional journals, social networking and other public websites, and the media.

**Large but Uncertain Costs**

Losses of sensitive economic information and technologies to foreign entities represent significant costs to US national security. The illicit transfer of technology with military applications to a hostile state such as Iran or North Korea could endanger the lives of US and allied military personnel. The collection of confidential US Government economic information—whether by a potential adversary or a current ally—could undercut US ability to develop and enact policies in areas ranging from climate change negotiations to reform of financial market regulations. The theft of trade secrets from US companies by foreign economic rivals undermines the corporate sector’s ability to create jobs, generate revenues, foster innovation, and lay the economic foundation for prosperity and national security.

Data on the effects of the theft of trade secrets and other sensitive information are incomplete, however, according to an ONCIX-sponsored survey of academic literature on the costs of economic espionage.

- Many victims of economic espionage are unaware of the crime until years after loss of the information.
- Even when a company knows its sensitive information has been stolen by an insider or that its computer networks have been penetrated, it may choose not to report the event to the FBI or other law enforcement agencies. No legal requirement to report a loss of sensitive information or a remote computer intrusion exists, and announcing a security breach of this kind could tarnish a company’s reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders.

- A company also may not want to publicly accuse a corporate rival or foreign government of stealing its secrets from fear of offending potential customers or business partners.

- Finally, it is inherently difficult to assign an economic value to some types of information that are subject to theft. It would, for example, be nearly impossible to estimate the monetary value of talking points for a meeting between officials from a US company and foreign counterparts.

**The Cost of Economic Espionage to One Company**

Data exist in some specific cases on the damage that economic espionage or theft of trade secrets has inflicted on individual companies. For example, an employee of Valspar Corporation unlawfully downloaded proprietary paint formulas valued at $20 million, which he intended to take to a new job in China, according to press reports. This theft represented about one-eighth of Valspar’s reported profits in 2009, the year the employee was arrested.

Even in those cases where a company recognizes it has been victimized by economic espionage and reports the incident, calculation of losses is challenging and can produce ambiguous results. Different methods can be used that yield divergent estimates, which adds to the difficulty of meaningfully comparing cases or aggregating estimated losses.

- An executive from a major industrial company told ONCIX representatives in late 2010 that his company has used historical costs—tallying salaries, supplies, utilities, and similar direct expenses—to estimate losses from cases of attempted theft of its trade secrets. This method has the advantage of using known and objective
data, but it underestimates the extent of losses in many cases because it does not capture the effect of lost intellectual property on future sales and profits.

- Harm is calculated in US civil court cases involving the theft of trade secrets by measuring the "lost profits" or "reasonable royalty" that a company is unable to earn because of the theft. Although this method requires subjective assumptions about market share, profitability, and similar factors, it does offer a more complete calculation of the cost than relying strictly on historical accounting data.

- Estimates from academic literature on the losses from economic espionage range so widely as to be meaningless—from $2 billion to $400 billion or more a year—reflecting the scarcity of data and the variety of methods used to calculate losses.

A Possible Proxy Measure of the Costs of Economic Espionage to the United States

New ideas are often a company's or an agency's most valuable information and are usually of greatest interest to foreign collectors. Corporate and government spending on research and development (R&D) is one measure of the cost of developing new ideas, and hence is an indicator of the value of the information that is most vulnerable to economic espionage. R&D spending has been tracked by the National Science Foundation (NSF) since 1953. For 2008, the most recent year available, the NSF calculated that US industry, the Federal Government, universities, and other nonprofit organizations expended $398 billion on R&D, or 2.8 percent of the US Gross Domestic Product.

Pervasive Threat from Intelligence Adversaries and Partners

Many states view economic espionage as an essential tool in achieving national security and economic prosperity. Their economic espionage programs combine collection of open source information, HUMINT, signals intelligence (SIGINT), and cyber operations—to include computer network intrusions and exploitation of insider access to corporate and proprietary networks—to develop information that could give these states a competitive edge over the United States and other rivals.

- China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of US economic information and technology.

- Other countries with closer ties to the United States have conducted CNE and other forms of intelligence collection to obtain US economic and technology data, often taking advantage of the access they enjoy as allies or partners to collect sensitive military data and information on other programs.

Recent Insider Thefts of Corporate Trade Secrets with a Link to China

David Yen Lee...chemist with Valspar Corporation...between late 2006 and early 2009 used access to internal computer network to download about 160 secret formulas for paints and coatings to his own storage media...intended to take this proprietary information to a new job with Nippon Paint in Shanghai, China...arrested March 2009...pleaded guilty to one count of theft of trade secrets; sentenced in December 2010 to 15 months in prison.

Meng Hong...DuPont Corporation research chemist...in mid-2009 downloaded proprietary information on organic light-emitting diodes (OLED) to personal e-mail account and thumb drive...intended to transfer this information to Peking University, where he had accepted a faculty position; sought Chinese Government funding to commercialize OLED research...arrested October 2009...pleaded guilty to one count of theft of trade secrets; sentenced in October 2010 to 14 months in prison.

Yu Xiang Dong (aka Mike Yu)...product engineer with Ford Motor Company who in December 2006 accepted a job at Ford's China branch...copied approximately 4,000 Ford documents onto an external hard drive to help obtain a job with a Chinese automotive company...arrested in October 2009...pleaded guilty to two counts of theft of trade secrets; sentenced in April 2011 to 70 months in prison.
China: Persistent Collector

Chinese leaders consider the first two decades of the 21st century to be a window of strategic opportunity for their country to focus on economic growth, independent innovation, scientific and technical advancement, and growth of the renewable energy sector.

China’s intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to corporate networks to steal trade secrets using removable media devices or e-mail. Of the seven cases that were adjudicated under the Economic Espionage Act—both Title 18 USC § 1831 and § 1832—in Fiscal Year 2010, six involved a link to China.

US corporations and cyber security specialists also have reported an onslaught of computer network intrusions originating from Internet Protocol (IP) addresses in China, which private sector specialists call “advanced persistent threats.” Some of these reports have alleged a Chinese corporate or government sponsor of the activity, but the IC has not been able to attribute many of these private sector data breaches to a state sponsor. Attribution is especially difficult when the event occurs weeks or months before the victims request IC or law enforcement help.

- In a February 2011 study, McAfee attributed an intrusion set they labeled “Night Dragon” to an IP address located in China and indicated the intruders had exfiltrated data from the computer systems of global oil, energy, and petrochemical companies. Starting in November 2009, employees of targeted companies were subjected to social engineering, spear-phishing e-mails, and network exploitation. The goal of the intrusions was to obtain information on sensitive competitive proprietary operations and on financing of oil and gas field bids and operations.

- In January 2010, VeriSign iDefense identified the Chinese Government as the sponsor of intrusions into Google’s networks. Google subsequently made accusations that its source code had been taken—a charge that Beijing continues to deny.

- Mandiant reported in 2010 that information was pilfered from the corporate networks of a US Fortune 500 manufacturing company during business negotiations in which that company was looking to acquire a Chinese firm. Mandiant’s report indicated that the US manufacturing company lost sensitive data on a weekly basis and that this may have helped the Chinese firm attain a better negotiating and pricing position.

- Participants at an ONCIX conference in November 2010 from a range of US private sector industries reported that client lists, merger and acquisition data, company information on pricing, and financial data were being extracted from company networks—especially those doing business with China.

Russia: Extensive, Sophisticated Operations

Motivated by Russia’s high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward US and other Western interests at the expense of Russia, Moscow’s highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia’s economic development and security.

- For example, the 10 Russian Foreign Intelligence Service (SVR) “illegals” arrested in June 2010 were tasked to collect economic and technology information, highlighting the importance of these issues to Moscow.\(^c\)

\(^c\) An illegal is an officer or employee of an intelligence organization who is dispatched abroad and who has no overt connection with the intelligence organization with which he or she is connected or with the government operating that intelligence organization.
Russian Leaders Link Intelligence Operations and Economic Interests

The SVR "must be able to swiftly and adequately evaluate changes in the international economic situation, understand the consequences for the domestic economy and... more actively protect the economic interests of our companies abroad."
—Vladimir Putin, President, Russian Federation, October 2007

"Intelligence... aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology."
—Mikhail Fradkov, Director, SVR, December 2010

Source: Russian press reports.

US Partners: Leveraging Access

Certain allies and other countries that enjoy broad access to US Government agencies and the private sector conduct economic espionage to acquire sensitive US information and technologies. Some of these states have advanced cyber capabilities.

Outlook

Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will remain at high levels and continue to threaten US economic security. The nature of these attempts will be shaped by the accelerating evolution of cyberspace, policy choices made by the economic and political rivals of the United States, and broad economic and technological developments.

Near Certainties

Evolving cyber environment. Over the next three to five years, we expect that four broad factors will accelerate the rate of change in information technology and communications technology in ways that are likely to disrupt security procedures and provide new openings for the collection of sensitive US economic and technology information. These were identified in studies conducted by Cisco Systems and discussed at the ONCIX conference in November 2010. At the same time, the growing complexity and density of cyberspace will provide more cover for remote cyber intruders and make it even harder than today to establish attribution for these incidents.

The first factor is a technological shift. According to a Cisco Systems study, the number of devices such as smartphones and laptops in operation worldwide that can connect to the Internet and other networks is expected to increase from about 12.5 billion in 2010 to 25 billion in 2015. This will cause a proliferation in the number of operating systems and endpoints that malicious actors such as foreign intelligence services or corrupt insiders can exploit to obtain sensitive information. Meanwhile, the underlying hardware and software of information systems will become more complex.

• Marketing and revenue imperatives will continue to lead IT product vendors to release products with less than exhaustive testing, which will also create opportunities for remote exploitation.

An economic shift will change the way that corporations, government agencies, and other organizations share storage, computing, network, and application resources. The move to a "cloud computing" paradigm—which is much cheaper for companies than hosting computer services in—
Projected Growth in Number of IT Devices Connected to Networks and the Internet, 2003-2020

Millions

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2010</th>
<th>2015</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: CISCO Systems

house—will mean that employees will be able to work and access data anywhere and at any time, and not just while they are at the office, laboratory, or factory. Although cloud computing offers some security advantages, such as robust backup in the event of a systems disruption, the movement of data among multiple locations will increase the opportunities for theft or manipulation by malicious actors.

The cultural shift involves the rise in the US workforce of different expectations regarding work, privacy, and collaboration. Workers will tend to draw few distinctions between their home and work lives, and they will expect free access to any information they want—whether personal or professional—from any location.

- Current technology already enables many US workers to conduct business from remote locations and on-the-go at any time of day. This alteration relies on the ability of workers to connect to one another and their companies through the Internet—increasing their flexibility and corporate productivity but potentially increasing the risk of theft.

Finally, a geopolitical shift will continue the globalization of economic activities and knowledge creation. National boundaries will deter economic espionage less than ever as more business is conducted from wherever workers can access the Internet. The globalization of the supply chain for new—and increasingly interconnected—IT products will offer more opportunities for malicious actors to compromise the integrity and security of these devices.

Little change in principal threats. The IC anticipates that China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace. Both will almost certainly continue to deploy significant resources and a wide array of tactics to acquire this information from US sources, motivated by the desire to achieve economic, strategic, and military parity with the United States.

China will continue to be driven by its longstanding policy of “catching up fast and surpassing” Western powers. An emblematic program in this drive is Project 863, which provides funding and guidance for efforts to clandestinely acquire US technology and sensitive economic information. The project
was launched in 1986 to enhance China's economic competitiveness and narrow the science and technology gap between China and the West in areas such as nanotechnology, computers, and biotechnology.

- The growing interrelationships between Chinese and US companies—such as the employment of Chinese-national technical experts at US facilities and the off-shoring of US production and R&D to facilities in China—will offer Chinese Government agencies and businesses increasing opportunities to collect sensitive US economic information.
- Chinese actors will continue conducting CNE against US targets.

Two trends may increase the threat from Russian collection against US economic information and technology over the next several years.

- The many Russian immigrants with advanced technical skills who work for leading US companies may be increasingly targeted for recruitment by the Russian intelligence services.
- Russia's increasing economic integration with the West is likely to lead to a greater number of Russian companies affiliated with the intelligence services—often through their employment of ostensibly retired intelligence officers—doing business in the United States.

Technologies likely to be of greatest interest. Although all aspects of US economic activity and technology are of potential interest to foreign intelligence collectors, we judge that the highest interest may be in the following areas.

Information and communications technology (ICT). ICT is a sector likely to remain one of the highest priorities of foreign collectors. The computerization of manufacturing and the push for connectedness mean that ICT forms the backbone of nearly every other technology used in both civilian and military applications.

- Beijing's Project 863, for example, lists the development of "key technologies for the construction of China's information infrastructure" as the first of four priorities.

Military technologies. We expect foreign entities will continue efforts to collect information on the full array of US military technologies in use or under development. Two areas are likely to be of particular interest:

- Marine systems. China's desire to jump-start development of a blue-water navy—to project power in the Taiwan Strait and defend maritime trade routes—will drive efforts to obtain sensitive US marine systems technologies.
- Aerospace/aeronautics. The air supremacy demonstrated by US military operations in recent decades will remain a driver of foreign efforts to collect US aerospace and aeronautics technologies. The greatest interest may be in UAVs because of their recent successful use for both intelligence gathering and kinetic operations in Afghanistan, Iraq, and elsewhere.

Civilian and dual-use technologies. We expect that foreign collection on US civilian and dual-use technologies will follow overall patterns of investment and trade. The following sectors—which are expected to experience surges in investment and are priorities for China—may be targeted more aggressively.

- Clean technologies. Energy-generating technologies that produce reduced carbon dioxide and other emissions will be the fastest growing investment sectors in nine of 11 countries recently surveyed by a US consulting company—a survey that included China, France, and India.
- Advanced materials and manufacturing techniques. One focus of China's 863 program is achieving mastery of key new materials and advanced manufacturing technologies to boost industrial competitiveness, particularly in the aviation and high-speed rail sectors. Russia and Iran have aggressive programs for developing and collecting on one specific area of advanced materials development: nanotechnology.
Rising Prices Increase Value of Commodity Information to Foreign Collectors (Index, 2002=100)

*2011 values as of April
Source: International Monetary Fund, World Economic Outlook Database.

- **Healthcare, pharmaceuticals, and related technologies.** Healthcare services and medical devices/equipment will be two of the five fastest growing international investment sectors, according to a US consulting firm. The massive R&D costs for new products in these sectors—up to $1 billion for a single drug—the possibility of earning monopoly profits from a popular new pharmaceutical, and the growing need for medical care by aging populations in China, Russia, and elsewhere are likely to drive interest in collecting valuable US healthcare, pharmaceutical, and related information.

- **Agricultural technology.** Surging prices for food—which have increased by 70 percent since 2002, according to the food price index published by the International Monetary Fund (IMF)—and for other agricultural products may increase the value of and interest in collecting on US technologies related to crop production, such as genetic engineering, improved seeds, and fertilizer.\(^d\)

**Business information.** As with technologies, we assess that nearly all categories of sensitive US economic information will be targeted by foreign entities, but the following sectors may be of greatest interest:

- **Energy and other natural resources.** Surging prices for energy and industrial commodities—which have increased by 210 percent and 96 percent, respectively, since 2002 according to IMF indices—may make US company information on these resources priority targets for intelligence services and other collectors.\(^e\)

- As noted earlier, cyber intrusions originating in China, but not necessarily attributed to the Chinese Government, since at least 2009 have targeted sensitive operational and project-financing information of US and other international oil, energy, and petrochemical companies, according to reports published by McAfee.

---
\(^d\)The IMF’s Food Price Index is a weighted index that includes the spot prices of cereal grains, vegetable oils and protein meals, meat, seafood, sugar, bananas, and oranges.

\(^e\)The Fuel (energy) index published by the IMF is a weighted index that includes the spot prices of crude oil, natural gas, and coal. The Industrial Inputs Index is a weighted index that includes the spot price of agricultural raw materials (timber, fibers, rubber and hides) and non-precious metals (such as copper, aluminum, and iron ore).
Business deals. Some foreign companies—at times helped by their home countries’ intelligence services—will collect sensitive information from US economic actors that are negotiating contracts with or competing against them.

Macroeconomic information. In the wake of the global financial crisis of 2008-2009 and related volatility in the values of currencies and commodities, sensitive macroeconomic information held by the US private sector and government agencies is likely to remain a prime collection target for both intelligence services and foreign corporations. Chinese and Russian intelligence collectors may pursue, for example, non-public data on topics such as interest rate policy to support their policymakers’ efforts to advance the role of their currencies and displace the dollar in international trade and finance. Such information also could help boost the performance of sovereign wealth funds controlled by governments like China’s, whose China Investment Corporation managed more than $300 billion in investments as of late 2010.¹

Possible Game Changers

Any of a range of less-likely developments over the next several years could increase the threat from economic espionage against US interests.

Emergence of new state threats. The relative threat to sensitive US economic information and technologies from different countries is likely to evolve as a function of international economic and political developments.

One or more fast-growing regional powers may judge that changes in its economic and political interests merit the risk of an aggressive program of espionage against US technologies and sensitive economic information.

Growing role of non-state and non-corporate actors. The migration of most business and technology development activities to cyberspace is making it easier for actors without the resources of a nation-state or a large corporation to become players in economic espionage. Such new actors may act as surrogates or contractors for intelligence services or major companies, or they could conduct espionage against sensitive US economic information and technology in pursuit of their own objectives.

Hackers for hire. Some intelligence services with less-developed cyber programs already use relationships with nominally independent hackers to augment their capabilities to target political and military information or to carry out operations against regime enemies. For example, the Iranian Cyber Army, a hacker group with links to the Iranian Government, has used social engineering techniques to obtain control over Internet domains and disrupt the political opposition, according to research conducted under an ONCIX contract.

No evidence of involvement by independent hackers in economic espionage has been found in intelligence or academic reporting to date, in large part due to the absence of a profitable market for the resale of stolen information. This “cyber underground” could, however, become a fruitful recruiting ground for the tools and talents needed to support economic espionage. Following the model used by some intelligence services in exploiting the cyber environment for political or military espionage, a foreign government or corporation could build relationships with hackers for the development of customized malware or remote access exploits for the exfiltration of sensitive US economic or technology information.

Hacktivists. Political or social activists also may use the tools of economic espionage against US companies, agencies, or other entities. The self-styled whistleblowing group WikiLeaks has already published computer files provided by corporate insiders indicating allegedly illegal or unethical behavior at a Swiss bank, a Netherlands-based commodities company, and an international pharmaceutical trade association. LulzSec—another hacktivist group—has exfiltrated data from several businesses that it posted for public viewing on its website.

¹A sovereign wealth fund is a government investment fund, funded by foreign currency reserves but managed separately from official currency reserves. In other words, it is a pool of money that a government invests for profit.
Corporate trade secrets or information about critical US technology may be at similar risk of disclosure to activist groups by disgruntled insiders.

- Antipoverty activists, for instance, could seek to publish the details of a new medicine under development by a US pharmaceutical company, with the goal of ending the firm's "monopoly" profits and making the product more widely available.
- Antiwar groups could disclose information about a new weapons system in the hope of dissuading the United States from deploying it.
Annex A

Intelligence Community and Private Sector Measures to Counter Economic Espionage and Manage Collection in Cyberspace

The IC is working closely with all segments of the public and private sectors to try to counter espionage activities that target our sensitive economic data and technology. We cannot expect to stop entirely or prevent hostile activity to collect US public and private sector information, but we can work to minimize the activity and mitigate its effects.

Intelligence Community Responses

The IC and especially counterintelligence (CI) officers have already taken a number of steps to improve collaboration, collection, and analysis across the CI, economics, and cyber disciplines.

Improved collaboration. Over the past few years, the IC has established multiple organizations and working groups to better understand the cyber espionage threat. These have contributed to a better understanding of the use of cyber in economic espionage.

- The National Cyber Counterintelligence Working Group established in 2011 is composed of 16 IC and other federal agencies and is creating a coordinated response to the cyber intelligence threat.
- The FBI is leading the National Cyber Investigative Joint Task Force, which brings together multiple agencies to collaborate on intrusions into US systems.

CI officers are considering an expansion of collaboration to include enhanced information sharing with Department of Justice attorneys. CI officers could introduce questions for attorneys to pose to offenders during the investigation process. They might also look at ways to tie plea bargains and sentencing decisions to suspects’ willingness to cooperate with the CI Community during damage assessments.

Improved analysis and collection. The IC has made great strides over the past few years in understanding the cyber espionage threat to US Government systems, but our knowledge of cyber-enabled economic espionage threats to the US private sector remains limited.

Defense Model Shows Limits to Mandatory Reporting Requirements

DoD’s partnership with cleared defense contractors (CDCs) highlights difficulties in establishing an effective framework to improve the IC’s understanding of foreign cyber threats and promote threat awareness in industry. The defense industrial base conducts $400 billion in business with the Pentagon each year and maintains a growing repository of government information and intellectual property on unclassified networks. CDCs are required to file reports of suspicious contacts indicative of foreign threats—including cyber—to their personnel, information, and technologies.

- Despite stringent reporting requirements for CDCs, DSS reports that only 10 percent of CDCs actually provide any sort of reporting in a given year.
- Another shortcoming of the defense model is that contractors do not always report theft of intellectual property unless it relates specifically to Pentagon contracts, according to outreach discussions with corporate officers.
- Corporate security officers also have noted that US Government reporting procedures are often cumbersome and redundant, with military services and agencies such as DSS and the FBI often seeking the same information but in different formats.

Operations. CI professionals are adapting how they detect, deter, and disrupt collection activity in cyberspace because of the challenges in detecting the traditional indicators of collection activity—spotting, assessing, and recruiting.
It is imperative that we improve our ability to attribute technical and human activity in the cyber environment so that we can improve our understanding of the threat and our ability to generate a greater number of offensive CI responses.

Training and awareness. Expanding our national education and awareness campaign aimed at individuals and corporations is an essential defensive strategy for countering threats from cyber-enabled economic collection and espionage. We are building on current outreach initiatives that the FBI and ONCIX have already initiated.

