PANEL VI:

PUBLIC BUT CLASSIFIED: "A SYSTEM AWASH IN OPEN SECRETS"?

MODERATOR:
VIET DINH
Executive Order 13587 of October 7, 2011

Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. Policy. Our Nation’s security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

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 structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. 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.

Sec. 2. General Responsibilities of Agencies.

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and
(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. Senior Information Sharing and Safeguarding Steering Committee.

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch’s successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM–ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PDD–1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. Classified Information Sharing and Safeguarding Office.

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM–ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies
and standards needed to achieve classified information sharing and safeguarding goals; and
(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. Executive Agent for Safeguarding Classified Information on Computer Networks.

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the “Executive Agent”), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD–42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent’s responsibilities, in addition to those specified by NSD–42, shall include the following:
(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;
(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent’s timely development and issuance of technical policies and standards;
(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and
(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

Sec. 6. Insider Threat Task Force.

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be comprised of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force’s responsibilities shall include the following:
(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program’s Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. General Provisions. (a) For the purposes of this order, the word “agencies” shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.


(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM–ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD–42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD–42, and Executive Orders 12333, as amended, 12966, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided here.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower
Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:
   (1) the authority granted by law to an agency, or the head thereof; or
   (2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) 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,
October 7, 2011.
Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

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. Purpose. This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Sec. 2. Controlled Unclassified Information (CUI).
   (a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

   (b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

   (c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. Review of Current Designations.
   (a) Each agency head shall, within 180 days of the date of this order:
      (1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

      (2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

   (b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

Sec. 4. Development of CUI Categories and Policies.
(a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.

(b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.

(c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

(e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.

(f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Sec. 5. Implementation.

(a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.

(b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

(c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

Sec. 6. General Provisions.

(a) This order shall be implemented in a manner consistent with:
(1) applicable law, including protections of confidentiality and privacy rights;
(2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and
(3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.

(b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.

(c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.

(d) 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.

(e) This order shall be implemented subject to the availability of appropriations.

(f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(g) The Presidential Memorandum of May 7, 2008, entitled "Designation and Sharing of Controlled Unclassified Information (CUI)" is hereby rescinded.

THE WHITE HOUSE,
November 4, 2010.

[FR Doc. 2010–26300
Filed 11–9–10; 8:45 am]
Billing code 3195–W1–P
§798. Disclosure of classified information

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined under this title or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

(d)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—
(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of such violation.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1).

(3) Except as provided in paragraph (4), the provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)--(p)), shall apply to—
(A) property subject to forfeiture under this subsection;
(B) any seizure or disposition of such property; and
(C) any administrative or judicial proceeding in relation to such property,

if not inconsistent with this subsection.

(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

(5) As used in this subsection, the term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.


CODIFICATION

Another section 798 was renumbered section 798A of this title.

AMENDMENTS


1994—Subsec. (a). Pub. L. 103–322 substituted “fined under this title” for “fined not more than $10,000” in concluding provisions.

Executive Order - Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

NOW, THEREFORE, I, BARACK OBAMA, 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:

PART 1 -- ORIGINAL CLASSIFICATION

Section 1.1. Classification Standards. (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. Classification Levels. (a) Information may be classified at one of the following three levels:
(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.3. Classification Authority. (a) The authority to classify information originally may be exercised only by:

(1) the President and the Vice President;

(2) agency heads and officials designated by the President; and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position.

(5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

(d) All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in this order and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of classified information and on the sanctions in section 5.5 of this order that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original
classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information.

Sec. 1.4. Classification Categories. Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) the development, production, or use of weapons of mass destruction.

Sec. 1.5. Duration of Classification. (a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination
Required," or classified information that contains incomplete declassification instructions or lacks
declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.6. Identification and Markings. *(a)* At the time of original classification, the following shall be
indicated in a manner that is immediately apparent:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name and position, or by personal identifier, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b);

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); or

(D) in the case of information that should clearly and demonstrably be expected to reveal the identity of a
confidential human source or a human intelligence source or key design concepts of weapons of mass
destruction, the marking prescribed in implementing directives issued pursuant to this order; and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in
section 1.4 of this order.