- IC outreach to all US Government agencies, state and local governments, academia, nongovernmental organizations, industry associations, and companies is critical for promoting threat awareness, as well as for a better understanding of nongovernmental perspectives. Partners outside the IC are becoming aware of the wide range of potentially sensitive information in their possession and the extent of foreign efforts to acquire it.
- Outreach efforts include awareness and mitigation strategies for insider threat issues. The unique access of insiders to information technology systems and organizational processes makes this the most dangerous approach to cyber economic collection and espionage, as insiders can act alone to guide CNE or to download sensitive data to portable media.

ONCIX already engages in dialogue with ASIS International—an industry association for security professionals—and the Department of State’s Overseas Security Advisory Council on the challenges facing both the public and private sectors with regard to cyber-enabled economic collection and espionage.

Finally, IC outreach efforts to the private sector on economic espionage need to fully engage corporate and other partners in order to be credible. We can facilitate partnerships to share best practices, threat updates and analysis, and data on intrusions. One company security officer has suggested that the IC must speak to industry in language geared to the private sector’s needs and experience and emphasize, for example, that the protection of trade secrets is critical to corporate profitability and growth.

As a follow-up to the public/private sector Workshop on Cyber-Enabled Economic Espionage held in 2010, ONCIX should consider sponsoring another conference with Department of Justice and private sector stakeholders on lessons learned regarding successful convictions under Section 1831 of the Economic Espionage Act.

Corporate Responses

The private sector already has a fiduciary duty to account for corporate risk and the bottom-line effects of data breaches, economic espionage, and loss or degradation of services. A key responsibility of chief executive officers and boards of directors is to ensure that the protection of trade secrets and computer networks is an integral part of all corporate decisions and processes and that all managers—not just security and information systems officials—have a stake in the outcome.\(^a\) Viewing network security and data protection as a business matter that has a significant impact on profitability will lead to more effective risk management and ensure that adequate resources are allocated to address cyber threats to companies.

- Only 5 percent of corporate chief financial officers are involved in network security matters, and just 13 percent of companies have a cross-functional cyber risk team that bridges the technical, financial, and other elements of a company, according to a 2010 study.

Judicial Mandate for Boards of Directors To Secure Corporate Information

Delaware’s Court of Chancery ruled in the 1996 Caremark case that a director’s good faith duty includes a duty to attempt to ensure that a corporate

\(^a\)Legal and human resources officers are two sets of key stakeholders given the role that corporate insiders have historically played in contributing to economic espionage and the theft of trade secrets.
information and reporting system exists and that failure to do so may render a director liable for losses caused by the illegal conduct of employees. The Delaware Supreme Court clarified this language in the 2006 Stone v. Ritter case—deciding that directors may be liable for the damages resulting from legal violations committed by the employees of a corporation, if directors fail to implement a reporting system or controls or fail to monitor such systems.

Companies that successfully manage the economic espionage threat realize and convey to their employees that threats to corporate data extend beyond company firewalls to include other locations where company data is moved or stored. These include cloud sites, home computers, laptops, portable electronic devices, portable data assistants, and social networking sites.

- A survey of 200 information technology and security professionals in February 2011 revealed that 65 percent do not know what files and data leave their enterprise.
- According to a March 2011 press report, 57 percent of employees save work files to external devices on a weekly basis.
- E-mail systems are often less protected than databases yet contain vast quantities of stored data. E-mail remains one of the quickest and easiest ways for individuals to collaborate—and for intruders to enter a company’s network and steal data.

Cyber threats to company information are compounded when employees access data through portable devices or network connections while traveling overseas. Many FIS co-opt hotel staffs to allow access to portable devices left unattended in rooms. It is also much easier for FIS to monitor and exploit network connections within their own borders.

- Foreign collectors engage in virtual methods to collect sensitive corporate data and take advantage of victims’ reluctance to report digital penetrations and low awareness of foreign targeting, according to legal academic research.

Corporate security officers have told ONCIX that US Government reporting procedures on economic espionage and cyber intrusions are often cumbersome and redundant. Agencies such as DSS and the FBI often seek the same information but in different formats.
Best Practices in Data Protection Strategies and Due Diligence for Corporations

**Information Strategy**

- Develop a "transparency strategy" that determines how closed or open the company needs to be based on the services provided.

**Insider Threat Programs and Awareness**

- Institute security training and awareness campaigns; convey threats to company information accessed through portable devices and when traveling abroad.
- Establish an insider threat program that consists of information technology-enabled threat detection, foreign travel and contact notifications, personnel security and evaluation, insider threat awareness and training, and reporting and analysis.
- Conduct background checks that vet users before providing them company information.
- Implement non-disclosure agreements with employees and business partners.
- Establish employee exit procedures; most employees who steal intellectual property commit the theft within one month of resignation.

**Effective Data Management**

- Get a handle on company data—not just in databases but also in e-mail messages, on individual computers, and as data objects in web portals; categorize and classify the data, and choose the most appropriate set of controls and markings for each class of data; identify which data should be kept and for how long. Understand that it is impossible to protect everything.
- Establish compartmentalized access programs to protect unique trade secrets and proprietary information; centralize intellectual property data—which will make for better security and facilitate information sharing.
- Restrict distribution of sensitive data; establish a shared data infrastructure to reduce the quantity of data held by the organization and discourage unnecessary printing and reproduction.

**Network Security, Auditing, and Monitoring**

- Conduct real-time monitoring/auditing of the networks; maintain thorough records of who is accessing servers, and modifying, copying, deleting, or downloading files.
- Install software tools—content management, data loss prevention, network forensics—on individual computer workstations to protect files.
• Encrypt data on servers and password-protect company information.

• Incorporate multi-factor authentication measures—biometrics, PINs, and passwords combined with knowledge-based questions—to help verify users of information and computer systems.

• Create a formal corporate policy for mobility—develop measures for centrally controlling and monitoring which devices can be attached to corporate networks and systems and what data can be downloaded, uploaded, and stored on them.

• Formalize a social media policy for the company and implement strategies for minimizing data loss from on-line social networking.

Contingency Planning

• Establish a continuity of operations plan—back up data and systems; create disaster recovery plans; and plan for data breach contingencies.

• Conduct regular penetration testing of company infrastructure as well as of third-party shared service provider systems.

• Establish document creation, retention, and destruction policies.

Resources for Help

• Contact ONCIX or the FBI for assistance in developing effective data protection strategies. If a data breach is suspected, contact the FBI or other law enforcement/organizations for help in identifying and neutralizing the threat.
Annex B

West and East Accuse China and Russia of Economic Espionage

Other advanced industrial countries principally blame China and Russia for economic espionage that results in large but uncertain monetary costs and job losses. They perceive that China and Russia continue to use traditional human and technical collection methods—particularly against small- and medium-sized businesses—to gather economic information and technologies that save them research and development (R&D) resources and provide entrepreneurial and marketing advantage for their corporate sectors.

- Germany’s Federal Office for the Protection of the Constitution (BfV) estimates that German companies lose $28 billion-$71 billion and 30,000-70,000 jobs per year from foreign economic espionage. Approximately 70 percent of all cases involve insiders.

- South Korea says that the costs from foreign economic espionage in 2008 were $82 billion, up from $26 billion in 2004. The South Koreans report that 60 percent of victims are small- and medium-sized businesses and that half of all economic espionage comes from China.9

- Japan’s Ministry of Economy, Trade, and Industry conducted a survey of 625 manufacturing firms in late 2007 and found that more than 35 percent of those responding reported some form of technology loss. More than 60 percent of those leaks involved China.

France’s Renault Affair Highlights Tendency to Blame China

Broad French concerns with Chinese economic espionage formed the background of the hasty—and subsequently retracted—accusations by corporate and political leaders in January 2011 that three top executives with the Renault automobile company had taken bribes from China in exchange for divulging technology.

- An investigation by the French internal security service revealed that the accusations against China lacked substance and may have stemmed from a corrupt corporate security officer’s attempts to generate investigative work for a friend’s consulting business.

Past Chinese economic espionage against the French automotive industry—including the parts manufacturer Valeo—probably made the French willing to give credence to any accusation of similar malfeasance against China.

Countries acknowledge the growing use of cyber tools for foreign economic collection and espionage and often note difficulties in understanding losses associated with these cyber collection methods. A 2010 survey of 200 industry executives from the power, oil, gas, and water sectors in 12 Western countries, China, and Russia indicates that 85 percent of respondents experienced network intrusions and that government-sponsored sabotage and espionage was the most often cited cyber threat.

- A 2010 Canadian Government report claimed that 86 percent of large Canadian corporations had been hit and that cyber espionage against the private sector had doubled in two years, according to a press report.

- The German BfV offers no reliable figures on the number of cases and amount of damage caused by cyber-enabled economic espionage, adding that their intelligence services are “groping in the dark.” The German Government has noted the use of CNE tools and removable media devices, claiming that $99 million are spent annually for IT security.

- UK officials note that the cost of an information security incident averages between $16,000 and $32,000 for a small company and between

9We have no information on the methodologies that the Germans and South Koreans used to calculate their losses.
$1.6 million and $3.2 million for firms with more than 500 employees. The United Kingdom estimates that attacks on computer systems, including industrial espionage and theft of company trade secrets, cost the private sector $34 billion annually, of which more than 40 percent represents theft of intellectual property such as designs, formulas, and company secrets.

- Germany and South Korea judge that China, in particular, increasingly uses cyber tools to steal trade secrets and achieve plausible deniability, according to press reporting.\(^b\)

- Unidentified CNE operators have accessed more than 150 computers at France’s Finance Ministry since late 2010, exfiltrating and redirecting documents relating to the French G-20 presidency to Chinese sites, according to a press report.

- The British Security Service’s Center for the Protection of National Infrastructure warned hundreds of UK business leaders in 2010 of Chinese economic espionage practices, including giving gifts of cameras and memory sticks equipped with cyber implants at trade fairs and exhibitions. This followed similar notification sent to 300 UK business leaders in 2007 warning them of a coordinated cyber espionage campaign against the British economy.

- German officials also noted that business travelers’ laptops are often stolen during trips to China. The Germans in 2009 highlighted an insider case in which a Chinese citizen downloaded highly sensitive product data from the unidentified German company where he worked to 170 CDs.

- The Director-General of the British Security Service publicly stated that Russia, as well as China, is targeting the UK’s financial system.

- A Russian automotive company bribed executives at South Korea’s GM-Daewoo Auto and Technology to pass thousands of computer files on car engine and component designs in 2009, according to a press report.

- A German insider was convicted of economic espionage in 2008 for passing helicopter technology to the Russian SVR in exchange for $10,000. The insider communicated with his Russian handler through anonymous e-mail addresses.

Countries Suspect Each Other of Committing Economic Espionage

Allies often suspect each other of economic espionage—underlining how countries can be partners in traditional security matters yet competitors in business and trade. Foreign corporate leaders may make accusations that are not publicly endorsed by their governments.

- According to a 2010 press report, the Germans view France and the United States as the primary perpetrators of economic espionage “among friends.”

- France’s Central Directorate for Domestic Intelligence has called China and the United States the leading “hackers” of French businesses, according to a 2011 press report.

\(^b\) We lack insight on the processes that the Germans and South Koreans used to attribute cyber activities to China.
Some countries exercise various legislative, intelligence, and diplomatic options to respond to the threat of cyber-enabled economic collection and espionage.

- France and South Korea have proposed new legislation or changes to existing laws to help mitigate the effects of economic espionage. France also is considering a public economic intelligence policy and a classification system for business information.
- France, the United Kingdom, and Australia have issued strategies and revamped bureaucracies to better align resources against cyber and economic espionage threats. France created a 12-person Economic Intelligence Office in 2009 to coordinate French corporate intelligence efforts. The United Kingdom established an Office of Cyber Security to coordinate Whitehall policy under a senior official and a Cyber Security Operations Centre within the Government Communications Headquarters (GCHQ) SIGINT unit. Australia created a cyber espionage branch within its Security Intelligence Organization in 2010.
- The United Kingdom is mobilizing its intelligence services to gather intelligence on potential threats and for operations against economic collection and espionage in cyberspace, according to press reports.

German Espionage Legislation Has Limited Results

Germany's Federal Prosecutor General initiated 31 preliminary proceedings on espionage in 2007, resulting in just one arrest and one conviction. German authorities note that espionage cases are often hindered by diplomatic immunity protections and by attribution issues from operating abroad through cyberspace.

Nearly all countries realize that public and private partnerships are crucial to managing the effects of cyber-enabled economic collection and espionage. The United Kingdom notes that 80 percent of its critical national infrastructure is owned and operated by the private sector. German authorities would likely be more corporate feedback and say that most enterprises either do not know when they are victims of cyber espionage or do not want to publicly admit their weaknesses. Most countries engage in some form of corporate outreach.

- The French intelligence services offer regular threat briefings to private companies, according to press reports.
- German authorities regularly exchange information with corporate security officers through a private/public working group that includes Daimler AG, Volkswagen, Porsche, Bayer, the German post office, and the railroad industry.

Corporate Leaders Speak Out on Chinese Espionage

Some foreign corporate executives have singled out Chinese espionage as a threat to their companies.

- British entrepreneur James Dyson—inventor of the bagless vacuum cleaner—warned in 2011 that Chinese students were stealing technological and scientific secrets from UK universities, according to a press report. He noted that Chinese students were also planting software bugs that would relay information to China even after their departure from the universities.
- The CEO of an Australian mining firm said that worries over Chinese and other corporate espionage drove him to adopt a more transparent quarterly pricing mechanism for commodities such as iron ore. He claimed that selling products at market-clearing prices visible to all would minimize the impact of differential information that one party may hold, according to a press article.
## Contents

**Dedication** iii

**Foreword** xi
By Laurel Bellows
President, American Bar Association

**Introduction** xii
By Judy Miller and Harvey Rishikof, Co-Chairs

**Acknowledgments** xvii

### CHAPTER 1

**Purpose of This Handbook** 1
Written by Vincent I. Polley and Jill D. Rhodes
Context 2
What to do? 4

### CHAPTER 2

**Understanding Cyber and Data Security Risks and Best Practices** 7
Written by Lucy L. Thomson and Randy V. Sabett
I. New Technologies Create Unprecedented Challenges for Lawyers 7
II. Causes of Data Breaches 13
III. Data Breaches and Information Security: Addressing Threats and Risks to Data in the Law Office 27
IV. Steps to Protect Confidential Law Firm Records and Prevent Data Breaches—Top Considerations 33

### CHAPTER 3

Data Security and Lawyers’ Legal and Ethical Obligations to Clients 37
Section I. Introduction 37
A. The Problem: Lawyers and Law Firms Have Become High-Priority Targets for Cyber Attacks 37
B. Preparations That Lawyers and Law Firms Would Be Wise to Make 39
Section II. Lawyers’ Legal Obligations to Provide Data Security Arising from Generally Applicable Law 41
Written by Thomas J. Smedinghoff and Ruth Hill Bro
A. Duty to Provide Data Security 41
B. Duties Regarding Specific Data Elements and Controls 57
C. Duty to Warn of Security Breaches 59
Section III. Lawyers’ Obligations to Provide Data Security Arising from Ethics Rules and Other Law Specifically Governing Lawyers 62
Written by Peter Geraghty, Lucian T. Pera, and Alfred J. Saikali
A. Lawyer Ethics Rules 62
B. The Law of Lawyering 67
C. Examples of the Emerging Application of Ethics and Lawyerly Law to Confidentiality to New Technology 68
Section IV. Duty to Advise Clients concerning Use of Cyber and Other Digital Technologies 81
Written by Roland Tappe
A. Introduction 81
B. Foundations for Obligations to Advise on Cybersecurity 83
C. Seven Occasions That Warrant Discussion of Cybersecurity 83
Section V. Practical Considerations 97

### CHAPTER 4

Understanding the Practice Setting 103
Section I. Law Firms 103
Written by Alan Charles Rasi and Jonathan P. Adams, of Sidley Austin, LLP
A. Introduction to Cybersecurity for Law Firms 103
B. Cybersecurity Issues and Challenges for Law Firms 106
CONTENTS

C. How Law Firms May Address Cyber Risk 110
D. Top Ten Suggestions for Law Firm Lawyers 114
Sidebar—Solo & Small Law Firms 116
   Written by Jeffrey Allen and Ashley Hallene
Sidebar—Mid-sized Law Firms 123
   Written by Jason Gonzalez and Anthony Chavez
Sidebar—Large Law Firms 126
   Written by Alan Raul and Jon Adams
Section II. How to Tackle Data Security Issues for In-House Counsel 129
   Written by Anjil Garg and Demetrios Eletheriou
Section III. Considerations for the Government Lawyer 148
   Written by Clark Walton and Timothy H. Edgar
   I. Government Data: A Problem of Growing Insecurity 149
   II. A Variety of Insecurities 152
   III. Legal Considerations 154
Section IV. Public Interest Lawyers 161
   Written by Michelle Richardson
   I. Introduction 161
   II. Issues 161
   III. Implications 163
   IV. Top List of Considerations 167

CHAPTER 5
Best Practices for Incident Response and Cyber Coverage 169
Section I. Achieving Preparedness through Alignment with Voluntary Consensus Standards 170
   Written by George B. Hoff, Jr. and John A. DiMaria
   I. Introduction 170
   II. ISO 22301, the International Standard for Business Continuity Management Systems 172
   III. Challenges for Law Firms and Associations 175
   IV. Opportunities for Law Firms and Associations of All Types and Sizes 179
   V. Conclusion 187

viii CONTENTS

Section II—Cyber Liability Insurance for Law Firms and Legal Organizations 189
   Written by James L. Rhyner and H. Wesley Sunu
   I. Insurance as a Cyber Risk Management Tool 189
   II. Why Consider Cyber Insurance? 192
   III. What Are the Implications of Not Having Your Insurance in Place? 195
   IV. List of Considerations 197

CHAPTER 3, SECTION II APPENDICES
Appendix A. Federal Statutes 199
Appendix B. State Statutes 201
Appendix C. Federal Regulations 207
Appendix D. Court Decisions 211
Appendix E. FTC Decisions and Consent Decrees 212

CHAPTER 3, SECTION III APPENDICES
Appendix F 217
   A). ABA Formal Ethics Opinions 217
   B). ABA Treatises and Annotated Model Standards 219
   C). State Bar Ethics Opinions that address e-mail usage (with links to the full text where available) 220
   D). State Bar Ethics Opinions that address cordless and cell phone usage 232
Appendix G—Outsourcing 234
   ABA Formal Opinion Headnotes 234
   A). ABA Treatises and Annotated Model Standards 235
   B). Bar Association Reports 236
   C). Digests of State Bar Association Ethics Opinions on Outsourcing 236
Appendix H—Cloud Computing 245
   A). ABA Reference Material and Bar Association Reports on Cloud Computing 245
   B). Digests of State Bar Ethics Opinions on Cloud Computing 245
Chapter 2
Understanding Cyber and Data Security Risks and Best Practices
Written by Lucy L. Thomson and Randy V. Sabett

I. New Technologies Create Unprecedented Challenges for Lawyers

Lawyers and law offices are facing unprecedented challenges from the widespread use of electronic records and mobile devices. Gone are the days when lawyers wrote memos and briefs on yellow legal pads and determined legal positions after consulting libraries of beautifully maintained books. Now, most lawyers use smartphones and work on laptops and tablets—state-of-the-art computer devices are the cornerstones of the "electronic courtroom" of the future.

Many law firms operate data centers with global networks of computers, servers, mobile devices, websites, and social media. They are responsible for the full range of information security, data governance, preservation, and incident response functions. Others outsource these functions but must still ensure they are being carried out effectively. Seeking efficiencies from new technologies, most lawyers and law firms use e-mail extensively. Some are considering whether to implement "bring your own device" (BYOD) policies in the organization. They are exploring the use of "cloud" computing for storing and processing data and information.

It is now common practice for law offices to outsource a variety of services to external vendors and business partners located domestically and overseas. Legal organizations interconnect electronically with business partners for a variety of purposes, ranging from IT, finance, accounting, and

8 THE ABA CYBERSECURITY HANDBOOK

HR to procurement and investigations. Legal process outsourcing (LPO), the outsourcing of a variety of legal work, is a growing trend that includes areas such as litigation support for document review, due diligence, legal research, and law libraries. Many of the billions of dollars law offices spend on e-discovery services are used to hire outside vendors.

Responsibilities to Protect Sensitive and Confidential Data
Lawyers must safeguard their own business records, including intellectual property, lawyer work product, and financial and employment records, to name a few. Electronic records are an integral part of every lawyer's business.

Clients provide records to a lawyer or law firm on a confidential basis. In those circumstances, clients may be informed about or believe they understand the security posture of the law firm. Throughout the course of representing clients, lawyers receive volumes of sensitive and confidential data and information—attorney-client privilege information, client trade secrets, and all types of personally identifiable information (PII), such as financial, health-care, and law enforcement records.

That said, law firms also receive sensitive and confidential information through litigation or compulsory process, or as a result of investigations or adversary actions against individuals and organizations. In these cases, not only adversaries, but also third parties are often swept up in lawsuits or other legal proceedings. Given that lawyers have access to the most sensitive and secret information in civil and criminal cases—including private investigations, records sealed or under a protective order, classified data, grand jury records, and other similar information—it is critical that this information be protected from breaches and unlawful exposure.

In addition, a staggering array of sensitive information is acquired by law firms in e-discovery. A sobering fact is that much of the data and information obtained by law firms may have been created, used, and maintained in

2. See Chapter 3, which provides an in-depth discussion of the responsibilities of lawyers to protect sensitive and confidential information.
a secure environment and then transferred—often without the knowledge, agreement, or consent of the individual or organization that created or collected the information—to an environment where the extent of security protections in the law office may be unknown or is not assured.3

In order to protect confidential information, law offices must know what data they have, where it resides, its level of sensitivity, and how it is secured. In addition to the expected locations for data such as computer servers, desktop and laptop computers, and mobile devices (including mobile phones and tablet computers), information may reside in other, somewhat less expected locations. For example, backups can contain significant amounts of sensitive information. Also, sensitive data may be created on a mobile device and posted to social media. Likewise, as more and more operations move to the cloud, so will the associated data.

The Threat
In today’s digital world, threats to information systems are evidenced almost everywhere a computer, server, laptop, smartphone, thumb drive, or other electronic device is operating.4 The proliferation of mobile devices and wireless technology that enables mobile commerce (m-commerce) and a continually expanding array of applications (apps)—more than 1.5 million—presents many vulnerable points in the flow of sensitive data in computer networks. The lack of security resulting in unencrypted data on computers, laptops, and other mobile devices that are lost or unaccounted for creates another type of threat. Electronic records are not the only problem—examples of lax security include volumes of paper documents as well. Many data breaches occur when documents containing personal information are thrown in the trash or in dumpsters where strangers can retrieve them.

Attacks to information security vary greatly in terms of who is conducting an attack, the purpose of the attack, and the means of conducting it. Attackers seeking to compromise an organization’s computer systems have a wide variety of motives, which may include embarrassment to the organization, economic espionage, pecuniary interests, political and ideological goals, creating misleading information, and simple maliciousness. Threats to information security, however, include more than attacks. They also include natural disasters and accidental events.

Law Firms Are Prime Targets—The Significant Resulting Damage
The notification requirements of the state data breach laws have helped to highlight the significant increase in the number of data breaches during the past several years.5 Forty-six states currently have some type of data breach notification law.6 As a result of the huge volume of critical data lawyers collect about companies and individuals, hackers are targeting law firms.

Attackers are targeting industries in order to steal personal information (for identity theft or other similar crimes) and money and credit card numbers (for financial gain), as well as to advance their strategic priorities. In the case of law firms, there are many reasons for hackers to target the information being held by the firms. From a value perspective, law firms hold some of the highest “quality” data concerning their clients. Whether intellectual property, strategic business data, or litigation-related theories, firms hold some of the most sought-after information on target companies.

The consequences to clients, and even innocent third parties, of a data breach can be devastating—potentially subjecting them to identity theft, fraud, negative publicity, and even financial ruin. Breaches have also resulted in damage to business reputations, bank losses, and bankruptcy, with resulting civil damage actions, administrative proceedings, or criminal indictments.

Much of the valuable data law firms hold—particularly intellectual property, strategic business data, and knowledge of mergers and acquisitions and international transactions—carries with it obligations associated with attorney-client privileged data. Loss of such data due to a data breach can destroy the privilege.

3. Until a law office has conducted a risk assessment and adopted a comprehensive information security program, it will not be in a position to vouch for an appropriate level of security and its ability to protect sensitive and confidential data and information, it requested by a client or the Court.


Understanding Cyber and Data Security Risks and Best Practices

Similarly, protective orders imposed by courts to preserve the secrecy of sensitive data can be violated in the event of a data breach. Although Rule 26(b) of the Federal Rules of Civil Procedure allows broad discovery on a variety of issues, Rule 26(c)(7) allows a court to issue an order that "a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a designated way." If a data breach were to occur at a firm subject to such an order, arguably that order could be violated and the firm might face serious consequences.

From a business perspective, a breach of security or information loss by a law firm can have significant negative effects. If a firm loses client information, the client might decide to take its business elsewhere. For lawyers in the firm, a data breach may result in ethical violations that have serious impacts.8

Breaches on the Rise—Threats and Vulnerabilities Illustrated

Massive data breaches are occurring with alarming frequency. Failed security has resulted in thousands of data breaches that have led to the loss or compromise of millions of personally identifiable records.9 In order to prevent data breaches, it is essential to analyze and understand the root causes of the security failures and develop a specific plan to address them. Analysis of the types of breaches that have occurred is very illuminating, for the conclusion is that most of these breaches did not have to happen.

To protect one of the most valuable and vulnerable assets of all organizations—data and information—is not only good business practice, it will avoid the high costs associated with responding to data breaches, potential liability, negative press, embarrassment, and ultimately loss of trust of clients, judges, and the public.9

---

7. Chapter 3 provides an in-depth discussion of the responsibilities of lawyers to protect sensitive and confidential information.
9. The high costs of responding to data breaches have been well-documented. The Ponemon Institute concluded that data breaches can have "severe economic consequences," and calculated the average cost for the organizations participating in the study to be $2.4 million over a two-year period. The Annual Benchmark Study on Patient Privacy & Data Security, PONEMON INSTITUTE, LLC (Dec. 6, 2012), available at http://www.2idesk.com/
II. Causes of Data Breaches

Hacker Attacks
Over the past several years, the information of millions of individuals has been compromised through data breaches, often resulting in identity theft and fraud. Data breach trends over the past several years reveal that hackers were responsible for about one third of the hundreds of data breaches. Several of the largest breaches involved sophisticated global organizations of hackers who infiltrated information systems at vulnerable points—where sensitive personal records were unsecured, even though those same records were encrypted in company networks. Advanced persistent threats (APTs) are among the most serious types of cyber attacks because their focus is espionage. Originating in the Asian Pacific countries, these attacks employ undetectable "zero-day" exploits (taking advantage of vulnerabilities in software that are known, but not yet fixed) and social-engineering techniques against company employers to breach networks. The typical intrusion by the APT involves undetected access into a victim computer system (in violation of federal and state law) and then the theft of significant amounts of data. Through the intrusions, hackers grab a foothold into a company's network, sometimes for years, and even remaining after a company has discovered them and taken corrective measures.

Both large and small law firms have been the target of hacker attacks in the United States as well as abroad. Every Mandynt, a cybersecurity firm that helps organizations secure their networks against threats and resolve computer security incidents of all kinds, estimated that eighty major law firms were breached in 2011 alone. In 2011 in Washington, DC, the law firm Wiley Rein was a victim of a massive attack by Chinese hackers referred to as Byzantine Candor that encompassed twenty major companies. Security researchers have referred to the hackers as the "Comment group," since they infiltrated computers using hidden web-page computer code known as "comments." Their attack methodology began with phishing attacks that transmitted malware (malicious code) in e-mails to members of the firm. Audit log files showed that the malware enabled the hackers to access encrypted passwords they were able to crack offline. The hackers were able to access the firm's network and steal sensitive data by acting as network administrators, collecting critical data and exfiltrating it over the course of months. The thousands of pages of e-mails the hackers stole included confidential communications with clients.

When a law firm is hacked, the consequences of failing to employ adequate security can be unexpected and widespread, leading to embarrassing disclosures, injury to innocent third parties, lawsuits, government investigations and fines, and ultimately ceasing business. The UK law firm ACS:Law was breached in September 2010 by hackers who were angry at the tactics used by the law firm to target individuals they claimed were engaged in illegal file sharing. As a result of a distributed denial-of-service (DDoS) attack, the law firm's website crashed, causing unencrypted e-mails sent to broadband users accused (improperly in most cases) of sharing pornography to be publicly visible on the law firm's website. The e-mails were then apparently downloaded by the public "hundreds of thousands" of times. It was reported that one email contained the personal details of 10,000 people accused of file sharing pornography, including names and home addresses, IP addresses, and in some cases, credit card information.
ensuing litigation for harassment by Privacy International (PI) on behalf of the individuals whose information was breached, they asserted the breach was caused by "poor server administration" and a lack of security. As a result of the breach, the law firm ceased operation. The lawyer who owned the firm was fined £1,000 by the UK Information Commissioner’s Office in May 2011 (the fine would have been £200,000 if the law firm had not gone out of business). The Information Commissioner found:

Sensitive personal details relating to thousands of people were made available for download to a worldwide audience and will have caused them embarrassment and considerable distress. The security measures A&J had in place were barely fit for purpose in a person’s home environment, let alone a business handling such sensitive details.20

In another case, after a bookkeeper at a Toronto firm clicked on an e-mail attachment or link or downloaded an app with malware, a “Trojan banker” virus established a backdoor through the bookkeeper’s computer. The program mimics (spoofs) a bank’s website to lure the unsuspecting user to enter critical personal and account information. It worked as a keylogger, transmitting keys, including passwords, in real time to the hackers. Enabling the hackers to monitor deposits into the account, in December 2012 they stole a six-figure amount of money from the firm’s trust account.21 Law offices, which are known to have large amounts of money in these accounts, are easy targets for this type of hacking.

Additionally, in a different breach, a large volume of e-mail with client documents attached was stolen from the small Alexandria, Virginia, law firm Puckett & Faraj in early 2012 by the hacking group Anonymous.22 Not only were detailed legal documents about the firm’s defense of high-profile military defendants accused of war crimes stolen, but also personal lawyer correspondence relating to other clients and matters. The hackers were able to gain access to Google e-mail accounts because the firm failed to use strong passwords, and by exploiting vulnerabilities in the firm’s website.23 The law firm apparently was targeted by the hackers for representing a US marine convicted of negligent dereliction of duty in a 2005 attack in Haditha, Iraq, that resulted in the deaths of 24 unarmed civilians.

Mobile Devices

Data breaches are pervasive because they are not only the result of hacker attacks, but they are also caused by sloppy security practices. More than one third of data breaches resulted from the theft or loss of laptops, computers, hard drives, backup tapes, PDAs, or other portable media containing unencrypted personal information.24 From 2012 through mid-2013, the loss or theft of 132 mobile devices resulted in the exposure of 2,681,311 personal records.25 In January 2013, Oldcastle Law Group in Georgia reported that an employee’s laptop was stolen during a break-in to her car in December 2012. The firm said they believe the laptop may have contained personal information relating to Oldcastle ACP employees, including names, bank account information, and Social Security numbers.26

Some of the largest breaches involving lost or stolen unencrypted mobile devices are identified in the following table.
Table 2.1 Breaches caused by lost or stolen mobile devices\textsuperscript{27}

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Records Breached</th>
<th>Lost/Stolen Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2013</td>
<td>TRRCA—SAIC</td>
<td>4,600,000</td>
<td>Backup tapes stolen</td>
</tr>
<tr>
<td>February 2008</td>
<td>Bank of NY Mellon Corp.</td>
<td>4,500,000</td>
<td>Tapes lost by third-party vendor</td>
</tr>
<tr>
<td>November 2011</td>
<td>Surrey Physicians Service and Foundation, CA</td>
<td>4,200,000</td>
<td>Desktop computer stolen</td>
</tr>
<tr>
<td>March 2010</td>
<td>Educational Credit Mgr. Co.</td>
<td>1,100,000</td>
<td>Portable device stolen</td>
</tr>
<tr>
<td>March 2011</td>
<td>HealthNet, CA—IBM</td>
<td>2,900,000</td>
<td>Server drives lost</td>
</tr>
<tr>
<td>February 2011</td>
<td>Jacobi Medical Center, Bronx, NY</td>
<td>1,700,000</td>
<td>Backup tapes stolen</td>
</tr>
<tr>
<td>October 2011</td>
<td>Nemours, DE</td>
<td>1,400,000</td>
<td>3 backup tapes missing</td>
</tr>
<tr>
<td>November 2009</td>
<td>Health Net, CT</td>
<td>1,300,000</td>
<td>Portable hard drives lost</td>
</tr>
<tr>
<td>October 2009</td>
<td>BlueCross BlueShield, TN</td>
<td>1,000,000</td>
<td>Hard drives missing</td>
</tr>
<tr>
<td>September 2009</td>
<td>Oklahoma Dept Human Services</td>
<td>1,000,000</td>
<td>Computer stolen</td>
</tr>
</tbody>
</table>

These breaches illustrate the sheer magnitude of the exposure of personal records and the potential damage to millions of individuals. In light of available security measures and their widespread acceptance within the information security community, there is no excuse for organizations that collect and store PII and other sensitive information to fail to fulfill their duty to protect the information.

The importance of addressing these types of breaches is illustrated by a recent Federal Trade Commission (FTC) case involving the operator of a leading cord blood bank. In February 2013, Cbr Systems, Inc., agreed to settle FTC charges that its failure to provide reasonable and appropriate security for consumers’ personal information contributed to a December 2010 security breach during which unencrypted backup tapes a Cbr laptop, external hard drive, and USB drive containing consumers’ personal information, were stolen from a Cbr employee’s personal vehicle.\textsuperscript{28}

Data breaches can be prevented by encrypting the data on the devices, enforcing procedures that do not permit individuals to transport sensitive data on moveable media, keeping careful track of the devices, and having the highest standards and requirements for couriers to move backup tapes and CDs to offsite storage facilities or from one location to another.

The Identity Theft Resource Center has analyzed the problem this way: “This is 100% avoidable, either through use of encryption, or other safety measures. Laptops, portable storage devices and briefcases full of files, outside of the workplace, are still ‘breaches waiting to happen.’ With tiered permissions, truncation, redaction and other recording tools, PII can be left where it belongs—behind encrypted walls at the workplace.”\textsuperscript{29}

\textbf{Bring Your Own Device (BYOD)—While BYOD may appear to be a good approach for organizations seeking to reduce costs and accommodate a generation of younger lawyers who are investing in the latest mobile devices, it may be a trap for the unwary. By permitting individuals to create and access sensitive data with their personal devices, the law office transfers control to others who may not have appropriate security to safeguard the data. Permitting BYOD may also remove from IT managers the critical knowledge about what data the law office has obtained and how it is processed and secured.}

Many difficult issues must be addressed before a law office adopts a BYOD policy. As the use of mobile devices explodes around the globe,\textsuperscript{30}

\begin{footnote}{27} 2008-12 Data Breach Reports, Identity Theft Resource Center.\end{footnote}

\begin{footnote}{28} According to the complaint, the unencrypted backup tapes included names, gender, Social Security numbers, dates of birth, driver’s license numbers, credit and debit card numbers, card expiration numbers, checking account numbers, addresses, email addresses, telephone number and adoption type of nearly 300,000 Cbr customers. The unencrypted devices also contained network information, including passwords and protocols, which could have permitted an intruder to access Cbr’s network where sensitive personal health information was stored. The settlement requires Cbr to establish and maintain a comprehensive information security program and submit to independent security audits every other year for 20 years. See Cord Blood Bank Settles FTC Charges that it Failed to Protect Consumers’ Sensitive Personal Information, Federal Trade Commission (Jan. 28, 2013), http://bit.ly/npa20130128cbrsclm.


30. Mobile devices are the fastest growing computing technology. By the end of 2013, the number of mobile-connected devices will exceed the number of people on earth, and by 2017 it is expected that there will be nearly 14 mobile devices per capita. Cisco Visual}
Concerns about the security of data and communications with mobile devices are increasing. Some mobile breaches are the result of vulnerabilities in the design and configuration of mobile devices. As well, hackers have inserted malware into apps so when users download them onto mobile devices, the malware allows the hackers to gain access to sensitive information. Certain malware on mobile devices can subvert search results and redirect users to a web page where they are encouraged to download malware. Malware can cause users' personal information to be publicly disclosed without their knowledge. Hackers can intercept unencrypted data as they are transmitted to and from mobile devices. These examples provide only highlights of the many threats posed by mobile devices. The vulnerabilities are particularly serious if the mobile devices are used to communicate with legal clients by e-mail or through social media, or to view, process, or store confidential client data or information.

There are a number of steps a law office should take to protect confidential data on mobile devices, if it chooses to permit personal devices on the network. Where possible, the law firm should use Mobile Device Management, which provides a centralized way to manage mobile devices remotely, including, significantly, the ability to lock or erase a lost device remotely and check its geographic location. Only known users and devices should be permitted on the network; app providers should be known as well. Phones that have been jailbroken or rooted should not be permitted on the network. Phones and tablets that are used to create, transmit, or store sensitive data, even in e-mail, should have centralized management of passwords with acceptable password policies, and all user data should be encrypted. Such management software is readily available from many vendors.


13. The FBI has issued a warning about malware that attacks Android operating systems for mobile devices and is designed to lure users to compromise these mobile devices. See Smartphone Users Should be Aware of Malware Targeting Mobile Devices and Safety Measures to Help Avoid Compromise, FBI (October 12, 2012), http://www.fbi.gov/scams-safety-style-scams-scams.


20 THE ABA CYBERSECURITY HANDBOOK

Malicious Insiders

Malicious insider attacks are on the rise and pose a serious threat to the security of sensitive information. These attacks have accounted for a third of the data breaches in recent years. The motivation for employees to steal data may range from financial gain (theft of trade secrets and other sensitive information for sale) to revenge for perceived wrongs committed against them. Individuals who abused administrative privileges led to a significant number of breaches, and security failures such as not suspending system access for terminated employees caused many breaches as well.

This is a serious risk for law firms. For example, a federal grand jury in Pittsburgh indicted a legal secretary who had been fired from a law firm. She and two colleagues were charged with hacking into a computer server at the law firm, where they installed software that could be used to capture the passwords of anyone on the firm’s network. Subsequently, they illegally obtained personal financial information of law firm employees.16

In one of the most publicized insider cases, involving the Bank of New York Mellon, a computer technician who worked in the bank’s information technology department stole the identities of 2,000 bank employees and opened bank and brokerage accounts. He then used them to steal more than $1.1 million from charities, nonprofit groups, and other entities.17 The defendant pleaded guilty to grand larceny, money laundering, and computer tampering.

During the first quarter of 2013, twenty-six to twenty-eight insider breaches were reported by organizations tracking data breaches.18 In 2012, eighty-eight insider breaches were reported. From 2007 to 2012, 372 data breaches caused by insiders were reported. About one quarter of the reported


Understanding Cyber and Data Security Risks and Best Practices

insider breaches were perpetrated by employees who had some type of job change—they were fired, had resigned, were newly hired, or had changed roles within the organization.

Defending an organization’s perimeter from external attack does not protect against valuable information seeping out due to insider malefactor, whether that behavior is characterized as malicious, mischievous, or ignorant/accidental. Carnegie Mellon University has published a list of best practices to minimize the risk of insider attacks. Databases are vulnerable to attacks from both insiders and hackers. These vulnerabilities are well documented and include the use of default and weak passwords, failure to patch known vulnerabilities, misconfigurations, and excessive privileges granted to users. Specific security measures must be taken to protect personal data in the databases of legal organizations.

Inadvertent Postings on Websites and Other Disclosures

Through careless handling, personal data—particularly Social Security numbers—are often exposed in postal mailings. In addition, data may also be posted on websites where it is accessible to individuals who are not intended to access it. For example, in June 2011 a UK government council (Surrey County Council) was fined £120,000 by the UK Information Commissioner’s Office for violating the UK Data Protection Act. Officials had sent confidential personal health information to the wrong e-mail addresses.

THE ABA CYBERSECURITY HANDBOOK

In February 2012 the St. Joseph Health System alerted more than 31,000 patients in California that their personal health information records may have been searchable on the Internet. A New York company advised clients in April 2013 of the “unintentional exposure” of their Social Security numbers that occurred as a result of a system mistake involving a recent Rollins TODAY mailing that had inadvertently displayed SSNs in a number sequence on the mailing label.

Improper Disposal of Personal Information—Sensitive personal records in paper and as digital formats must be protected. At least twenty-nine states have enacted laws that require entities to destroy, dispose of, or otherwise make personal information unreadable or undecodeable. A breach in February 2013 by the Walt and Associates Law Firm involved hundreds of personal documents that were found in a Bernallillo County recycling center in Tijeras, New Mexico, containing dozens of people’s criminal histories, depositions, and even medical records. The March 2013 newspaper report “Tulsa Medical Records Turn Up on Ponca City Newspaper Loading Dock” highlights the problem of sloppy handling of sensitive records. A three-inch stack of medical records from Tulsa’s Saint Francis Hospital showed up in Ponca City on the loading dock of the local newspaper—in a stack of pallets shipped from a recycling operation near Tulsa.

Peer-to-peer (P2P) file-sharing technology may also create a significant risk of a breach when it is installed on the same computer as sensitive and personal information. P2P is a way to share music, videos, and documents,

38. CERT Insider Threat Center, CARNEGIE MELLON UNIVERSITY, http://www.cert.org/insider_threat/
39. Josh Shaul, Steps to Comprehensive Database Security and Compliance, APPLIC-ATION SECURITY, INC. (2011), available at http://www.us-cert.gov/GFIRST/presentations/2011/Combating_Database_Insider_Threat.pdf. Specific security measures that must be taken to protect personal data include: (1) inventory your databases; (2) classify systems with sensitive data; (3) scan for vulnerabilities and misconfigurations, keep up-to-date with security patches, enforce strong passwords; and audit configurations and settings; (4) identity privileged users (DBA’s); (5) validate access to sensitive data, assign restricted permissions on tables with sensitive information; (6) prioritize and fix what you can; (7) monitor database activity; and (8) encrypt data in-transit and at rest using network-level encryption and volume-level encryption.
46. The FTC has notified almost 100 organizations that personal information, including sensitive data about customers and employees, has been shared from the organizations’ computer networks and is available on file-sharing networks to any users of these networks.
play games, and facilitate online telephone conversations. It enables computer users to form a network and share digital files directly with other computers on the network. When the P2P file-sharing software is not configured properly, sensitive records not intended for sharing may be accessible to anyone on the P2P network. People who use P2P file-sharing software can inadvertently share files: they might accidentally choose to share drives or folders that contain sensitive information, or they could save a private file to a shared drive or folder by mistake, making that private file available to others. In addition, viruses and other malware can change the drives or folders designated for sharing, putting private files at risk. If a law office uses Skype, or permits lawyers to work on a home computer or mobile device, confidential client information could inadvertently be at risk.

**Threats Based on Accidental, Inadvertent, or Natural Events**

While it is common to focus on external threats and risks related to protecting data, often times, it is vulnerabilities created due to a lack of knowledge or understanding about basic cybersecurity that lead to breaches and weaknesses. In addition, natural events can also impact information systems and increase risks of data breaches.

1. **Human error**—Even when acting in good faith, people make mistakes that can cause an information system to operate incorrectly or leave an organization vulnerable. These errors include typographical errors, failure to follow security procedures, incompetence, and mistakes in judgment.