(b) Specific information required in paragraph (a) of this section may be excluded if it would reveal
additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or
other means, indicate which portions are classified, with the applicable classification level, and which
portions are unclassified. In accordance with standards prescribed in directives issued under this order, the
Director of the Information Security Oversight Office may grant and revoke temporary waivers of this
requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings or other indicia implementing the provisions of this order, including abbreviations and
requirements to safeguard classified working papers, shall conform to the standards prescribed in
implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a
U.S. classification that provides a degree of protection at least equivalent to that required by the entity that
furnished the information. Foreign government information retaining its original classification markings need
not be assigned a U.S. classification marking provided that the responsible agency determines that the
foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as
classified at that level of classification despite the omission of other required markings. Whenever such
information is used in the derivative classification process or is reviewed for possible declassification,
holders of such information shall coordinate with an appropriate classification authority for the application of
omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified
information constitutes a small portion of an otherwise unclassified document or prepare a product to allow
for dissemination at the lowest level of classification possible or in unclassified form.
(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

Sec. 1.7. Classification Prohibitions and Limitations.

(a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may not be reclassified after declassification and release to the public under proper authority unless:

(1) the reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;

(2) the information may be reasonably recovered without bringing undue attention to the information;

(3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office, and

(4) for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information.

Sec. 1.8. Classification Challenges. (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.
(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

(c) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

Sec. 1.9. Fundamental Classification Guidance Review.
(a) Agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. The initial fundamental classification guidance review shall be completed within 2 years of the effective date of this order.

(b) The classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of this order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of this order.

(c) The classification guidance review shall include original classification authorities and agency subject matter experts to ensure a broad range of perspectives.

(d) Agency heads shall provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office and shall release an unclassified version of this report to the public.

PART 2 -- DERIVATIVE CLASSIFICATION

Sec. 2.1. Use of Derivative Classification. (a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:
(1) be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) observe and respect original classification decisions; and

(3) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources, or the marking established pursuant to section 1.6(a)(4)(D) of this order; and

(B) a listing of the source materials.
(c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the order, with an emphasis on avoiding over-classification, at least once every 2 years. Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

Sec. 2.2. Classification Guides. (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

(d) Agencies shall incorporate original classification decisions into classification guides on a timely basis and in accordance with directives issued under this order.

(e) Agencies may incorporate exemptions from automatic declassification approved pursuant to section 3.3(j) of this order into classification guides, provided that the Panel is notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

(f) The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years from the date of the origin of the document, except for:

(1) information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction; and

(2) specific information incorporated into classification guides in accordance with section 2.2(e) of this order.

PART 3 -- DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. Authority for Declassification. (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) Information shall be declassified or downgraded by:

(1) the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;

(2) the originator's current successor in function, if that individual has original classification authority;

(3) a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or
(4) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

(c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

(d) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(e) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the National Security Advisor. The information shall remain classified pending a prompt decision on the appeal.

(f) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

(g) No information may be excluded from declassification under section 3.3 of this order based solely on the type of document or record in which it is found. Rather, the classified information must be considered on the basis of its content.

(h) Classified nonrecord materials, including artifacts, shall be declassified as soon as they no longer meet the standards for classification under this order.

(i) When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.

Sec. 3.2. Transferred Records. (a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession of the records after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National
Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

Sec. 3.3. Automatic Declassification. (a) Subject to paragraphs (b)–(d) and (g)–(i) of this section, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(i) of this section. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which should clearly and demonstrably be expected to:

(1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

(5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(c)(1) An agency head shall notify the Panel of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and that the agency proposes to exempt from automatic declassification at 25 years.
(2) The notification shall include:

(A) a description of the file series;

(B) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(C) except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

(3) The Panel may direct the agency not to exempt a designated file series or to declassify the information within that series at an earlier date than recommended. The agency head may appeal such a decision to the President through the National Security Advisor.

(4) File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending Panel review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(d) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) After consultation with the Director of the National Declassification Center (the Center) established by section 3.7 of this order and before the records are subject to automatic declassification, an agency head or senior agency official may delay automatic declassification for up to five additional years for classified information contained in media that make a review for possible declassification exemptions more difficult or costly.

(3) Other than for records that are properly exempted from automatic declassification, records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information and could reasonably be expected to fall under one or more of the exemptions in paragraph (b) of this section shall be identified prior to the onset of automatic declassification for later referral to those agencies.

(A) The information of concern shall be referred by the Center established by section 3.7 of this order, or by the centralized facilities referred to in section 3.7(e) of this order, in a prioritized and scheduled manner determined by the Center.

(B) If an agency fails to provide a final determination on a referral made by the Center within 1 year of referral, or by the centralized facilities referred to in section 3.7(e) of this order within 3 years of referral, its equities in the referred records shall be automatically declassified.