2. **Accidents**—Various kinds of accidents can affect information systems, including fires, water pipe breaks, physical damage to computer equipment, the erasure of media caused by accidental exposure to magnetic fields, and accidental deletion of information.

---


subjected to a flood of spam," New York–based law firm White & Case restricts lawyers from using file-hosting programs such as Dropbox.8

Wireless communication creates opportunities for hackers to intercept sensitive data such as passwords for logging in to corporate networks and online banking sites. Public Wi-Fi locations such as airports, hotels, and coffee shops—convenient places to check e-mail—often do not have security features necessary to protect confidential client data. Hackers can use a proxy server to create a fake Wi-Fi hotspot (an "evil twin") and intercept or redirect confidential communications. Law offices must encrypt the information to protect it.8

Business Partners Can Be a Weak Link—A Two-Edged Sword for Law Firms

The Mandiant APT1 report8 emphasized the significant problem of business partners as an attack vector into companies of strategic interest to global hackers. From the point of view of hackers, law firms are considered "business partners" of major corporate clients with a trove of proprietary data—a weak link to be exploited.

In addition, it can be said that the security of a law firm is only as strong as that of its weakest business partner. Law firms and corporate legal departments are outsourcing a variety of legal work to outside businesses. If the security of those outside businesses is weak, then the law firm itself is vulnerable.

47. See The State Bar of California, Standing Committee on Professional Responsibility and Conduct Final Opinion Interim No. 08-2002: Warning about the lack of security features in most Wi-Fi locations. Available at http://ethics.calbca.ca.gov/Ethics.aspx. "Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?"
54. These publications included the New York Times, Washington Post, LA Times, Forbes, and NPR, tech publications such as Ars Technica, Wired, Tech News, The Tech Herald and The Hacker News, legal publications such as Law Tech News, Corporate Counsel, Legal Times and National Law journal, and independent media such as Think Progress, The Brad Blog, Salon and FireDogLaw.
56. Id.
57. D.C. Office of Bar Counsel, Kevin Zerez, Esq., on behalf of SnoqFlopChamber.com and VelvetRevolution, Inc., NGOs dedicated to corporate and government transparency and accountability, filed a disciplinary complaint against three Hunton & Williams lawyers.
III. Data Breaches and Information Security: Addressing Threats and Risks to Data in the Law Office

What is “Data Security”?
The breaches and threats described above illustrate the need for data security and a frequent absence of it across law offices and other legal practices. In order to address these risks, lawyers need to understand data security and the basics of risk management.

Simply put, data security involves protection of digital assets. It is critical for law offices to have appropriate data security because of the huge volume of data lawyers collect about companies and individuals. Just as the government, companies, and individuals protect their physical assets, data security must be an integral part of any technology solution.

“Confidentiality,” “integrity,” and “availability” are the three cornerstone goals that every data security program is designed to achieve.

- **Confidentiality**—Protection of information against unauthorized disclosure, whether intentional or accidental.
- **Integrity**—Protection of information against corruption, tampering, or other alteration; this capability includes safeguarding the accuracy and completeness of information.
- **Availability**—Ensuring that information and systems can be reliably and promptly accessed and used when they are needed.

“Data security” can be defined as a risk management process that security professionals undertake when protecting information and information systems. The process includes identifying the universe of possible threats to information assets, determining whether the assets are vulnerable to these threats, and implementing appropriate and cost-effective safeguards needed to address the threats. A threat is the possibility that any man-made, accidental, or natural event may damage information or information systems. Vulnerabilities exist when there is an absence of, or weakness in, a safeguard to address a threat, leaving information assets unprotected.

Data security encompasses a number of disciplines. Some examples include:

- **Computer Security**: Protecting data and information within an information system, including securing the operating system, applications, and access to workstations and mobile devices.
- **“Logical” or Network Security**: Protecting information as it is transmitted from system-to-system using computer networks and securing computer networks from intrusion and unauthorized access.
- **Physical Security**: Protecting physical facilities and infrastructure from intrusion, theft, tampering, vandalism, unauthorized access, accidents, and natural disasters.
- **Telecommunications Security**: Protecting information and preventing it from unauthorized access to telecommunications systems other than computer networks, such as phone and voicemail systems, facsimile machines, pagers, broadcasting systems, and video conferencing systems.
- **Security Management Practices**: Protecting a firm’s information assets by the actions of its management, such as developing and implementing security policies and procedures, classifying and determining the value of information and client assets, risk analysis, risk management, auditing, and business continuity and disaster recovery.
- **Personnel Security**: Providing assurances that personnel utilized by a firm (including all lawyers, employees, consultants, and contractors) are competent, adequately trained, trustworthy, and managed appropriately.

Several private sector organizations and the National Institute of Standards in Technology (NIST) have issued standards, guidance, and compliance tools that organizations may use to develop and implement their security plans. These are based on a common body of knowledge among security professionals of what steps are needed to protect sensitive data and information systems. 58

58. The various NIST and other governmental standards and guidelines are excellent resources and provide much more detail on accepted best practices. See e.g., NIST SPECIAL PUBLICATION 800-53, Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations (April 2013).

Other resources include various IT security associations. See e.g., SANS, www.sans.org (last visited May 17, 2013). The ISEEC Information Security Management System (ISM) family of standards is based on the governing principle that an organization should design, implement, and maintain a coherent set of processes and systems to manage risks to its information.
Why Is Data Security Important?
A law office will, undoubtedly, face many challenges related to its Internet presence besides security (such as, for example, software compatibility, document control systems, time entry and billing software, relationships with service providers, or any number of other issues). A lack of attention to security issues, however, could lead to significant problems. Business could be temporarily disrupted if a minor compromise occurs. More serious results could be felt if, for example, a sustained attack or breach of security occurs. In the case of more significant compromises, the continuity of the law firm’s business could be severely affected and, in the worst scenarios, the firm could be forced out of business.

Ultimately, a firm could face substantial and hard-to-quantify liability if a data security breach was to occur. Instead of waiting for a breach to take place, proactive measures must be implemented that will significantly lessen the likelihood of a compromise. These actions can potentially lead to the reduced likelihood of liability.

Firms seeking to establish an online presence should take security into account from the very beginning. Firms with an established online presence should determine the need for, and implement, an appropriate level of security. Whether new or established, all law offices should have an ongoing assessment process that allows their security posture to address risks over time as conditions dictate. This awareness and ongoing assessment process are critical to two major areas of online security: security management (i.e., what must be done to keep the systems properly secured) and security implementation (i.e., how the systems are actually secured).

Who Is Responsible?
Data security must be adopted at the highest level of a law office and then flow down through the rest of the organization. Without such “buy in” by the firm management, there will be no incentive for the rest of the members of the firm to adopt appropriate technology and follow good security practices.


The Need for Risk Assessment
Ensuring the confidentiality, integrity, and availability of data is fundamental to protecting the information in legal offices. Information security is not a mystery—it is based on a systematic assessment of threats and risks that are present in a particular information system.

Legal organizations must conduct a risk assessment as part of their security management processes. Based on a risk assessment, appropriate security controls can be selected, implemented, and continuously monitored, so that risks and vulnerabilities are reduced to a reasonable and appropriate level.59

The purpose of a risk assessment is to inform law office decision makers and support risk responses by identifying: (1) relevant threats to law offices or threats directed through organizations against the law firm, (2) vulnerabilities, both internal and external, to the law firm, (3) impact (i.e., harm) to the firm and its clients that may occur given the potential for threats exploiting vulnerabilities, and (4) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

The principal goal of the law firm’s risk management process should be to protect the organization and its ability to perform its mission, not just its IT assets. A risk analysis process includes, but is not limited to, the following activities:

1. Evaluate the likelihood and impact of potential risks to sensitive and confidential information;
2. Implement appropriate security measures to address the risks identified in the risk analysis;
3. Document the chosen security measures and, where required, the rationale for adopting those measures; and
4. Maintain continuous, reasonable, and appropriate security protections.60

59 Id.

60 A prototype for conducting a risk assessment and assessing compliance with the HIPAA Privacy and Security Rules, for example, are available. See New HIPAA Tool Helps Organizations Meet Security Requirements, NIST (Nov. 22, 2013) http://www.nist.gov/evi/
Understanding Cyber and Data Security Risks and Best Practices

Risk analysis should be an ongoing process in which the law office regularly reviews its audit logs to track access to confidential records and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to sensitive and confidential information.

Achieving Optimal Network Security through Continuous Monitoring
To protect against massive data breaches, it is clear that the legal profession, as well as companies in the retail, healthcare, education, and financial sectors, as well as government agencies, must take immediate action to strengthen their security posture. This includes constant monitoring of systems, security status, and risks, often referred to as continuous monitoring. Continuous monitoring of systems and networks is essential to protect against the broad range of serious threats to information systems.61

At the direction of the US Congress, NIST is developing a common information security framework for the federal government and its contractors.62 Robust continuous monitoring will provide law firms with the information necessary to make cost-effective, risk-based decisions.63 While NIST guidance has been developed for government agencies, it is equally appropriate for private sector organizations, including law firms.

Information security continuous monitoring is a critical part of organization-wide risk management. To properly support an organization's risk management framework, security must be incorporated into the architecture and design of the organization’s information systems and supporting information technology (IT) assets. Continuous monitoring provides an understanding of threats and threat activities; evaluates the security impact of actual and proposed changes to the system; assesses all security controls, collecting, correlating, and analyzing security-related information; provides actionable communication of security status across all levels of the organization; and provides active management of risk by organizational officials.

Continuous monitoring is designed to provide meaningful, actionable intelligence and reporting—instead of merely collecting data. Cybersecurity situational awareness will inform law offices about the threat, vulnerability, and compliance posture of the system, as well as provide information about incidents that will need to be investigated. Potential threats must be investigated, and targeted attacks can be detected in advance or addressed as they occur, enabling a highly proactive security posture. The results of continuous monitoring will ensure that all the information necessary to address security incidents and potential attacks is readily available for analysis and review. The objective is to address the multitude of security threats and risks in a timely, disciplined, and structured fashion.

Is Protecting the Privacy and Security of Confidential and Sensitive Law Firm Records an Attainable Goal?
It is not necessary or appropriate to assume that electronic records cannot be protected from data breaches. Lawyers and law offices have a responsibility to protect confidential records from unauthorized access, whether malicious or unintentional, by both insiders and hackers. The model Ethics 20/20 rules adopted by the ABA in 2012 explicitly require that lawyers provide "competent representation" by keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology (Rule 1.1). Further, to protect the confidentiality of information, 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" (Rule 1.6). 64

To do this, organizations must have appropriate privacy and security policies in place to protect the data, as well as risk-based management, operational, and technical controls necessary to ensure information security. By conducting a risk assessment and prioritizing steps to secure an information system, the majority of privacy and security risks can be addressed. As the amount of sensitive and confidential information collected in electronic form continues to grow, the imperative of information security will only become stronger.

IV. Steps to Protect Confidential Law Firm Records and Prevent Data Breaches—Top Considerations

Data breaches can and must be prevented. 65 Law offices that collect, use, store, and share sensitive and confidential information must accept responsibility for protecting the information and ensuring that it is not compromised by hackers or malicious insiders or inadvertently accessed, lost, or stolen. Following are some top considerations for lawyers and law offices to begin to address data security issues:

1. Develop a comprehensive information security plan specifically designed to prevent data breaches. The plan must include appropriate security for all aspects of the computer network, including technical, operational, and management controls. Prioritize security resources so that the most critical and vulnerable aspects of the system are addressed first. For example, spear phishing is currently a common attack methodology used by hackers; address it by creating a culture of security throughout the law office, and enforce security policies to combat this problem. 66

2. Conduct a risk assessment. Carefully document how the security controls selected and implemented address all risks identified. Ensure that information security continuous monitoring is an integral part of organization-wide risk management.

3. Secure the law firm’s sensitive data using appropriate encryption technology. Inadequate or inappropriate key management can result in data breaches and/or loss of data; ensure appropriate encryption is utilized on mobile devices.

4. Where possible, use Mobile Device Management to protect confidential data on mobile devices, including the ability to lock or erase a lost device remotely and check its geographic location.

5. Only known users and devices should be permitted on the network; app providers should be known as well. Phones that have been jailbroken or rooted should not be permitted on the network. Phones and tablets that are used to create, transmit, or store sensitive data, even in e-mail, should have centralized management of passwords with acceptable password policies, and all user data should be encrypted.

6. Develop a data retention and destruction plan so personal data is not at risk—sanitize regularly.

7. Be prepared if a data breach occurs. Engage in pre-event liaison planning—identify and build bridges with ISPs, law enforcement, and other key security resources, so you know who to go to when an incident or breach occurs, and so they know who you are.

8. Build internal company/firm teams of first-responders who have been briefed on the issues and their implications, so they do not have to think through such things for the very first time in the middle of an incident or data breach.

64. Chapter 3 provides an in-depth discussion of the responsibilities of lawyers to protect sensitive and confidential information.

65. See LUCY THOMSON, DATA BREACH AND ENCRYPTION HANDBOOK 16, 241-253 (ABA, 2011).

66. Provide training to teach employees not to open e-mail attachments or click on links from unknown sources. One follow-up approach security experts have found to be effective is to send mock spear phishing e-mails to all staff and that down the accounts of those employees who click on attachments or website links that may contain malware. King & Spalding has advised employees they will not be permitted to log into personal e-mail accounts from work-issued computers, including laptops, beginning May 1, 2013. Available at news.ks.com (April 17, 2013).
Lawyers and law firms, business owners, and data custodians and their lawyers in the private sector and in government around the globe must redouble their efforts to understand the risks of collecting, storing, and sharing sensitive and confidential information, the many ways data can be breached, and the tools available to protect the data. They must develop the expertise to avoid these breaches and to address them appropriately if and when they occur.
Cybersecurity: Legislation, Hearings, and Executive Branch Documents

Rita Tahan, Information Research Specialist (tahan@loc.gov, 7-6739)
August 8, 2014 (R43317)
Jump to Main Text of Report

Summary
Cybersecurity vulnerabilities challenge governments, businesses, and individuals worldwide. Attacks have been initiated against individuals, corporations, and countries. Targets have included government networks, companies, and political organizations, depending upon whether the attacker was seeking military intelligence, conducting diplomatic or industrial espionage, engaged in cybercrime, or intimidating political activists. In

Related Author
+ Rita Tahan

Related Policy Issue
+ Cybersecurity

Contents
+ Legislation
  + CRS Reports and Other CRS Products: Legislation
  + Hearings in the 113th Congress
  + Hearings in the 112th Congress

addition, national borders mean little or nothing to cyberattackers, and attributing an attack to a specific location can be difficult, which may also make a response problematic.

Despite many recommendations made over the past decade, no major legislative provisions relating to cybersecurity have been enacted since 2002. In April 2011, the Obama Administration sent Congress legislative proposals that would have given the federal government new authority to ensure that corporations owning assets most critical to the nation’s security and economic prosperity adequately addressed risks posed by cybersecurity threats. This report provides links to cybersecurity legislation in the 112th and 113th Congresses.

- Major Legislation in the 113th Congress, Table 1 and Table 2
- Major Legislation in the 112th Congress, Table 3 and Table 5
- Senate Floor Debate: S. 3414 (112th Congress), Table 4
- House Floor Debate: H.R. 3523 (112th Congress), Table 6

Congress has held cybersecurity hearings every year since 2001. This report also provides links to cybersecurity-related committee hearings in the 112th and 113th Congresses.

- House Hearings (113th Congress), Table 7 and Table 8
- House Committee Markups (113th Congress), Table 9
- Senate Hearings (112th Congress), Table 10 and Table 12
- Other Hearings (113th Congress), Table 11 and Table 13
- House Hearings (112th Congress), Table 14 and Table 15
- House Markups (112th Congress), Table 16
- Senate Hearings (112th Congress), Table 17 and Table 18
- Congressional Committee Investigative Reports, Table 19

For a discussion of selected legislative proposals in the 112th and 113th Congresses, see CRS Report R42114, Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions, by Eric A. Fischer.

Executive orders authorize the President to manage federal government operations. Presidential directives pertain to all aspects of U.S. national security policy as authorized by the President. This report provides a list of executive orders and presidential directives pertaining to information and computer security.

- Executive Orders and Presidential Directives, Table 20

For a selected list of authoritative reports and resources on cybersecurity, see CRS Report R42507, Cybersecurity: Authoritative Reports and Resources, by Topic, by Rita Tahan. For selected cybersecurity data, statistics, and glossaries, see CRS Report R43310, Cybersecurity: Data, Statistics, and Glossaries, by Rita Tahan.

Cybersecurity: Legislation, Hearings, and Executive Branch Documents

Legislation

No major legislative provisions relating to cybersecurity have been enacted since 2002, despite many recommendations made over the past decade.

In April 2011, the White House sent a comprehensive, seven-part legislative proposal (White House Proposal) to Congress. Some elements of that proposal were included in both House and Senate bills. The House passed a series of bills that addressed a variety of issues—from toughening law enforcement of cybercrimes to giving the Department of Homeland Security oversight of federal information technology and critical infrastructure security to lessening liability for private companies that adopt cybersecurity best practices. The Senate pursued a comprehensive cybersecurity bill (S. 3414) with several committees working to create a single vehicle for passage, backed by the White House, but the bill failed to overcome two cloture votes, and did not pass. Despite the lack of enactment of cybersecurity legislation in the 113th Congress, there still appears to be considerable support in principle for significant legislation to address most of the issues identified above.

Six cybersecurity bills have passed the House in the 113th Congress, similar to those passed in the 112th Congress. Three Senate bills in the 113th Congress have been marked up by committee.

In February 2013, the White House issued an executive order designed to improve the cybersecurity of U.S. critical infrastructure. Executive Order 13636 attempts to enhance the security and resiliency of critical infrastructure through voluntary, collaborative efforts involving federal agencies and owners and operators of privately owned critical infrastructure, as well as the use of existing federal regulatory authorities. Given the absence of comprehensive cybersecurity legislation, some security observers contend that E.O. 13636 is a necessary step in securing vital assets against cyberthreats. Others have expressed the view that the executive order could make enactment of a bill less likely or could lead to government intrusiveness into private-sector activities, through increased regulation under existing statutory authority. For further discussion of the executive order, see CRS Report R42984, The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress, by Eric A. Fischer et al.

Table 1 and Table 2 provide lists of Senate and House legislation under consideration in the 113th Congress, in order by the date introduced.

CRS Reports and Other CRS Products: Legislation

- CRS Legal Sidebar WSLG478, House Intelligence Committee Marks Up Cybersecurity Bill CISPA, by Richard M. Thompson
- CRS Legal Sidebar WSLG480, Privacy and Civil Liberties Issues Raised by CISPA, by Andrew Nolan

Table 1. Legislation: Senate (113th Congress)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Title</th>
<th>Committee(s)</th>
<th>Date Introduced</th>
<th>Latest Major Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hearing held</td>
<td></td>
</tr>
<tr>
<td>S. 1897</td>
<td>Personal Data Privacy and Security Act of 2014</td>
<td>Judiciary</td>
<td>January 8, 2014</td>
<td>No action</td>
<td></td>
</tr>
<tr>
<td>S. 1638</td>
<td>Cybersecurity Public Awareness Act of 2013</td>
<td>Homeland Security and Governmental Affairs</td>
<td>October 31, 2013</td>
<td>No action</td>
<td></td>
</tr>
<tr>
<td>S. 1193</td>
<td>Data Security and Breach Notification Act of 2013</td>
<td>Commerce, Science, and Transportation</td>
<td>June 20, 2013</td>
<td>No action</td>
<td></td>
</tr>
<tr>
<td>S. 1111</td>
<td>Cyber Economic Espionage Accountability Act</td>
<td>Judiciary</td>
<td>June 6, 2013</td>
<td>No action</td>
<td></td>
</tr>
<tr>
<td>S. 884</td>
<td>Data Cyber Theft Act</td>
<td>Finance</td>
<td>May 7, 2013</td>
<td>No action</td>
<td></td>
</tr>
</tbody>
</table>

### Table 2. Legislation: House (113th Congress)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Title</th>
<th>Committee(s)</th>
<th>Date Introduced</th>
<th>Latest Major Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.R. 4505</td>
<td>DOD Cloud Security Act</td>
<td>Armed Services; Oversight and Government Reform</td>
<td>April 28, 2014</td>
<td>Referred to committees</td>
<td>April 28, 2014</td>
</tr>
<tr>
<td>H.R. 4500</td>
<td>To improve the management of cyber and information technology ranges and facilities of the Department of Defense</td>
<td>Armed Services</td>
<td>April 28, 2014</td>
<td>Referred to committee April 28, 2014</td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity: Legislation, Hearings, and Executive Branch Documents

<table>
<thead>
<tr>
<th>Bill</th>
<th>Title</th>
<th>Committee</th>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.R. 624</td>
<td>Cyber Intelligence Sharing and Protection Act (CISPA)</td>
<td>Permanent Select Committee on Intelligence</td>
<td>February 13, 2013</td>
<td>Passed House, Roll no. 117. Referred to Senate Select Committee on Intelligence April 18, 2013</td>
</tr>
<tr>
<td>H.Res. 164</td>
<td>Providing for consideration of the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities</td>
<td>Rules</td>
<td>April 16, 2013</td>
<td>Passed House, Roll no. 109. Motion to reconsider laid on the table Agreed to without objection. April 17, 2013</td>
</tr>
</tbody>
</table>

Source: Legislative Information System (LIS).

Table 3 and Table 5 list major Senate and House legislation considered by the 112th Congress, in order by date introduced. The tables include bills with committee action, floor action, or significant legislative interest. Table 4 provides Congressional Record links to Senate http://www.crs.gov/pages/Reports.aspx?PRODCODE=R43317&Source=author[10/16/2014 3:59:09 PM]
floor debate of S. 3414, the Cybersecurity Act of 2012. Table 6 provides Congressional Record links to House floor debate of H.R. 3523, the Cyber Intelligence Sharing and Protection Act.

Table 3. Major Legislation: Senate (112th Congress)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Title</th>
<th>Committee(s)</th>
<th>Date Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. 3414</td>
<td>Cybersecurity Act of 2012</td>
<td>N/A (Placed on Senate Legislative Calendar under Read the First Time)</td>
<td>July 19, 2012</td>
</tr>
<tr>
<td>S. 3342</td>
<td>SECURE IT</td>
<td>N/A (Placed on Senate Legislative Calendar under General Orders. Calendar No. 438)</td>
<td>June 27, 2012</td>
</tr>
<tr>
<td>S. 2151</td>
<td>SECURE IT</td>
<td>Commerce, Science, and Transportation</td>
<td>March 1, 2012</td>
</tr>
<tr>
<td>S. 1535</td>
<td>Personal Data Protection and Breach Accountability Act of 2011</td>
<td>Judiciary</td>
<td>September 8, 2011</td>
</tr>
<tr>
<td>S. 1342</td>
<td>Grid Cyber Security Act</td>
<td>Energy and Natural Resources</td>
<td>July 11, 2011</td>
</tr>
<tr>
<td>S. 413</td>
<td>Cybersecurity and Internet Freedom Act of 2011</td>
<td>Homeland Security and Governmental Affairs</td>
<td>February 17, 2011</td>
</tr>
</tbody>
</table>

Source: Legislative Information System (LIS).

Table 4. Senate Floor Debate: S. 3414 (112th Congress)

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Congressional Record Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Act of 2012: Motion to Proceed</td>
<td>July 26, 2012</td>
<td>S5419-S5449</td>
</tr>
<tr>
<td>Cybersecurity Act of 2012: Motion to Proceed — Continued and Cloture Vote</td>
<td>July 26, 2012</td>
<td>S5450-S5467</td>
</tr>
<tr>
<td>Cybersecurity Act of 2012</td>
<td>July 31, 2012</td>
<td>S5694-S5705</td>
</tr>
<tr>
<td>Cybersecurity Act of 2012: Continued</td>
<td>July 31, 2012</td>
<td>S5705-S5724</td>
</tr>
<tr>
<td>Cybersecurity Act of 2012: Motion to Proceed</td>
<td>November 14, 2012</td>
<td>S6774-S6784</td>
</tr>
</tbody>
</table>

**Source:** Congressional Record (GPO).

**Table 5. Major Legislation: House (112th Congress)**

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Title</th>
<th>Committee(s)</th>
<th>Date Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.R. 4263</td>
<td>SECURE IT Act of 2012: Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology</td>
<td>Oversight and Government Reform, the Judiciary, Armed Services, and Intelligence (Permanent Select)</td>
<td>March 27, 2012</td>
</tr>
</tbody>
</table>

Cybersecurity: Legislation, Hearings, and Executive Branch Documents

H.R. 3523    Cyber Intelligence Sharing and Protection Act

Committee on Intelligence
(Permanent Select)
November 30, 2011

H.R. 2096    Cybersecurity Enhancement Act of 2012

Science, Space, and Technology
June 2, 2011

H.R. 174    Homeland Security Cyber and Physical Infrastructure Protection Act of 2011

Technology, Education and the Workforce; Homeland Security
January 5, 2011

H.R. 76    Cybersecurity Education Enhancement Act of 2011

Homeland Security; House Oversight and Government Reform
January 5, 2011

Source: Legislative Information System (LIS).

Table 6. House Floor Debate: H.R. 3523 (112th Congress)

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Congressional Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Intelligence Sharing and Protection Act: Providing for Consideration of Motion to Suspend the Rules</td>
<td>April 26, 2012</td>
<td>H2147-2156</td>
</tr>
<tr>
<td>Cyber Intelligence Sharing and Protection Act: Consideration of the Bill</td>
<td>April 26, 2012</td>
<td>H2156-2186</td>
</tr>
</tbody>
</table>

Source: Congressional Record (GPO).

Hearings in the 113th Congress

The following tables list cybersecurity hearings in the 113th Congress. Table 7 and Table 8 contain identical content but are organized differently. Table 7 lists House hearings arranged by date (most recent first), and Table 8 lists House hearings arranged by committee. When viewed in HTML, the document titles are active links to the committee's website for that particular hearing.

Table 7. House Hearings (113th Congress), by Date

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Committee</th>
<th>Subcommittee</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Data Mining Threatens Student Privacy</td>
<td>June 25, 2014</td>
<td>Homeland Security</td>
<td>Cybersecurity, Infrastructure</td>
</tr>
<tr>
<td>Title</td>
<td>Date</td>
<td>Committee</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------</td>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland</td>
<td>May 21, 2014</td>
<td>Homeland Security</td>
<td></td>
</tr>
<tr>
<td>Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime</td>
<td>April 16, 2014</td>
<td>Homeland Security</td>
<td></td>
</tr>
<tr>
<td>International Cybercrime Protection</td>
<td>March 6, 2014</td>
<td>Science, Space and Technology</td>
<td></td>
</tr>
<tr>
<td>Data Security: Examining Efforts to Protect Americans’ Financial Information</td>
<td>March 5, 2014</td>
<td>Financial Services</td>
<td></td>
</tr>
<tr>
<td>Protecting Consumer Information: Can Data Breaches Be Prevented?</td>
<td>February 5, 2014</td>
<td>Energy and Commerce</td>
<td></td>
</tr>
<tr>
<td>Healthcare.gov: Consequences of Stolen Identity</td>
<td>January 19, 2014</td>
<td>Science, Space and Technology</td>
<td></td>
</tr>
<tr>
<td>HHS’ Own Security Concerns About Healthcare.gov</td>
<td>January 16, 2014</td>
<td>Oversight and Government Reform</td>
<td></td>
</tr>
<tr>
<td>Cyber Side-Effects: How Secure is the Personal Information Entered into the</td>
<td>November 13, 2013</td>
<td>Homeland Security</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Committee</th>
<th>Sub话题</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Incident Response: Bridging the Gap Between Cybersecurity and</td>
<td>October 30, 2013</td>
<td>Homeland Security</td>
<td>Cybersecurity, Infrastructure Protection and Security Technologies</td>
</tr>
<tr>
<td>Emergency Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity: 21st Century Threats, Challenges, and Opportunities</td>
<td>October 23, 2013</td>
<td>Permanent Select Committee on Intelligence</td>
<td></td>
</tr>
<tr>
<td>Hub</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia: The Cyber Security Battleground</td>
<td>July 23, 2013</td>
<td>Foreign Affairs</td>
<td>Asia and the Pacific</td>
</tr>
<tr>
<td>Reporting Data Breaches: Is Federal Legislation Needed to Protect</td>
<td>July 18, 2013</td>
<td>Energy and Commerce</td>
<td>Commerce, Manufacturing and Trade</td>
</tr>
<tr>
<td>Consumers?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluating Privacy, Security, and Fraud Concerns with ObamaCare’s</td>
<td>July 17, 2013</td>
<td>(Joint Hearing) Homeland Security and Oversight and Government Reform</td>
<td></td>
</tr>
<tr>
<td>Information Sharing Apparatus</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Espionage and the Theft of U.S. Intellectual Property and</td>
<td>July 9, 2013</td>
<td>Energy and Commerce</td>
<td>Oversight and Investigation</td>
</tr>
<tr>
<td>Technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Threats and Security Solutions</td>
<td>May 21, 2013</td>
<td>Energy and Commerce</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity: An Examination of the Communications Supply Chain</td>
<td>May 21, 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitating Cyber Threat Information Sharing and Partnering with the</td>
<td>May 16, 2013</td>
<td>Homeland Security</td>
<td>Cybersecurity, Infrastructure Protection and Security Technologies</td>
</tr>
<tr>
<td>Private Sector to Protect Critical Infrastructure: An Assessment of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHS Capabilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure from Cyber Attack and Ensuring Privacy and Civil</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liberties</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity: Legislation, Hearings, and Executive Branch Documents

- **Protecting Small Business from Cyber-Attacks**
  - March 21, 2013
  - Small Business
  - Healthcare and Technology

- **Cybersecurity and Critical Infrastructure [CLOSED hearing]**
  - March 20, 2013
  - Appropriations

- **Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure**
  - March 20, 2013
  - Homeland Security
  - Cybersecurity, Infrastructure Protection and Security Technologies

- **DHS Cybersecurity: Roles and Responsibilities to Protect the Nation’s Critical Infrastructure**
  - March 13, 2013
  - Homeland Security

- **Investigating and Prosecuting 21st Century Cyber Threats**
  - March 13, 2013
  - Judiciary
  - Crime, Terrorism, Homeland Security and Investigations

- **Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force**
  - March 13, 2013
  - Armed Services
  - Intelligence, Emerging Threats and Capabilities

- **Cyber R&D [Research and Development] Challenges and Solutions**
  - February 26, 2013
  - Science, Space, and Technology

- **Advanced Cyber Threats Facing Our Nation**
  - February 14, 2013
  - Select Committee on Intelligence

*Source:* Compiled by the Congressional Research Service (CRS).

### Table 8. House Hearings (113th Congress), by Committee

<table>
<thead>
<tr>
<th>Committee</th>
<th>Subcommittee</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Committee</th>
<th>Topic</th>
<th>Event Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Breaches Be Prevented?</td>
<td></td>
</tr>
<tr>
<td>Energy and Commerce</td>
<td>Commerce, Manufacturing and Trade Reporting Data Breaches: Is Federal</td>
<td>July 18, 2013</td>
</tr>
<tr>
<td></td>
<td>Legislation Needed to Protect Consumers?</td>
<td></td>
</tr>
<tr>
<td>Energy and Commerce</td>
<td>Oversight and Investigation Cyber Espionage and the Theft of U.S.</td>
<td>July 9, 2013</td>
</tr>
<tr>
<td></td>
<td>Intellectual Property and Technology</td>
<td></td>
</tr>
<tr>
<td>Energy and Commerce</td>
<td>Cyber Threats and Security Solutions</td>
<td>May 21, 2013</td>
</tr>
<tr>
<td>Financial Services</td>
<td>Financial Institutions and Consumer Credit Data Security: Examining</td>
<td>March 5, 2014</td>
</tr>
<tr>
<td></td>
<td>Efforts to Protect Americans' Financial Information</td>
<td></td>
</tr>
<tr>
<td>Foreign Affairs</td>
<td>Asia and the Pacific Asia: The Cyber Security Battleground</td>
<td>July 23, 2013</td>
</tr>
<tr>
<td>Foreign Affairs</td>
<td>Europe, Eurasia, and Emerging Threats Cyber Attacks: An Unprecedented</td>
<td>March 21, 2013</td>
</tr>
<tr>
<td></td>
<td>to U.S. National Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How Data Mining Threatens Student Privacy</td>
<td></td>
</tr>
<tr>
<td>Homeland Security</td>
<td>Counterterrorism and Intelligence Assessing Persistent and Emerging</td>
<td>May 21, 2014</td>
</tr>
<tr>
<td></td>
<td>Cyber Threats to the U.S. Homeland</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Electromagnetic Pulse (EMP): Threat to Critical Infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protecting Your Personal Data: How Law Enforcement Works With the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Private Sector to Prevent Cybercrime</td>
<td></td>
</tr>
<tr>
<td>Homeland Security</td>
<td>Cyber Side-Effects: How Secure is the Personal Information Entered</td>
<td>November 13, 2013</td>
</tr>
<tr>
<td></td>
<td>into the Flawed Healthcare.gov?</td>
<td></td>
</tr>
<tr>
<td>Homeland Security</td>
<td>Cyber Incident Response: Bridging the Gap Between Cybersecurity and</td>
<td>October 30, 2013</td>
</tr>
<tr>
<td></td>
<td>Emergency Management</td>
<td></td>
</tr>
<tr>
<td>Committee</td>
<td>Title</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Homeland Security (Joint</td>
<td>Cybersecurity, Infrastructure Protection and Security Technologies</td>
<td>May 16, 2013</td>
</tr>
<tr>
<td>Hearing with Oversight and</td>
<td>Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities</td>
<td></td>
</tr>
<tr>
<td>Government Reform)</td>
<td>Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties</td>
<td>April 25, 2013</td>
</tr>
<tr>
<td>Reform</td>
<td>HHS' Own Security Concerns About HealthCare.gov</td>
<td>January 16, 2014</td>
</tr>
<tr>
<td>Reform (Joint Hearing with</td>
<td>International Cybercrime Protection</td>
<td>March 6, 2014</td>
</tr>
<tr>
<td>Homeland Security)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 9. House Committee Markups (113th Congress), by Date

<table>
<thead>
<tr>
<th>Committee</th>
<th>Subcommittee</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
</table>

Source: Compiled by CRS.

Table 10. Senate Hearings (113th Congress), by Date

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Committee</th>
<th>Subcommittee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks</td>
<td>July 15, 2014</td>
<td>Judiciary</td>
<td>Crime and Terrorism</td>
</tr>
<tr>
<td>Data Breach on the Rise: Protecting Personal</td>
<td>April 2, 2014</td>
<td>Homeland Security and</td>
<td></td>
</tr>
<tr>
<td>Event Description</td>
<td>Date</td>
<td>Committee</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Protecting Personal Consumer Information from Cyber Attacks and Data Breaches</td>
<td>March 26, 2014</td>
<td>Commerce, Science &amp; Transportation</td>
<td></td>
</tr>
<tr>
<td>Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's</td>
<td>March 26, 2014</td>
<td>Homeland Security and Governmental Affairs</td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nomination of Vice Admiral Michael S. Rogers, USN to be admiral and Director,</td>
<td>March 11, 2014</td>
<td>Armed Services</td>
<td></td>
</tr>
<tr>
<td>National SecurityAgency/Chief, Central Security Services/Commander, U.S. Cyber</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.S. Strategic Command and U.S. Cyber Command in review of the fiscal 2015 Defense</td>
<td>February 27, 2014</td>
<td>Armed Services</td>
<td></td>
</tr>
<tr>
<td>Authorization Request and the Future Years Defense Program</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversight of Financial Stability and Data Security</td>
<td>February 6, 2014</td>
<td>Banking, Housing and Urban Affairs</td>
<td></td>
</tr>
<tr>
<td>Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime</td>
<td>February 4, 2014</td>
<td>Judiciary</td>
<td></td>
</tr>
<tr>
<td>Safeguarding Consumers' Financial Data, Panel 2</td>
<td>February 3, 2014</td>
<td>Banking, Housing, and Urban Affairs</td>
<td></td>
</tr>
<tr>
<td>National Security and International Trade and Finance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Partnership Between NIST (National Institute of Standards and Technology) and</td>
<td>July 25, 2013</td>
<td>Commerce, Science and Transportation</td>
<td></td>
</tr>
<tr>
<td>the Private Sector: Improving Cybersecurity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resilient Military Systems and the Advanced Cyber Threat (CLOSED BRIEFING)</td>
<td>June 26, 2013</td>
<td>Armed Services</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity: Preparing for and Responding to the Enduring Threat</td>
<td>June 12, 2013</td>
<td>Appropriations</td>
<td></td>
</tr>
<tr>
<td>Cyber Threats: Law Enforcement and Private Sector Responses</td>
<td>May 8, 2013</td>
<td>Judiciary</td>
<td></td>
</tr>
<tr>
<td>Defense Authorization: Cybersecurity Threats: To receive a briefing on cybersecurity</td>
<td>March 19, 2013</td>
<td>Armed Services</td>
<td></td>
</tr>
<tr>
<td>threats in review of the Defense Authorization Request for</td>
<td></td>
<td>Emerging Threats and Capabilities</td>
<td></td>
</tr>
</tbody>
</table>

Cybersecurity: Legislation, Hearings, and Executive Branch Documents
Fiscal Year 2014 and the Future Years Defense Program

Table 11. Other Hearings (113th Congress), by Date

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Committee</th>
<th>Subcommittee</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.-China Cybersecurity Issues</td>
<td>July 11, 2013</td>
<td>Congressional-Executive Commission on China</td>
<td></td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.

Table 12. Senate Hearings (113th Congress), by Committee

<table>
<thead>
<tr>
<th>Committee</th>
<th>Subcommittee</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriations</td>
<td></td>
<td>Cybersecurity: Preparing for and Responding to the Enduring Threat</td>
<td>June 12, 2013</td>
</tr>
<tr>
<td>Armed Services</td>
<td></td>
<td>Nomination of Vice Admiral Michael S. Rogers, USN to be admiral and Director, National Security Agency/Chief, Central Security Services/Commander, U.S. Cyber Command</td>
<td>March 11, 2014</td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.
<table>
<thead>
<tr>
<th>Committee/Matter</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking, Housing, and Urban Affairs</td>
<td>Oversight of Financial Stability and Data Security</td>
<td>February 6, 2014</td>
</tr>
<tr>
<td>Commerce, Science &amp; Transportation</td>
<td>Protecting Personal Consumer Information from Cyber Attacks and Data Breaches</td>
<td>March 26, 2014</td>
</tr>
<tr>
<td>Homeland Security and Governmental Affairs</td>
<td>Data Breach on the Rise: Protecting Personal Information from Harm</td>
<td>April 2, 2014</td>
</tr>
<tr>
<td>Homeland Security and Governmental Affairs</td>
<td>Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure</td>
<td>March 26, 2014</td>
</tr>
<tr>
<td>Judiciary</td>
<td>Crime and Terrorism</td>
<td>July 15, 2014</td>
</tr>
<tr>
<td>Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Judiciary</td>
<td>Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime</td>
<td>February 4, 2014</td>
</tr>
<tr>
<td>Judiciary</td>
<td>Cyber Threats: Law Enforcement and Private</td>
<td>May 8, 2013</td>
</tr>
</tbody>
</table>

Table 13. Other Hearings (113th Congress), by Committee

<table>
<thead>
<tr>
<th>Committee</th>
<th>Subcommittee</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>on China</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>on China</td>
<td></td>
<td>Commercial Rule of Law</td>
<td></td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.

Hearings in the 112th Congress

The following tables list cybersecurity hearings in the 112th Congress. Table 14 and Table 15 contain identical content but are organized differently. Table 14 lists House hearings arranged by date (most recent first) and Table 15 lists House hearings arranged by committee. Table 16 lists House markups by date; Table 17 and Table 18 contain identical content. Table 17 lists Senate hearings arranged by date and Table 18 lists Senate hearings arranged by committee. Table 19 lists two congressional committee investigative reports: the House Permanent Select Committee on Intelligence investigative report into the counterintelligence and security threats posed by Chinese telecommunications companies doing business in the United States, and the Senate Permanent Subcommittee on Investigations’ review of U.S. Department of Homeland Security efforts to engage state and local intelligence “fusion centers.” When viewed in HTML, the document titles are active links to the committee’s website for that particular hearing.

Table 14. House Hearings (112th Congress), by Date

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Committee</th>
<th>Subcommittee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE</td>
<td>September 13, 2012</td>
<td>Permanent Select Committee on Intelligence</td>
<td>Emergency Preparedness, Response, and Communications</td>
</tr>
<tr>
<td>Resilient Communications: Current Challenges and Future Advancements</td>
<td>September 12, 2012</td>
<td>Homeland Security</td>
<td></td>
</tr>
<tr>
<td>Digital Warriors: Improving Military</td>
<td>July 25, 2012</td>
<td>Armed Services</td>
<td>Emerging Threats and Capabilities</td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.