(C) If any disagreement arises between affected agencies and the Center regarding the referral review period, the Director of the Information Security Oversight Office shall determine the appropriate period of review of referred records.

(D) Referrals identified prior to the establishment of the Center by section 3.7 of this order shall be subject to automatic declassification only in accordance with subparagraphs (d)(3)(A)–(C) of this section.

(4) After consultation with the Director of the Information Security Oversight Office, an agency head may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.
(e) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(f) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

(g) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, such information shall be declassified when comparable information concerning the United States nuclear program is declassified.

(h) Not later than 3 years from the effective date of this order, all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

(1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:

(A) the identity of a confidential human source or a human intelligence source; or

(B) key design concepts of weapons of mass destruction.

(2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.

(3) Records exempted from automatic declassification under this paragraph shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(i) Specific records exempted from automatic declassification prior to the establishment of the Center described in section 3.7 of this order shall be subject to the provisions of paragraph (h) of this section in a scheduled and prioritized manner determined by the Center.

(j) At least 1 year before information is subject to automatic declassification under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information that the agency proposes to exempt from automatic declassification under paragraphs (b) and (h) of this section.

(1) The notification shall include:

(A) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

(B) an explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and

(C) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.
(2) The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. An agency head may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

(k) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition (destruction) date of those records in each Agency Records Control Schedule or General Records Schedule, although the duration of classification shall be extended if the record has been retained for business reasons beyond the scheduled disposition date.

Sec. 3.4. Systematic Declassification Review. (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review for records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize their review of such records in accordance with priorities established by the Center.

(b) The Archivist shall conduct a systematic declassification review program for classified records: (1) accessioned into the National Archives; (2) transferred to the Archivist pursuant to 44 U.S.C. 2203; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

Sec. 3.5. Mandatory Declassification Review. (a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and

(3) the information is not the subject of pending litigation.

(b) Information originated by the incumbent President or the incumbent Vice President; the incumbent President's White House Staff or the incumbent Vice President's Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) If an agency has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requester of this fact and the prior review decision and advise the requester of appeal rights provided under subsection (e) of this section.

(e) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to
information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(f) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of National Intelligence shall develop special procedures for the review of information pertaining to intelligence sources, methods, and activities; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

(g) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

(h) This section shall not apply to any request for a review made to an element of the Intelligence Community that is made by a person other than an individual as that term is defined by 5 U.S.C. 552a(a)(2), or by a foreign government entity or any representative thereof.

Sec. 3.6. Processing Requests and Reviews. Notwithstanding section 4.1(i) of this order, in response to a request for information under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information, or identifies such documents in the process of implementing sections 3.3 or 3.4 of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

(c) Agencies may extend the classification of information in records determined not to have permanent historical value or nonrecord materials, including artifacts, beyond the time frames established in sections 1.5(b) and 2.2(f) of this order, provided:

(1) the specific information has been approved pursuant to section 3.3(j) of this order for exemption from automatic declassification; and

(2) the extension does not exceed the date established in section 3.3(j) of this order.

Sec. 3.7. National Declassification Center. (a) There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. There shall be a Director of the Center who shall be appointed or removed by the Archivist in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence.

(b) Under the administration of the Director, the Center shall coordinate:

(1) timely and appropriate processing of referrals in accordance with section 3.3(d)(3) of this order for accessioned Federal records and transferred presidential records.

(2) general interagency declassification activities necessary to fulfill the requirements of sections 3.3 and 3.4 of this order;
(3) the exchange among agencies of detailed declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order;

(4) the development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;

(5) the development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;

(6) the linkage and effective utilization of existing agency databases and the use of new technologies to document and make public declassification review decisions and support declassification activities under the purview of the Center; and

(7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.

(c) Agency heads shall fully cooperate with the Archivist in the activities of the Center and shall:

(1) provide the Director with adequate and current declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order; and

(2) upon request of the Archivist, assign agency personnel to the Center who shall be delegated authority by the agency head to review and exempt or declassify information originated by their agency contained in records accessioned into the National Archives, after consultation with subject-matter experts as necessary.

(d) The Archivist, in consultation with representatives of the participants in the Center and after input from the general public, shall develop priorities for declassification activities under the purview of the Center that take into account the degree of researcher interest and the likelihood of declassification.

(e) Agency heads may establish such centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes. Once established, all referral processing of accessioned records shall take place at the Center, and such agency facilities and operations shall be coordinated with the Center to ensure the maximum degree of consistency in policies and procedures that relate to records determined to have permanent historical value.