Source: Compiled by CRS.
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Date</th>
<th>Committee</th>
<th>Subcommittee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Threats to Capital Markets and Corporate Accounts</td>
<td>June 1, 2012</td>
<td>Financial Services</td>
<td>Capital Markets and Government Sponsored Enterprises</td>
</tr>
<tr>
<td>Iranian Cyber Threat to U.S. Homeland</td>
<td>April 26, 2012</td>
<td>Homeland Security</td>
<td>Cybersecurity, Infrastructure Protection and Security Technologies and Counterterrorism and Intelligence</td>
</tr>
<tr>
<td>Cybersecurity: Threats to Communications Networks and Public-Sector Responses</td>
<td>March 28, 2012</td>
<td>Energy and Commerce</td>
<td>Communications and Technology</td>
</tr>
<tr>
<td>Fiscal Year 2013 Budget Request for Information Technology and Cyber Operations Programs</td>
<td>March 20, 2012</td>
<td>Armed Services</td>
<td>Emerging Threats and Capabilities</td>
</tr>
<tr>
<td>Cybersecurity: The Pivotal Role of Communications Networks</td>
<td>March 7, 2012</td>
<td>Energy and Commerce</td>
<td>Communications and Technology</td>
</tr>
<tr>
<td>NASA Cybersecurity: An Examination of the Agency’s Information Security</td>
<td>February 29, 2012</td>
<td>Science, Space, and Technology</td>
<td>Investigations and Oversight</td>
</tr>
<tr>
<td>Combating Online Piracy (H.R. 3261, Stop</td>
<td>November 16, 2011</td>
<td>Judiciary</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Date</td>
<td>Committee</td>
<td>Committee Title</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Institutionalizing Irregular Warfare Capabilities</td>
<td>November 3, 2011</td>
<td>Armed Services</td>
<td>Emerging Threats and Capabilities</td>
</tr>
<tr>
<td>Cyber Threats and Ongoing Efforts to Protect the Nation</td>
<td>October 4, 2011</td>
<td>Permanent Select Intelligence</td>
<td></td>
</tr>
<tr>
<td>The Cloud Computing Outlook</td>
<td>September 21, 2011</td>
<td>Science, Space, and Technology</td>
<td>Technology and Innovation</td>
</tr>
<tr>
<td>Cybersecurity: Threats to the Financial Sector</td>
<td>September 14, 2011</td>
<td>Financial Services</td>
<td>Financial Institutions and Consumer Credit</td>
</tr>
<tr>
<td>Cybersecurity: An Overview of Risks to Critical Infrastructure</td>
<td>July 26, 2011</td>
<td>Energy and Commerce</td>
<td>Oversight and Investigations</td>
</tr>
<tr>
<td>Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat</td>
<td>July 7, 2011</td>
<td>Oversight and Government Reform</td>
<td></td>
</tr>
<tr>
<td>Field Hearing: &quot;Hacked Off: Helping Law Enforcement Protect Private Financial Information&quot;</td>
<td>June 29, 2011</td>
<td>Financial Services (field hearing in Hoover, AL)</td>
<td></td>
</tr>
<tr>
<td>Event Description</td>
<td>Date</td>
<td>Committee</td>
<td>Sub-Committee</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Protecting Information in the Digital Age: Federal Cybersecurity Research and</td>
<td>May 25, 2011</td>
<td>Science, Space and Technology</td>
<td>Research and Science Education and Technology</td>
</tr>
<tr>
<td>Development Efforts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology</td>
<td>April 15, 2011</td>
<td>Foreign Affairs</td>
<td>Oversight and Investigations</td>
</tr>
<tr>
<td>Budget Hearing—National Protection and Programs Directorate, Cybersecurity and</td>
<td>March 31, 2011</td>
<td>Appropriations</td>
<td>Energy and Power</td>
</tr>
<tr>
<td>Infrastructure Protection Programs</td>
<td></td>
<td>(closed/classified)</td>
<td></td>
</tr>
<tr>
<td>2012 Budget Request from U.S. Cyber Command</td>
<td>March 16, 2011</td>
<td>Armed Services</td>
<td>Emerging Threats and Capabilities</td>
</tr>
<tr>
<td>What Should the Department of Defense’s Role in Cyber Be?</td>
<td>February 11, 2011</td>
<td>Armed Services</td>
<td>Emerging Threats and Capabilities</td>
</tr>
<tr>
<td>Preventing Chemical Terrorism: Building a Foundation of Security at Our Nation’s</td>
<td>February 11, 2011</td>
<td>Homeland Security</td>
<td>Cybersecurity, Infrastructure Protection and Security Technologies</td>
</tr>
<tr>
<td>Chemical Facilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Worldwide Threats</td>
<td>February 10, 2011</td>
<td>Permanent Select Intelligence</td>
<td></td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.
<table>
<thead>
<tr>
<th>Committee (closed/classified)</th>
<th>Subcommittee</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriations</td>
<td>Budget Hearing—National Protection and Programs Directorate, Cybersecurity and Infrastructure Protection Programs</td>
<td>March 31, 2011</td>
<td></td>
</tr>
<tr>
<td>Armed Services</td>
<td>Institutionalizing Irregular Warfare Capabilities</td>
<td>November 3, 2011</td>
<td></td>
</tr>
<tr>
<td>Armed Services</td>
<td>2012 Budget Request for U.S. Cyber Command</td>
<td>March 16, 2011</td>
<td></td>
</tr>
<tr>
<td>Armed Services</td>
<td>What Should the Department of Defense’s Role in Cyber Do?</td>
<td>February 11, 2011</td>
<td></td>
</tr>
<tr>
<td>Energy and Commerce</td>
<td>Cybersecurity: Threats to Communications Networks and Public-Sector Responses</td>
<td>March 28, 2012</td>
<td></td>
</tr>
<tr>
<td>Energy and Commerce</td>
<td>Cybersecurity: The Pivotal Role of Communications Networks</td>
<td>March 7, 2012</td>
<td></td>
</tr>
<tr>
<td>Financial Services</td>
<td>Cyber Threats to Capital Markets and Corporate Account</td>
<td>June 1, 2012</td>
<td></td>
</tr>
<tr>
<td>Financial Services</td>
<td>Cybersecurity: Threats to the Financial Sector</td>
<td>September 14, 2011</td>
<td></td>
</tr>
<tr>
<td>Financial Services</td>
<td>Field Hearing: “Hacked Off: Helping Law Enforcement Protect</td>
<td>June 29, 2011</td>
<td></td>
</tr>
<tr>
<td>Financial Services</td>
<td>“Hacked Off: Helping Law Enforcement Protect</td>
<td>June 29, 2011</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Agency</th>
<th>Subcommittee</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreign Affairs</td>
<td>Oversight and Investigations</td>
<td>Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology April 15, 2011</td>
</tr>
</tbody>
</table>
Cybersecurity: Legislation, Hearings, and Executive Branch Documents

<table>
<thead>
<tr>
<th>Judiciary</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight and Government Reform</td>
<td>Cybersecurity: Assessing the Nation’s Ability to Address the Growing Cyber Threat</td>
<td>July 7, 2011</td>
</tr>
<tr>
<td>Permanent Select Intelligence</td>
<td>Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE</td>
<td>September 13, 2012</td>
</tr>
<tr>
<td>Permanent Select Intelligence</td>
<td>Cyber Threats and Ongoing Efforts to Protect the Nation</td>
<td>October 4, 2011</td>
</tr>
<tr>
<td>World Wide Threats</td>
<td></td>
<td>February 10, 2011</td>
</tr>
<tr>
<td>NASA Cybersecurity: An Examination of the Agency’s Information Security</td>
<td></td>
<td>February 29, 2012</td>
</tr>
<tr>
<td>The Cloud Computing Outlook</td>
<td></td>
<td>September 21, 2011</td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.

Table 16. House Markups (112th Congress), by Date

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Committee</th>
<th>Subcommittee</th>
</tr>
</thead>
</table>

### Table 17. Senate Hearings (112th Congress), by Date

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Committee</th>
<th>Subcommittee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security and the Grid</td>
<td>July 17, 2012</td>
<td>Energy and Natural Resources Committee</td>
<td></td>
</tr>
<tr>
<td>U.S. Strategic Command and U.S. Cyber Command</td>
<td>March 27, 2012</td>
<td>Armed Services</td>
<td>Emerging Threats and Capabilities</td>
</tr>
<tr>
<td>Cybersecurity Research and Development</td>
<td>March 20, 2012</td>
<td>Armed Services</td>
<td></td>
</tr>
<tr>
<td>The Freedom of Information Act: Safeguarding Critical Infrastructure Information and the Public's Right to Know</td>
<td>March 13, 2012</td>
<td>Judiciary</td>
<td></td>
</tr>
<tr>
<td>Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats</td>
<td>September 7, 2011</td>
<td>Judiciary</td>
<td></td>
</tr>
<tr>
<td>Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States</td>
<td>July 25, 2011</td>
<td>Small Business and Entrepreneurship</td>
<td></td>
</tr>
<tr>
<td>Privacy and Data Security: Protecting Consumers in the Modern</td>
<td>June 29, 2011</td>
<td>Commerce, Science and</td>
<td></td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.

Cybersecurity: Legislation, Hearings, and Executive Branch Documents

<table>
<thead>
<tr>
<th>World</th>
<th>June 21, 2011</th>
<th>Transportation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity: Evaluating the Administration's Proposals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity and Data Protection in the Financial Sector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protecting Cyberspace: Assessing the White House Proposal</td>
<td>May 23, 2011</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity of the Bulk-Power System and Electric Infrastructure</td>
<td>May 5, 2011</td>
<td>Energy and Natural Resources</td>
</tr>
<tr>
<td>and for Other Purposes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health and Status of the Defense Industrial Base</td>
<td>May 3, 2011</td>
<td>Armed Services</td>
</tr>
<tr>
<td>Cyber Security: Responding to the Threat of Cyber Crime and Terrorism</td>
<td>April 12, 2011</td>
<td></td>
</tr>
<tr>
<td>Oversight of the Federal Bureau of Investigation</td>
<td>March 30, 2011</td>
<td>Judiciary</td>
</tr>
<tr>
<td>Cybersecurity and Critical Electric Infrastructure® (closed hearing)</td>
<td>March 15, 2011</td>
<td>Energy and Natural Resources</td>
</tr>
<tr>
<td>Collaboration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Homeland Security Department's Budget Submission for Fiscal Year 2012</td>
<td>February 17, 2011</td>
<td>Homeland Security and Governmental Affairs</td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.

a. The March 15, 2011, hearing before the Committee on Energy and Natural Resources was closed.

Table 18. Senate Hearings (112th Congress), by Committee

<table>
<thead>
<tr>
<th>Committee</th>
<th>Subcommittee</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armed Services</td>
<td>Emerging Threats and Capabilities</td>
<td>Cybersecurity Research and Development</td>
<td>March 20, 2012</td>
</tr>
<tr>
<td>Armed Services</td>
<td>U.S. Strategic Command and U.S. Cyber Command</td>
<td></td>
<td>March 27, 2012</td>
</tr>
<tr>
<td>Banking, Housing and Urban Affairs</td>
<td></td>
<td>Cybersecurity and Data Protection in the Financial Sector</td>
<td>June 21, 2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Committee</th>
<th>Subject</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy and Natural Resources</td>
<td>Cybersecurity and the Grid</td>
<td>July 17, 2012</td>
</tr>
<tr>
<td>Energy and Natural Resources</td>
<td>Cybersecurity of the Bulk-Power System and Electric Infrastructure and For Other Purposes</td>
<td>May 5, 2011</td>
</tr>
<tr>
<td>Energy and Natural Resources (closed)</td>
<td>Cybersecurity and Critical Electric Infrastructure</td>
<td>March 15, 2011</td>
</tr>
<tr>
<td>Homeland Security &amp; Governmental Affairs</td>
<td>Oversight of Government Management, the Federal Workforce and the District of Columbia</td>
<td></td>
</tr>
<tr>
<td>Homeland Security and Governmental Affairs</td>
<td>Protecting Cyberspace: Assessing the White House Proposal</td>
<td>May 23, 2011</td>
</tr>
<tr>
<td>Homeland Security and Governmental Affairs</td>
<td>Homeland Security Department's Budget Submission for Fiscal Year 2012</td>
<td>February 17, 2011</td>
</tr>
<tr>
<td>Judiciary</td>
<td>Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats</td>
<td>September 7, 2011</td>
</tr>
<tr>
<td>Judiciary</td>
<td>Cybersecurity: Evaluating the Administration's Proposals</td>
<td>June 21, 2011</td>
</tr>
<tr>
<td>Judiciary</td>
<td>Cyber Security: Responding to the Threat of Cyber Crime and Terrorism</td>
<td>April 12, 2011</td>
</tr>
<tr>
<td>Judiciary</td>
<td>Oversight of the Federal Bureau of Investigation</td>
<td>March 30, 2011</td>
</tr>
<tr>
<td>Small Business and Entrepreneurship</td>
<td>Role of Small Business in Strengthening Cybersecurity Efforts in the United States</td>
<td>July 25, 2011</td>
</tr>
</tbody>
</table>

The March 15, 2011, hearing before the Committee on Energy and Natural Resources was closed.

Table 19. Congressional Committee Investigative Reports

<table>
<thead>
<tr>
<th>Title</th>
<th>Committee</th>
<th>Date</th>
<th>Pages</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Report on the U.S. National Security Issues Posed by</td>
<td>House Permanent Select Committee on</td>
<td>October 8,</td>
<td>60</td>
<td>The committee initiated this investigation in November 2011 to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States.</td>
</tr>
<tr>
<td>Chinese Telecommunications Companies Huawei and ZTE</td>
<td>Intelligence</td>
<td>2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal Support for and Involvement in State and Local Fusion Centers</td>
<td>U. S. Senate Permanent Subcommittee</td>
<td>October 3,</td>
<td>141</td>
<td>A two-year bipartisan investigation found that U.S. Department of Homeland Security efforts to engage state and local intelligence &quot;fusion centers&quot; has not yielded significant useful information to support federal counterterrorism intelligence efforts. In Section VI. &quot;Fusion Centers Have Been Unable to Meaningfully Contribute to Federal Counterterrorism Efforts,&quot; Part G. &quot;Fusion Centers May Have Hindered, Not Aided, Federal Counterterrorism Efforts,&quot; the report discusses the Russian &quot;Cyberattack&quot; in Illinois.</td>
</tr>
<tr>
<td></td>
<td>on Investigations</td>
<td>2012</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Compiled by CRS.

Executive Orders and Presidential Directives

Executive orders are official documents through which the President of the United States manages the operations of the federal government. Presidential directives guide the federal rulemaking policy and are signed or authorized by the President.

The following reports provide additional information on executive orders and presidential directives:

- CRS Report RS20846, Executive Orders: Issuance, Modification, and Revocation, by Vivian S. Chu and Todd Garvey, and
- CRS Report 98-611, Presidential Directives: Background and Overview, by Elaine Halchin.

Table 20 provides a list of executive orders and presidential directives pertaining to cybersecurity. (Titles are linked to documents.) For additional information on E.O. 13636 (Improving Critical Infrastructure Cybersecurity), see CRS Report R42984, The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress, by Eric A. Fischer et al.

### Table 20. Executive Orders and Presidential Directives
(by date of issuance)

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Source</th>
<th>Notes</th>
</tr>
</thead>
</table>
| E.O. 13636, Improving Critical Infrastructure Cybersecurity | February 12, 2013 | White House | E.O. 13636 addresses cybersecurity threats to critical infrastructure (CI) by, among other things,  
- expanding to other CI sectors an existing Department of Homeland Security program for information sharing and collaboration between the government and the private sector;  
- establishing a broadly consultative process for identifying CI with especially high priority for protection;  
- requiring the National Institute of Standards and Technology to lead in developing a Cybersecurity Framework of standards and best practices for protecting CI; and  
- requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks. |
<p>| Presidential Policy Directive (PPD) 21 - Critical Infrastructure Security and Resilience | February 12, 2013 | White House | This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (hereinafter referred to as &quot;critical infrastructure owners and operators&quot;). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the federal government, as well as enhances overall coordination and collaboration. The federal government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the |</p>
<table>
<thead>
<tr>
<th>Executive Order</th>
<th>Date</th>
<th>Issuing Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible</td>
<td>October 7, 2011</td>
<td>White House</td>
</tr>
<tr>
<td>E.O. 13407, Public Alert and Warning System</td>
<td>June 28, 2006</td>
<td>White House</td>
</tr>
<tr>
<td>E.O. 13286, Amendment of Executive Orders,</td>
<td>February 28,</td>
<td>White House</td>
</tr>
</tbody>
</table>

continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the federal government), and all classified information on those networks.

Assigns the Secretary of Homeland Security the responsibility to establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system to enable interoperability and the secure delivery of coordinated messages to the American people through as many communication pathways as practicable, taking account of Federal Communications Commission rules as provided by law.

Assigns the Secretary of Homeland Security the responsibility of coordinating the nation’s overall efforts in critical infrastructure protection across all sectors. HSPD-7 also designates the Department of Homeland Security (DHS) as lead agency for the nation’s information and telecommunications sectors.

Designates the Secretary of Homeland Security the...
Cybersecurity: Legislation, Hearings, and Executive Branch Documents

Transfer of Certain Functions to the Secretary of Homeland Security

Presidential Decision Directive/NSC-63
May 22, 1998
White House

July 5, 1990
White House

April 3, 1984
National Communications System (NCS)

Executive Agent of the National Communication System Committee of Principals, which are the agencies, designated by the President, that own or lease telecommunication assets identified as part of the National Communication System, or which bear policy, regulatory, or enforcement responsibilities of importance to national security and emergency preparedness telecommunications.

Sets as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber) by the year 2003. According to the PDD, any interruptions in the ability of these infrastructures to provide their goods and services must be "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."

Establishes the National Security Telecommunications and Information Systems Security Committee, now called the Committee on National Security Systems (CNSS). CNSS is an interagency committee, chaired by the Department of Defense. Among other assignments, NSD-42 directs the CNSS to provide system security guidance for national security systems to executive departments and agencies; and submit annually to the Executive Agent an evaluation of the security status of national security systems. NSD-42 also directs the Committee to interact, as necessary, with the National Communications System Committee of Principals.

Established a national communication system as those telecommunication assets owned or leased by the federal government that can meet the national security and emergency preparedness needs of the federal government, together with an administrative structure that could ensure that a

Cybersecurity: Legislation, Hearings, and Executive Branch Documents

**Note:** Descriptions compiled by CRS from government websites.

**Key CRS Policy Staff**

The following table provides names and contact information for CRS experts on policy issues related to cybersecurity bills currently being debated in the 113th Congress.

<table>
<thead>
<tr>
<th>Legislative Issues</th>
<th>Name/Title</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislation in the 113th Congress</td>
<td>Eric A. Fischer</td>
<td>7-7071</td>
<td><a href="mailto:efischer@crs.loc.gov">efischer@crs.loc.gov</a></td>
</tr>
<tr>
<td>Critical infrastructure protection</td>
<td>John D. Moteff</td>
<td>7-1435</td>
<td><a href="mailto:jmoteff@crs.loc.gov">jmoteff@crs.loc.gov</a></td>
</tr>
<tr>
<td>Chemical industry</td>
<td>Dana Shea</td>
<td>7-6844</td>
<td><a href="mailto:dshea@crs.loc.gov">dshea@crs.loc.gov</a></td>
</tr>
<tr>
<td>Defense industrial base</td>
<td>Catherine A. Theohary</td>
<td>7-0844</td>
<td><a href="mailto:ctheohary@crs.loc.gov">ctheohary@crs.loc.gov</a></td>
</tr>
<tr>
<td>Electricity grid</td>
<td>Richard J. Campbell</td>
<td>7-7905</td>
<td><a href="mailto:rcampbell@crs.loc.gov">rcampbell@crs.loc.gov</a></td>
</tr>
<tr>
<td>Financial institutions</td>
<td>N. Eric Weiss</td>
<td>7-6209</td>
<td><a href="mailto:eweiss@crs.loc.gov">eweiss@crs.loc.gov</a></td>
</tr>
<tr>
<td>Industrial control systems</td>
<td>Dana Shea</td>
<td>7-6844</td>
<td><a href="mailto:dshea@crs.loc.gov">dshea@crs.loc.gov</a></td>
</tr>
<tr>
<td><strong>Cybercrime</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal laws</td>
<td>Charles Doyle</td>
<td>7-6968</td>
<td><a href="mailto:cdoyle@crs.loc.gov">cdoyle@crs.loc.gov</a></td>
</tr>
<tr>
<td>Law enforcement</td>
<td>Kristin M. Finklea</td>
<td>7-6259</td>
<td><a href="mailto:kfkinklea@crs.loc.gov">kfkinklea@crs.loc.gov</a></td>
</tr>
<tr>
<td><strong>Cybersecurity workforce</strong></td>
<td>Wendy Ginsberg</td>
<td>7-3933</td>
<td><a href="mailto:wginsberg@crs.loc.gov">wginsberg@crs.loc.gov</a></td>
</tr>
<tr>
<td><strong>Cyberterrorism</strong></td>
<td>Catherine A. Theohary</td>
<td>7-0844</td>
<td><a href="mailto:ctheohary@crs.loc.gov">ctheohary@crs.loc.gov</a></td>
</tr>
<tr>
<td><strong>Cyberwar</strong></td>
<td>Catherine A. Theohary</td>
<td>7-0844</td>
<td><a href="mailto:ctheohary@crs.loc.gov">ctheohary@crs.loc.gov</a></td>
</tr>
<tr>
<td>Data breach notification</td>
<td>Gina Stevens</td>
<td>7-2581</td>
<td><a href="mailto:gestevens@crs.loc.gov">gestevens@crs.loc.gov</a></td>
</tr>
<tr>
<td>Economic issues</td>
<td>N. Eric Weiss</td>
<td>7-6209</td>
<td><a href="mailto:eweiss@crs.loc.gov">eweiss@crs.loc.gov</a></td>
</tr>
<tr>
<td><strong>Espionage</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced persistent threat</td>
<td>Catherine A. Theohary</td>
<td>7-0844</td>
<td><a href="mailto:ctheohary@crs.loc.gov">ctheohary@crs.loc.gov</a></td>
</tr>
<tr>
<td>Economic and industrial</td>
<td>Kristin M. Finklea</td>
<td>7-6259</td>
<td><a href="mailto:kfkinklea@crs.loc.gov">kfkinklea@crs.loc.gov</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity: Legislation, Hearings, and Executive Branch Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal issues</strong></td>
</tr>
<tr>
<td><strong>State-sponsored</strong></td>
</tr>
<tr>
<td><strong>Federal agency roles</strong></td>
</tr>
<tr>
<td><strong>Chief Information Officers (CIOs)</strong></td>
</tr>
<tr>
<td><strong>Commerce</strong></td>
</tr>
<tr>
<td><strong>Defense (DOD)</strong></td>
</tr>
<tr>
<td><strong>Executive Office of the President (EOP)</strong></td>
</tr>
<tr>
<td><strong>Homeland Security (DHS)</strong></td>
</tr>
<tr>
<td><strong>Intelligence Community (IC)</strong></td>
</tr>
<tr>
<td><strong>Justice (DOJ)</strong></td>
</tr>
<tr>
<td><strong>National Security Agency (NSA)</strong></td>
</tr>
<tr>
<td><strong>Science agencies (NIST, NSF, OSTP)</strong></td>
</tr>
<tr>
<td><strong>Treasury and financial agencies</strong></td>
</tr>
<tr>
<td><strong>Federal Information Security Management Act (FISMA)</strong></td>
</tr>
<tr>
<td><strong>Federal Internet monitoring</strong></td>
</tr>
<tr>
<td><strong>Hacktivism</strong></td>
</tr>
<tr>
<td><strong>Information sharing</strong></td>
</tr>
<tr>
<td><strong>Antitrust laws</strong></td>
</tr>
<tr>
<td><strong>Civil liability</strong></td>
</tr>
<tr>
<td><strong>Classified information</strong></td>
</tr>
<tr>
<td><strong>Freedom of Information Act (FOIA)</strong></td>
</tr>
<tr>
<td><strong>Privacy and civil liberties</strong></td>
</tr>
</tbody>
</table>

Cybersecurity: Legislation, Hearings, and Executive Branch Documents

Defense and diplomatic
Catherine A. Theohary
7-0844
ctheohary@crs.loc.gov

Law enforcement
Kristin M. Finklea
7-6259
kfinklea@crs.loc.gov

National strategy and policy
Eric A. Fischer
7-7071
efischer@crs.loc.gov

National security
John Rollins
7-5529
jrollins@crs.loc.gov

Public/private partnerships
Eric A. Fischer
7-7071
efischer@crs.loc.gov

Supply chain
Eric A. Fischer
7-7071
efischer@crs.loc.gov

Technological issues
Eric A. Fischer
7-7071
efischer@crs.loc.gov

Botnets
Eric A. Fischer
7-7071
efischer@crs.loc.gov

Cloud computing
Patricia Maloney Figliola
7-2508
pfigliola@crs.loc.gov

Mobile devices
Patricia Maloney Figliola
7-2508
pfigliola@crs.loc.gov

Research and development (R&D)
Patricia Maloney Figliola
7-2508
pfigliola@crs.loc.gov

Footnotes


FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity
Title 3—

The President

Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation’s critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the “Secretary”), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of
Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency’s activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National
Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").
(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification
of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) “Agency” means any authority of the United States that is an “agency” under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) “Critical Infrastructure Partnership Advisory Council” means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) “Fair Information Practice Principles” means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) “Independent regulatory agency” has the meaning given the term in 44 U.S.C. 3502(5).

(e) “Sector Coordinating Council” means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) “Sector-Specific Agency” has the meaning given the term in Presidential Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater
extent than the authority the agency has under existing law. Nothing in
this order shall be construed to alter or limit any authority or responsibility
of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect
the functions of the Director of OMB relating to budgetary, administrative,
or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with require-
ments and authorities to protect intelligence and law enforcement sources
and methods. Nothing in this order shall be interpreted to supersede measures
established under authority of law to protect the security and integrity
of specific activities and associations that are in direct support of intelligence
and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international
obligations.

(e) This order 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.

THE WHITE HOUSE,
February 12, 2013.
Executive Summary

Cyber threats are becoming increasingly more common, more sophisticated, and more dangerous. One way that private entities may defend against cyber attacks is by sharing technical cyber threat information – such as threat signatures, indicators, and alerts – with each other. Today, much of this sharing is taking place. Some private entities may, however, be hesitant to share cyber threat information with others, especially competitors, because they believe such sharing may raise antitrust issues.

Through this Statement, the Department of Justice’s Antitrust Division (the “Division”) and the Federal Trade Commission (the “Commission” or “FTC”) (collectively, the “Agencies”) explain their analytical framework for information sharing and make it clear that they do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing. Cyber threat information typically is very technical in nature and very different from the sharing of competitively sensitive information such as current or future prices and output or business plans.

Specific guidance in the context of cybersecurity information was previously provided by the Division’s October 2000 business review letter to the Electric Power Research Institute, Inc. (EPRI). The Division confirmed that it had no intention to initiate an enforcement action against EPRI’s proposal to exchange certain cybersecurity information, including exchanging actual real-time cyber threat and attack information. While this guidance is now over a decade old, it remains the Agencies’ current analysis that properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns.
1. Overview of Cybersecurity and Information Sharing

The Agencies share the President's view that "cyber threat is one of the most serious economic and national security challenges we face as a nation" and are committed to doing all they can to improve the safety of our nation's networks. Our modern economy and national security depend on a secure cyberspace. Core features of our nation's cybersecurity strategy are to improve our resilience to cyber incidents and to reduce and defend against cyber threats. One way to make progress on these fronts is by increasing cyber threat information sharing between the government and industry, and among industry participants. In his February 2013 Executive Order, the President highlighted the important role the government can play in sharing information with U.S. private sector entities, while ensuring that privacy and civil liberties protections are in place. Another important component of securing our IT infrastructure is through the sharing of cybersecurity information between and among private entities. In particular, the sharing of information about cybersecurity threats, such as incident or threat reports,

---


2 Through its Computer Crime and Intellectual Property Section, the Department of Justice (the "Department" or "DOJ") has trained prosecutors to focus on investigating and prosecuting cybercrime and intellectual property cases in each of the nation's 94 federal districts. The National Security Division's (NSD) National Security Cyber Specialists (NSCS) Network brings together the Department's full range of expertise on national security-related cyber matters, drawing on experts from NSD, the U.S. Attorney's Offices, and other Department components. The Department has emphasized using all of its legal tools to disrupt and dismantle criminal cyber infrastructure, such as botnets, and to arrest those responsible for building and operating such infrastructure for criminal purposes.


4 In its 2011 legislative proposal, the Administration defined a cybersecurity threat as "any action that may result in unauthorized access to, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system, or unauthorized exfiltration of information stored on or transiting an information system." Law Enforcement Provisions Related to Computer Security § 242(8) (2011), available at
indicators, threat signatures, and alerts (collectively, "cyber threat information") among these entities has the potential to greatly improve the safety of our systems.

Today, some private-to-private cyber threat information sharing is taking place, both informally and through formal exchanges or agreements, such as the many sector-specific Information Sharing Analysis Centers (ISACs) that have been established to advance the physical and cybersecurity of critical infrastructures. Sharing can take many forms – it may be unstructured or very structured, human-to-human or automated, or somewhere in between. There are a number of benefits that derive from these arrangements – foremost, they increase the security, availability, integrity, and efficiency of our information systems. This, in turn, leads to a more secure and productive nation.

Some private entities may be hesitant to share cyber threat information with each other, especially competitors, because they have been counseled that sharing of information among competitors may raise antitrust concerns. The Agencies do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing. While it is true that certain information sharing agreements among competitors can raise competitive concerns, sharing of the cyber threat information


5 Indicators may include, for example, file hashes, computer code, malicious URLs, source email addresses, and technical characteristics of malware (e.g., "a pdf file of a certain size attached").

6 Threat signatures are the characteristics of specific cyber threats that may be used (often by automated systems) to identify, detect, and/or interdict them. Typically, multiple indicators are used to generate a threat signature.

7 An alert is intended to provide timely notification of security threats or activity. See, e.g., 2014 Alerts, UNITED STATES COMPUTER EMERGENCY READINESS TEAM, available at http://www.us-cert.gov/ncas/alerts.

mentioned above is highly unlikely to lead to a reduction in competition and, consequently, would not be likely to raise antitrust concerns. To decrease uncertainty regarding the Agencies’ analysis of this type of information sharing, the Agencies are issuing this Statement to describe how they analyze cyber threat information sharing.

2. Antitrust Analysis of Information Sharing Agreements

a. General Overview

The Agencies’ Antitrust Guidelines, business review letters, and advisory opinions explain the analytical framework for information sharing and the competition issues that may arise with information exchanges generally. The Agencies’ primary concern in this context is that the sharing of competitively sensitive information — such as recent, current, and future prices, cost data, or output levels — may facilitate price or other


10 Individuals who are concerned about the legality of future business activities under the antitrust laws can formally request that the Division issue a statement of its present enforcement intentions. 28 C.F.R. §50.6 (2010). If firms are concerned about a specific proposed program, they may choose to utilize the Division’s business review process. Business review letters allow the Division to take these general principles and provide prospective guidance to specific proposals. The Division is committed to resolving the request as expeditiously as possible so that it does not get in the way of legitimate collaborations. See Business Reviews, ANTITRUST DIV., U.S. DEP’T OF JUSTICE, available at http://www.justice.gov/atr/public/busreview/index.html.

11 The Commission’s Rules of Practice provide that the Commission or its staff, in appropriate circumstances, may offer industry guidance in the form of an advisory opinion. See 16 C.F.R. §§ 1.1-1.4.; see also http://www.ftc.gov/tips-advice/competition-guidance/competition-advisory-opinions. FTC staff recently issued an advisory opinion to the U.S. Money Transmitters regarding an information exchange program advising that the program was unlikely to harm competition and may enhance consumer protection goals. Letter from Michael J. Bloom, Asst. Dir., Bureau of Competition, Fed. Trade Comm’n, to Ezra C. Levine, Senior Of Counsel, Morrison & Foerster LLP (Sept. 4, 2013), available at http://www.ftc.gov/policy/advisory-opinions/money-services-round-table.
competitive coordination among competitors. The joint DOJ/FTC Antitrust Guidelines for Collaborations Among Competitors provide a good overview of how the Agencies analyze information sharing as a general matter.

First, these Guidelines note that the antitrust agencies will typically examine information sharing agreements under a rule of reason analysis, which considers the overall competitive effect of an agreement. "Rule of reason analysis focuses on the state of competition with, as compared to without, the relevant agreement. The central question is whether the relevant agreement likely harms competition by increasing the ability or incentive profitably to raise price above or reduce output, quality, service, or innovation below what likely would prevail in the absence of the relevant agreement." In some cases, the nature of the agreement may demonstrate the lack of competitive harm. In examining the nature of the relevant agreement, the Agencies take into account the business purposes for the agreement. If competitive harm seems likely, the Agencies will analyze the agreement in more depth to evaluate countervailing efficiencies.

The Competitor Collaboration Guidelines further explain the Agencies’ analysis:

---

12 COMPETITOR COLLABORATION GUIDELINES, supra note 9, at 21; HEALTHCARE STATEMENTS, supra note 9, at 64 ("Exchanges of future prices ... are very likely to be considered anticompetitive); IP LICENSING GUIDELINES, supra note 9, at 13 ("The risk [that a joint venture would adversely affect competition] ... would be increased to the extent that, for example, the joint venture facilitates the exchange among the parties of competitively sensitive information relating to the [] markets in which the parties currently compete, or facilitates the coordination in such markets.").

13 COMPETITOR COLLABORATION GUIDELINES, supra note 9; see also HEALTH CARE STATEMENTS, supra note 9. (These include guidelines for the dissemination of price and cost data, as well as non-fee related information, among health care providers and have been applied outside of the Health Care context); Case law also recognizes that gathering and disseminating information can be procompetitive. See United States v. United States Gypsum Co., 438 U.S. 422, 441 n.16 (1978) ("The exchange of price data and other information among competitors does not invariably have anticompetitive effects; indeed such practices can in certain circumstances increase economic efficiency and render markets more, rather than less, competitive.").

14 COMPETITOR COLLABORATION GUIDELINES, supra note 9, at 4.
The [Antitrust] Agencies recognize that the sharing of information among competitors may be procompetitive and is often reasonably necessary to achieve the procompetitive benefits of certain collaborations ... Nevertheless, in some cases, the sharing of information related to a market in which the collaboration operates or in which the participants are actual or potential competitors may increase the likelihood of collusion on matters such as price, output, or other competitively sensitive variables. The competitive concern depends on the nature of the information shared. Other things being equal, the sharing of information relating to price, output, costs, or strategic planning is more likely to raise competitive concern than the sharing of information relating to less competitively sensitive variables. Similarly, other things being equal, the sharing of information on current operating and future business plans is more likely to raise concerns than the sharing of historical information.\(^\text{15}\)

Within this framework, when evaluating an exchange of information the Agencies consider the extent to which competitively sensitive information likely would be disclosed to competitors. Antitrust risk is lower when the shared information is less competitively sensitive and unlikely to lead to a lessening of competition; thus the nature and detail of the information disclosed and the context in which information is shared are highly relevant. Additionally, it is less likely that the information sharing arrangements will facilitate collusion on competitively sensitive variables if appropriate safeguards governing information sharing are implemented to prevent or minimize such disclosure.

b. **Antitrust Analysis of Cyber Threat Information Sharing**

The analytical framework outlined above applies irrespective of industry. Below we apply that analysis with respect to the exchange of cyber threat information.

First, sharing of cyber threat information can improve efficiency and help secure our nation’s networks of information and resources. It appears that this sharing is virtually always likely to be done in an effort to protect networks and the information stored on those networks, and to deter cyber attacks. If companies are not sharing such

\(^{15}\) *Id.* at 15. See also United States v. United States Gypsum Co., 438 U.S. 422 (1978), examining whether the information exchanged has a legitimate purpose, or is more likely to be used for collusive purposes.
information as part of a conspiracy of the type that typically harms competition, the Agencies’ rule of reason analysis would consider the valuable purpose behind the exchange of information.

Second, the Agencies would consider the nature of the cyber threat information to be shared among the private parties. The nature of the information being shared is very important to the analysis. Cyber threat information typically is very technical in nature. For example, one of the most common methods of identifying malware (e.g., a virus, worm, etc.) is through signature detection. A threat signature is like a digital fingerprint; it is a unique string of bits or data that uniquely identifies a specific threat. Signature-based detection involves searching for known patterns of data. Sharing a signature for a previously unknown threat will enable the recipient to take action to prevent, detect, or contain an attack. Similarly, knowing the source IP address or target port of a Denial of Service (DOS) attack\(^\text{16}\) may enable one to take protective measures against such an attack by blocking illegitimate traffic. The sharing of this type of information is very different from the sharing of competitively sensitive information such as current or future prices and output or business plans which can raise antitrust concerns.

Finally, the Agencies would consider whether the exchange is likely to harm competition. Generally speaking, cyber threat information covers a limited category of information\(^\text{17}\) and disseminating information of this nature appears unlikely in the abstract to increase the ability or incentive of participants to raise price or reduce output.

\(^{16}\) A DOS attack involves flooding a targeted system with incoming, useless traffic with the goal of making the attacked network unavailable to its intended users.

\(^{17}\) In addition, the Agencies understand that many companies have antitrust compliance programs in place to prevent the sharing of competitively sensitive information.
quality, service, or innovation. However, this type of analysis is intensely fact-driven. In the one instance in which the Division had occasion to review a cybersecurity information sharing arrangement, it concluded that antitrust concerns did not arise. This was in a favorable business review letter that the Division issued in 2000 to EPRI, a nonprofit organization "committed to providing and disseminating science and technology-based solutions to energy industry problems." The business review involved a proposal to share information to improve physical and cyber security. EPRI had developed an Enterprise Infrastructure Security (EIS) program to assist the various energy industries in addressing security risks raised by the increased interconnection, interdependence, and computerization of the energy sector, its suppliers, and customers.

EPRI proposed exchanging two types of information: best practices and information related to cybersecurity vulnerabilities. EPRI further noted that the program eventually might include a discussion and analysis of actual real time cyber threat and attack information from a variety of sources, including participants, federal and state governments, other infrastructure industries, cybersecurity experts and others, in order to more quickly identify and address in real time any actual cybersecurity threats and attacks on the reliability of the nation’s energy supply. All information exchanged would relate directly to physical and cybersecurity, and there would be no discussion of prices for equipment or recommendations in favor of a vendor. The Division concluded that "[a]s long as the information exchanged is limited…to physical and cybersecurity issues, the proposed interdictions on price, purchasing and future product innovation discussions should be sufficient to avoid any threats to competition. Indeed, to the extent that the

---

proposed information exchanges result in more efficient means of reducing cybersecurity costs, and such savings redound to the benefit of consumers, the information exchanges could be procompetitive in effect.\(^\text{19}\)

Although the nature, complexity, and number of threats have changed since the Division issued the EPRI letter, the legal analysis in the letter remains very current.\(^\text{20}\)

Thus, the Agencies’ guidance establishes that properly designed sharing of cyber threat information should not raise antitrust concerns.\(^\text{21}\)

\(^{19}\) *Id. at 3-4. See also* Letter from Joel I. Klein, Assistant Att’y Gen., Antitrust Div., U.S. Dep’t of Justice, to Robert B. Bell, Partner, Wiley, Rein & Fielding (July 1, 1998), *available at* http://www.justice.gov/atr/public/busreview/1824.htm (exchange of information including methods of remediating Year 2000 problems); Letter from Joel I. Klein, Assistant Att’y Gen., Antitrust Div., U.S. Dep’t of Justice, to Jerry J. Jasinski, President, Nat’l Assoc. of Mfrs. (Aug. 14, 1998), *available at* http://www.justice.gov/atr/public/busreview/1877.htm (exchange of information including methods of remediating Year 2000 problems, including promoting bilateral exchanges between Association members) (The Department noted it would be concerned if parties, under the guise of a Year 2000 remedial program, exchanged price or other competitively-sensitive information, agreed not to compete for particular business, agreed not to deal with certain suppliers or entered into other anticompetitive agreements); Letter from J. Mark Gidley, Acting Assistant Att’y Gen., Antitrust Div., U.S. Dep’t of Justice, to Stuart M. Pape, Partner, Patton, Boggs & Blow (Jan. 14, 1993), *available at* http://www.justice.gov/atr/public/busreview/211550.htm (in issuing a favorable review the Division noted that the “information to be exchanged among the venture participants, however, will be solely of a technical nature....”).

\(^{20}\) *See, e.g.*, Renata B. Hesse, Deputy Assistant Att’y Gen., Antitrust Div., U.S. Dep’t of Justice, At the Intersection of Antitrust & High-Tech: Opportunities for Constructive Engagement, Remarks as Prepared for the Conference on Competition and IP Policy in High-Technology Industries at 10-11 (Jan. 22, 2014), *available at* http://www.justice.gov/atr/public/speeches/303152.pdf. (“While this [EPRI] guidance is now over a decade old, it remains the Antitrust Division’s current analysis that properly designed sharing of cyber-security threat information is not likely to raise antitrust concerns.”).

\(^{21}\) Of course, if an information sharing arrangement is being used as a cover to fix prices, allocate markets, or otherwise limit competition, antitrust issues could arise.
Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014
Table of Contents

Executive Summary.................................................................................................................1
1.0 Framework Introduction.................................................................................................3
2.0 Framework Basics...........................................................................................................7
3.0 How to Use the Framework............................................................................................13
Appendix A: Framework Core..............................................................................................18
Appendix B: Glossary............................................................................................................37
Appendix C: Acronyms..........................................................................................................39

List of Figures

Figure 1: Framework Core Structure....................................................................................7
Figure 2: Notional Information and Decision Flows within an Organization.........................12

List of Tables

Table 1: Function and Category Unique Identifiers..............................................................19
Table 2: Framework Core......................................................................................................20
Executive Summary

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers.

To better address these risks, the President issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013, which established that “[i]t is the Policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.” In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Executive Order also requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program.

The Framework enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today’s multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be
used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Use of this voluntary Framework is the next step to improve the cybersecurity of our Nation’s critical infrastructure – providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation’s critical infrastructure as a whole.
1.0 Framework Introduction

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013.\(^1\) This Executive Order calls for the development of a voluntary Cybersecurity Framework (“Framework”) that provides a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk.

Critical infrastructure is defined in the EO as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization’s size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation’s infrastructure. Members of each critical infrastructure sector perform functions that are supported by information technology (IT) and industrial control systems (ICS).\(^2\) This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organization’s business, assets, health and safety of individuals, and the environment should be considered. To manage cybersecurity risks, a clear understanding of the organization’s business drivers and security considerations specific to its use of IT and ICS is required. Because each organization’s risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Executive Order requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization’s approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

---


To ensure extensibility and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework complements, and does not replace, an organization’s risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

Just as the Framework is not industry-specific, the common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities. These components are explained below.

- The **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. The Framework Core
then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- **Framework Implementation Tiers** ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

- A **Framework Profile** ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization’s risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.
The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2009\(^3\), ISO/IEC 27005:2011\(^4\), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39\(^5\), and the *Electricity Subsector Cybersecurity Risk Management Process (RMP)* guideline\(^6\).

1.3 Document Overview

The remainder of this document contains the following sections and appendices:

- **Section 2** describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- **Section 3** presents examples of how the Framework can be used.
- **Appendix A** presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- **Appendix B** contains a glossary of selected terms.
- **Appendix C** lists acronyms used in this document.

---


2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

2.1 Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in Figure 1:

![Figure 1: Framework Core Structure](image)

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”
Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process. The five Framework Core Functions are defined below. These Functions are not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See Appendix A for the complete Framework Core listing.

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at http://www.nist.gov/cyberframework/.
The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

### 2.2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization’s overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization’s management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization’s current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective. Successful implementation of the Framework is based upon achievement of the outcomes described in the organization’s Target Profile(s) and not upon Tier determination.
The Tier definitions are as follows:

Tier 1: Partial

- **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

- **Integrated Risk Management Program** – There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.

- **External Participation** – An organization may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 2: Risk Informed

- **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

- **Integrated Risk Management Program** – There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.

- **External Participation** – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

Tier 3: Repeatable

- **Risk Management Process** – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

- **Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.

- **External Participation** – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.
Tier 4: Adaptive

- **Risk Management Process** – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

- **Integrated Risk Management Program** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

- **External Participation** – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

### 2.3 Framework Profile

The Framework Profile (“Profile”) is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in the communication of risk within and between organizations. This Framework document does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps can contribute to the roadmap described above. Prioritization of gap mitigation is driven by the organization’s business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.
2.4 Coordination of Framework Implementation

Figure 2 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization’s overall risk management process and to the implementation/operations level for awareness of business impact.

Figure 2: Notional Information and Decision Flows within an Organization
3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization’s cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The following sections present different ways in which organizations can use the Framework.

3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization’s current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired outcomes, thus managing cybersecurity commensurate with the known risk. Conversely, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources to strengthen other cybersecurity practices.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including “How are we doing?” Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.
Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization’s overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization’s desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient
step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

### 3.3 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services. Examples include:

- An organization may utilize a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.

### 3.4 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

### 3.5 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology as required by the Executive Order to address individual privacy and civil liberties implications that may result from cybersecurity operations. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program may give rise to these considerations. Consistent with Section 3.4, technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and civil liberties implications may arise when personal information is used, collected, processed, maintained, or disclosed in connection with an organization’s cybersecurity activities. Some examples of activities that bear privacy or civil liberties considerations may include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; cybersecurity mitigation activities that result in denial of service or other similar potentially
adverse impacts, including activities such as some types of incident detection or monitoring that may impact freedom of expression or association.

The government and agents of the government have a direct responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or agents of the government that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.

To address privacy implications, organizations may consider how, in circumstances where such measures are appropriate, their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in Appendix A, the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

**Governance of cybersecurity risk**

- An organization’s assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements
- Process is in place to assess implementation of the foregoing organizational measures and controls

**Approaches to identifying and authorizing individuals to access organizational assets and systems**

- Steps are taken to identify and address the privacy implications of access control measures to the extent that they involve collection, disclosure, or use of personal information

**Awareness and training measures**

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities
- Service providers that provide cybersecurity-related services for the organization are informed about the organization’s applicable privacy policies
Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization’s anomalous activity detection and cybersecurity monitoring

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities
- Process is in place to conduct a privacy review of an organization’s cybersecurity mitigation efforts
Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization’s risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.
<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IDENTIFY (ID)</td>
<td>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.</td>
<td>ID.AM-1: Physical devices and systems within the organization are inventoried</td>
<td>• CCS CSC 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• COBIT 5 BA109.01, BA109.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.2.3.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 7.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-2: Software platforms and applications within the organization are inventoried</td>
<td>• CCS CSC 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• COBIT 5 BA109.01, BA109.02, BA109.05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.2.3.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 7.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-3: Organizational communication and data flows are mapped</td>
<td>• CCS CSC 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• COBIT 5 DSS05.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.2.3.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.13.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-4: External information systems are catalogued</td>
<td>• COBIT 5 APO02.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.11.2.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 AC-20, SA-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value</td>
<td>• COBIT 5 APO03.03, APO03.04, BA109.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.2.3.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.8.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</td>
<td>• COBIT 5 APO01.02, DSS06.03</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.2.3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.6.1.1</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Business Environment (ID.BE):</td>
<td></td>
<td>ID.BE-1: The organization’s role in the supply chain is identified and communicated</td>
<td>NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated</td>
<td>COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated</td>
<td>ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE-4: Dependencies and critical functions for delivery of critical services are established</td>
<td>NIST SP 800-53 Rev. 4 CP-2, SA-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE-5: Resilience requirements to support delivery of critical services are established</td>
<td>COBIT 5 APO02.06, APO03.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISB 62443-2:1:2009 4.2.2.1, 4.2.3.6</td>
<td></td>
</tr>
<tr>
<td>Governance (ID.GV):</td>
<td></td>
<td>ID.GV-1: Organizational information security policy is established</td>
<td>NIST SP 800-53 Rev. 4 PM-11, SA-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISB 62443-2:1:2009 4.3.2.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.5.1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COBIT 5 APO01.03, EDM01.01, EDM01.02</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-2:1:2009 4.3.2.3.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.6.1.1, A.7.2.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 PM-1, PS-7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COBIT 5 APO13.12</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-2:1:2009 4.3.2.3.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.6.1.1, A.7.2.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 PM-1, PS-7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COBIT 5 MEA03.01, MEA03.04</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA 62443-2:1:2009 4.4.3.7</td>
<td></td>
</tr>
</tbody>
</table>
## Cybersecurity Framework

**Function**

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| **ID.GY-4: Governance and risk management processes address cybersecurity risks** | including privacy and civil liberties obligations, are understood and managed | - ISO/IEC 27001:2013 A.18.1  
- NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) |
| **ID.RA-1: Asset vulnerabilities are identified and documented** | | - COBIT 5 DSS04.02  
- ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3  
- NIST SP 800-53 Rev. 4 PM-9, PM-11 |
| **ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources** | | - CCS CSC 4  
- COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04  
- ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12  
- ISO/IEC 27001:2013 A.12.6.1, A.18.2.3  
- NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 |
| **ID.RA-3: Threats, both internal and external, are identified and documented** | | - ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12  
- ISO/IEC 27001:2013 A.6.1.4  
- NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 |
| **ID.RA-4: Potential business impacts and likelihoods are identified** | | - COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04  
- ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12  
- NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 |
| **ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk** | | - COBIT 5 APO12.02  
- ISO/IEC 27001:2013 A.12.6.1  
- NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 |
| **ID.RA-6: Risk responses are identified and** | | - COBIT 5 APO12.05, APO13.02 |

**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTECT (PR)</td>
<td>PROTECT (PR)</td>
<td>prioritized</td>
<td>NIST SP 800-53 Rev. 4 PM-4, PM-9</td>
</tr>
<tr>
<td>Risk Management Strategy (ID.RM)</td>
<td>Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</td>
<td>ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders</td>
<td>COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, ISA 62443-2-1:2009 4.3.4.2, NIST SP 800-53 Rev. 4 PM-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM-2: Organizational risk tolerance is determined and clearly expressed</td>
<td>COBIT 5 APO12.06, ISA 62443-2-1:2009 4.3.2.6.5, NIST SP 800-53 Rev. 4 PM-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis</td>
<td>NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14</td>
</tr>
<tr>
<td>PROTECT (PR)</td>
<td>PROTECT (PR)</td>
<td>PR.AC-1: Identities and credentials are managed for authorized devices and users</td>
<td>CCS CSC 16, COBIT 5 DSS05.04, DSS06.03, ISA 62443-2-1:2009 4.3.3.5.1, ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, NIST SP 800-53 Rev. 4 AC-2, IA Family</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AC-2: Physical access to assets is managed and protected</td>
<td>COBIT 5 DSS01.04, DSS05.05, ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8, ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AC-3: Remote access is managed</td>
<td>COBIT 5 APO13.01, DSS01.04, DSS05.03, ISA 62443-2-1:2009 4.3.3.6.6, ISA 62443-3-3:2013 SR 1.13, SR 2.6, ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| PR.AC-4  |          | Access permissions are managed, incorporating the principles of least privilege and separation of duties | • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20  
• CCS CSC 12, 15  
• ISA 62443-2-1:2009 A.3.3.7.3  
• ISA 62443-3-3:2013 SR 2.1  
• NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 |
| PR.AC-5  |          | Network integrity is protected, incorporating network segregation where appropriate | • ISA 62443-2-1:2009 A.3.3.4  
• ISA 62443-3-3:2013 SR 3.1, SR 3.8  
• NIST SP 800-53 Rev. 4 AC-4, SC-7 |
| PR.AT-1  |          | All users are informed and trained | • CCS CSC 9  
• COBIT 5 APO07.03, BAI05.07  
• ISA 62443-2-1:2009 A.3.2.4.2  
• ISO/IEC 27001:2013 A.7.2.2  
• NIST SP 800-53 Rev. 4 AT-2, PM-13 |
| PR.AT-2  |          | Privileged users understand roles & responsibilities | • CCS CSC 9  
• COBIT 5 APO07.02, DSS06.03  
• ISA 62443-2-1:2009 A.3.2.4.2, A.3.2.4.3  
• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2  
• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| PR.AT-3  |          | Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | • CCS CSC 9  
• COBIT 5 APO07.03, APO10.04, APO10.05  
• ISA 62443-2-1:2009 A.3.2.4.2  
• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2  
• NIST SP 800-53 Rev. 4 PS-7, SA-9 |
| PR.AT-4  |          | Senior executives understand roles & responsibilities | • CCS CSC 9  
• COBIT 5 APO07.03 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
|          |          | PR.AT-5: Physical and information security personnel understand roles & responsibilities | • ISA 62443-2-1:2009 4.3.2.4.2  
• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,  
• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
|          |          | PR.DS-1: Data-at-rest is protected | • CCS CSC 17  
• COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06  
• ISA 62443-3-3:2013 SR 3.4, SR 4.1  
• ISO/IEC 27001:2013 A.8.2.3  
• NIST SP 800-53 Rev. 4 SC-28 |
| Data Security (PR.DS): |          | PR.DS-2: Data-in-transit is protected | • CCS CSC 17  
• COBIT 5 APO01.06, DSS06.06  
• ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2  
• NIST SP 800-53 Rev. 4 SC-8 |
|          |          | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition | • COBIT 5 BAI09.03  
• ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1  
• ISA 62443-3-3:2013 SR 4.2  
• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7  
• NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 |
|          |          | PR.DS-4: Adequate capacity to ensure availability is maintained | • COBIT 5 APO13.01  
• ISA 62443-3-3:2013 SR 7.1, SR 7.2  
• ISO/IEC 27001:2013 A.12.3.1 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.DS-5: Protections against data leaks are implemented</td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• CCS CSC 17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• COBIT 5 APO1.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</td>
</tr>
<tr>
<td>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 SI-7</td>
</tr>
<tr>
<td>PR.DS-7: The development and testing environment(s) are separate from the production environment</td>
<td></td>
<td></td>
<td>• COBIT 5 BAI07.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.12.1.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CM-2</td>
</tr>
<tr>
<td>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</td>
<td></td>
<td></td>
<td>• CCS CSC 3, 10</td>
</tr>
<tr>
<td>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained</td>
<td></td>
<td></td>
<td>• COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 7.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</td>
</tr>
<tr>
<td>PR.IP-2: A System Development Life Cycle to manage systems is implemented</td>
<td></td>
<td></td>
<td>• COBIT 5 APO13.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.3.3</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>PR.IP-3:</td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• COBIT 5 BA106.01, BA101.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 7.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</td>
</tr>
<tr>
<td>PR.IP-4:</td>
<td></td>
<td></td>
<td>• COBIT 5 APO13.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.3.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 7.3, SR 7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9</td>
</tr>
<tr>
<td>PR.IP-5:</td>
<td></td>
<td></td>
<td>• COBIT 5 DSS01.04, DSS05.05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.3.3.1, 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.4, 4.3.3.3.5, 4.3.3.3.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18</td>
</tr>
<tr>
<td>PR.IP-6:</td>
<td></td>
<td></td>
<td>• COBIT 5 BA109.03</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.4.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 MP-6</td>
</tr>
<tr>
<td>PR.IP-7:</td>
<td></td>
<td></td>
<td>• COBIT 5 APO11.06, DSS04.05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>PR.IP-8</td>
<td>Effectiveness of protection technologies is shared with appropriate parties</td>
<td>- ISO/IEC 27001:2013 A.16.1.6&lt;br&gt;- NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4</td>
<td></td>
</tr>
<tr>
<td>PR.IP-9</td>
<td>Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</td>
<td>- COBIT 5 DSS04.03&lt;br&gt;- ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1&lt;br&gt;- ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2&lt;br&gt;- NIST SP 800-53 Rev. 4 CP-2, IR-8</td>
<td></td>
</tr>
<tr>
<td>PR.IP-10</td>
<td>Response and recovery plans are tested</td>
<td>- ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11&lt;br&gt;- ISA 62443-3-3:2013 SR 3.3&lt;br&gt;- ISO/IEC 27001:2013 A.17.1.3&lt;br&gt;- NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14</td>
<td></td>
</tr>
<tr>
<td>PR.IP-11</td>
<td>Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)</td>
<td>- COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05&lt;br&gt;- ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3&lt;br&gt;- ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4&lt;br&gt;- NIST SP 800-53 Rev. 4 PS Family</td>
<td></td>
</tr>
<tr>
<td>PR.IP-12</td>
<td>A vulnerability management plan is developed and implemented</td>
<td>- ISO/IEC 27001:2013 A.12.6.1, A.18.2.2&lt;br&gt;- NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2</td>
<td></td>
</tr>
<tr>
<td><strong>Maintenance (PR.MA):</strong> Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.</td>
<td>PR.MA-1</td>
<td>Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools</td>
<td>- COBIT 5 BA109.03&lt;br&gt;- ISA 62443-2-1:2009 4.3.3.3.7&lt;br&gt;- ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5&lt;br&gt;- NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5</td>
</tr>
<tr>
<td>PR.MA-2</td>
<td>Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access</td>
<td>- COBIT 5 DSS05.04&lt;br&gt;- ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8&lt;br&gt;- ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>PR.PT-1:</strong> Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</td>
<td></td>
<td>- NIST SP 800-53 Rev. 4 MA-4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CCS CSC 14</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- COBIT 5 APO11.04</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ISA 62443-2-1:2009 4.3.3.3.2.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NIST SP 800-53 Rev. 4 AU Family</td>
<td></td>
</tr>
<tr>
<td><strong>PR.PT-2:</strong> Removable media is protected and its use restricted according to policy</td>
<td></td>
<td>- COBIT 5 DSS05.02, APO13.01</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ISA 62443-3-3:2013 SR 2.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7</td>
<td></td>
</tr>
<tr>
<td><strong>PR.PT-3:</strong> Access to systems and assets is controlled, incorporating the principle of least functionality</td>
<td></td>
<td>- COBIT 5 DSS05.02</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ISA 62443-2-1:2009 4.3.3.3.1, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ISO/IEC 27001:2013 A.9.1.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NIST SP 800-53 Rev. 4 AC-3, CM-7</td>
<td></td>
</tr>
<tr>
<td><strong>PR.PT-4:</strong> Communications and control networks are protected</td>
<td></td>
<td>- CCS CSC 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- COBIT 5 DSS05.02, APO13.01</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| DETECT (DE) | Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | - COBIT 5 DSS03.01  
- NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 |
| | | DE.AE-2: Detected events are analyzed to understand attack targets and methods | - ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8  
- ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2  
- NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 |
| | | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors | - ISA 62443-3-3:2013 SR 6.1  
- NIST SP 800-53 Rev. 4 SR 6.1 |
| | | DE.AE-4: Impact of events is determined | - COBIT 5 APO12.06  
- NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4 |
| | | DE.AE-5: Incident alert thresholds are established | - COBIT 5 APO12.06  
- ISA 62443-2-1:2009 4.2.3.10  
- NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 |
| | Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. | DE.CM-1: The network is monitored to detect potential cybersecurity events | - CCS CSC 14, 16  
- COBIT 5 DSS05.07  
- ISA 62443-3-3:2013 SR 6.2  
- NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 |
<p>| | | DE.CM-2: The physical environment is | - ISA 62443-2-1:2009 4.3.3.3.8 |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>monitored to detect potential cybersecurity events</td>
<td>NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20</td>
</tr>
<tr>
<td>DE.CM-4</td>
<td></td>
<td>DE.CM-4: Malicious code is detected</td>
<td>CCS CSC 5, COBIT 5 DSS05.01, ISA 62443-2-1:2009 4.3.4.3.8, ISA 62443-3-3:2013 SR 3.2, ISO/IEC 27001:2013 A.12.2.1, NIST SP 800-53 Rev. 4 SI-3</td>
</tr>
<tr>
<td>DE.CM-6</td>
<td></td>
<td>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</td>
<td>COBIT 5 APO07.06, ISO/IEC 27001:2013 A.14.2.7, A.15.2.1, NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4</td>
</tr>
<tr>
<td>DE.CM-7</td>
<td></td>
<td>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</td>
<td>NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4</td>
</tr>
<tr>
<td>DE.CM-8</td>
<td></td>
<td>DE.CM-8: Vulnerability scans are performed</td>
<td>COBIT 5 BA103.10, ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7, ISO/IEC 27001:2013 A.12.6.1, NIST SP 800-53 Rev. 4 RA-5</td>
</tr>
</tbody>
</table>

**Detection Processes (DE.DP):**
Detection processes and procedures are maintained and tested to ensure timely and accountable

<p>| DE.DP-1 |          | DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability | CCS CSC 5, COBIT 5 DSS05.01, ISA 62443-2-1:2009 4.4.3.1, ISO/IEC 27001:2013 A.6.1.1 |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>adequate awareness of anomalous events.</td>
<td>• NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14</td>
</tr>
</tbody>
</table>
|          |          | DE.DP-2: Detection activities comply with all applicable requirements | • ISA 62443-2-1:2009 4.4.3.2  
• ISO/IEC 27001:2013 A.18.1.4  
• NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 |
|          |          | DE.DP-3: Detection processes are tested | • COBIT 5 APO13.02  
• ISA 62443-2-1:2009 4.4.3.2  
• ISA 62443-3-3:2013 SR 3.3  
• ISO/IEC 27001:2013 A.14.2.8  
• NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 |
|          |          | DE.DP-4: Event detection information is communicated to appropriate parties | • COBIT 5 APO12.06  
• ISA 62443-2-1:2009 4.3.4.5.9  
• ISA 62443-3-3:2013 SR 6.1  
• ISO/IEC 27001:2013 A.16.1.2  
• NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 |
|          |          | DE.DP-5: Detection processes are continuously improved | • COBIT 5 APO11.06, DSS04.05  
• ISA 62443-2-1:2009 4.4.3.4  
• ISO/IEC 27001:2013 A.16.1.6  
• NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Planning (RS.RP):</td>
<td>Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.</td>
<td>RS.RP-1: Response plan is executed during or after an event</td>
<td>• COBIT 5 BA101.10&lt;br&gt;• CCS CSC 18&lt;br&gt;• ISA 62443-2-1:2009 4.3.4.5.1&lt;br&gt;• ISO/IEC 27001:2013 A.16.1.5&lt;br&gt;• NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8</td>
</tr>
<tr>
<td>Communications (RS.CO):</td>
<td>Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.</td>
<td>RS.CO-1: Personnel know their roles and order of operations when a response is needed</td>
<td>• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4&lt;br&gt;• ISO/IEC 27001:2013 A.6.1.1, A.16.1.1&lt;br&gt;• NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8</td>
</tr>
<tr>
<td>Respond (RS)</td>
<td></td>
<td>RS.CO-2: Events are reported consistent with established criteria</td>
<td>• ISA 62443-2-1:2009 4.3.4.5.5&lt;br&gt;• ISO/IEC 27001:2013 A.6.1.3, A.16.1.2&lt;br&gt;• NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO-3: Information is shared consistent with response plans</td>
<td>• ISA 62443-2-1:2009 4.3.4.5.2&lt;br&gt;• ISO/IEC 27001:2013 A.16.1.2&lt;br&gt;• NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO-4: Coordination with stakeholders occurs consistent with response plans</td>
<td>• ISA 62443-2-1:2009 4.3.4.5.5&lt;br&gt;• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</td>
<td>• NIST SP 800-53 Rev. 4 PM-15, SI-5</td>
</tr>
<tr>
<td>Analysis (RS.AN):</td>
<td>Analysis is conducted to ensure adequate response and support recovery activities.</td>
<td>RS.AN-1: Notifications from detection systems are investigated</td>
<td>• COBIT 5 DSS02.07&lt;br&gt;• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8&lt;br&gt;• ISA 62443-3-3:2013 SR 6.1&lt;br&gt;• ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5&lt;br&gt;• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-8</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
|          |          | **RS.AN-2:** The impact of the incident is understood | • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8  
• ISO/IEC 27001:2013 A.16.1.6  
• NIST SP 800-53 Rev. 4 CP-2, IR-4 |
|          |          | **RS.AN-3:** Forensics are performed | • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1  
• ISO/IEC 27001:2013 A.16.1.7  
• NIST SP 800-53 Rev. 4 AU-7, IR-4 |
|          |          | **RS.AN-4:** Incidents are categorized consistent with response plans | • ISA 62443-2-1:2009 4.3.4.5.6  
• ISO/IEC 27001:2013 A.16.1.4  
• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 |
| **Mitigation (RS.MI):** |          | **RS.MI-1:** Incidents are contained | • ISA 62443-2-1:2009 4.3.4.5.6  
• ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4  
• ISO/IEC 27001:2013 A.16.1.5  
• NIST SP 800-53 Rev. 4 IR-4 |
|          |          | **RS.MI-2:** Incidents are mitigated | • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10  
• ISO/IEC 27001:2013 A.12.2.1, A.16.1.5  
• NIST SP 800-53 Rev. 4 IR-4 |
|          |          | **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks | • ISO/IEC 27001:2013 A.12.6.1  
• NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 |
| **Improvements (RS.IM):** |          | **RS.IM-1:** Response plans incorporate lessons learned | • COBIT 5 BA101.13  
• ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4  
• ISO/IEC 27001:2013 A.16.1.6  
• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |
|          |          | **RS.IM-2:** Response strategies are updated | • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |
| **RECOVER (RC):** |          | **RC.RP-1:** Recovery plan is executed during or after an event | • CCS CSC 8  
• COBIT 5 DSS02.05, DSS03.04  
• ISO/IEC 27001:2013 A.16.1.5 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restoration of systems or</td>
<td>Improvements (RC.IM):</td>
<td>RC.IM-1: Recovery plans incorporate lessons learned</td>
<td>NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8</td>
</tr>
<tr>
<td>assets affected by</td>
<td>Recovery planning and processes are</td>
<td>RC.IM-2: Recovery strategies are updated</td>
<td>COBIT 5 BAI05.07</td>
</tr>
<tr>
<td>cybersecurity events.</td>
<td>improved by incorporating lessons learned into future activities.</td>
<td></td>
<td>ISA 62443-2-1:2009 4.4.3.4</td>
</tr>
<tr>
<td></td>
<td>Communications (RC.CO): Restoration activities are coordinated with internal and</td>
<td>RC.CO-1: Public relations are managed</td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td>external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.</td>
<td>RC.CO-2: Reputation after an event is repaired</td>
<td>COBIT 5 EDM03.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams</td>
<td>NIST SP 800-53 Rev. 4 CP-2, IR-4</td>
</tr>
</tbody>
</table>

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): [http://www.isaca.org/COBIT/Pages/default.aspx](http://www.isaca.org/COBIT/Pages/default.aspx)
Mappings between the Framework Core Subcategories and the specified sections in the Informative References represent a general correspondence and are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.
Appendix B: Glossary

This appendix defines selected terms used in the publication.

**Category**
The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”

**Critical Infrastructure**
Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.

**Cybersecurity**
The process of protecting information by preventing, detecting, and responding to attacks.

**Cybersecurity Event**
A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

**Detect (function)**
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

**Framework**
A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”

**Framework Core**
A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

**Framework Implementation Tier**
A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.

**Framework Profile**
A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.

**Function**
One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify,
Protect, Detect, Respond, and Recover.

**Identify (function)** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

**Informative Reference** A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory.

**Mobile Code** A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.

**Protect (function)** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

**Privileged User** A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

**Recover (function)** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

**Respond (function)** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

**Risk** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

**Risk Management** The process of identifying, assessing, and responding to risk.

**Subcategory** The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”
## Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS</td>
<td>Council on CyberSecurity</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technology</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IR</td>
<td>Interagency Report</td>
</tr>
<tr>
<td>ISA</td>
<td>International Society of Automation</td>
</tr>
<tr>
<td>ISAC</td>
<td>Information Sharing and Analysis Center</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>RFI</td>
<td>Request for Information</td>
</tr>
<tr>
<td>RMP</td>
<td>Risk Management Process</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
</tbody>
</table>