(f) Agency heads may exempt from automatic declassification or continue the classification of their own originally classified information under section 3.3(a) of this order except that in the case of the Director of National Intelligence, the Director shall also retain such authority with respect to the Intelligence Community.

(g) The Archivist shall, in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Director of the Information Security Oversight Office, provide the National Security Advisor with a detailed concept of operations for the Center and a proposed implementing directive under section 5.1 of this order that reflects the coordinated views of the aforementioned agencies.

PART 4 -- SAFEGUARDING

Sec. 4.1. General Restrictions on Access. (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head’s designee;

(2) the person has signed an approved nondisclosure agreement; and
(3) the person has a need-to-know the information.

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) An official or employee leaving agency service may not remove classified information from the agency's control or direct that information be declassified in order to remove it from agency control.

(d) Classified information may not be removed from official premises without proper authorization.

(e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.

(f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official or, with respect to the Intelligence Community, the Director of National Intelligence, shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information:

(1) prevent access by unauthorized persons;

(2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use:

(A) common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and

(B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.

(g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. "Confidential" information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(i)(1) Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(e) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order.

(2) Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government in accordance with statute, this order, directives implementing this order, direction of the President, or with the consent of the originating agency. For the
purposes of this section, "foreign government" includes any element of a foreign government, or an international organization of governments, or any element thereof.

(3) Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

(4) For purposes of this section, the Department of Defense shall be considered one agency, except that any dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued pursuant to section 6.2(b) of this order.

(5) Prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

Sec. 4.2. Distribution Controls. (a) The head of each agency shall establish procedures in accordance with applicable law and consistent with directives issued pursuant to this order to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in section 4.1(a) of this order.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information (including information marked pursuant to section 4.1(f)(1) of this order) to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of National Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution mechanism for classified information that it distributes. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.3. Special Access Programs. (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations. (1) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.
(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director of the Information Security Oversight Office and no more than one other employee of the Information Security Oversight Office or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency head shall brief the National Security Advisor, or a designee, on any or all of the agency's special access programs.

(6) For the purposes of this section, the term "agency head" refers only to the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each.

(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.4. Access by Historical Researchers and Certain Former Government Personnel. (a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need to-know the information may be waived for persons who:

(1) are engaged in historical research projects;

(2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or

(3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of the national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

PART 5 – IMPLEMENTATION AND REVIEW

Sec. 5.1. Program Direction. (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue such directives as are necessary to implement this order. These directives shall be binding on the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

(1) classification, declassification, and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;
(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

(c) The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this order with respect to the protection of intelligence sources, methods, and activities. Such directives shall be consistent with this order and directives issued under paragraph (a) of this section.

Sec. 5.2. Information Security Oversight Office. (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;

(4) have the authority to conduct on-site reviews of each agency’s program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the National Security Advisor within 60 days of the request for access. Access shall be denied pending the response;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the National Security Advisor;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.3. Interagency Security Classification Appeals Panel.

(a) Establishment and administration.
(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall designate a Chair from among the members of the Panel.

(2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative who meets the criteria in paragraph (a)(1) of this section to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

(3) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

(4) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Panel. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(5) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel’s functions.

(6) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(7) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel’s activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order;

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order; and

(4) appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the Federal Register. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the Federal courts; and

(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. The Panel shall report to the President through the National Security Advisor any instance in which it believes that an agency head is not cooperating fully with the Panel.
(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

(f) An agency head may appeal a decision of the Panel to the President through the National Security Advisor. The information shall remain classified pending a decision on the appeal.

Sec. 5.4, General Responsibilities. Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order;

(c) ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self inspection program, which shall include the regular reviews of representative samples of the agency's original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program;

(5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information be established before initiating administrative clearance procedures; and

(B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of:

(A) original classification authorities;
(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication;

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and

(10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.

Sec. 5.5. Sanctions. (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

PART 6 -- GENERAL PROVISIONS

Sec. 6.1. Definitions. For purposes of this order:

(a) "Access" means the ability or opportunity to gain knowledge of classified information.
(b) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) "Authorized holder" of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of this order.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Automatic declassification" means the declassification of information based solely upon:

1. the occurrence of a specific date or event as determined by the original classification authority; or

2. the expiration of a maximum time frame for duration of classification established under this order.

(f) "Classification" means the act or process by which information is determined to be classified information.

(g) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(h) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(i) "Classified national security information" or "classified information" means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(j) "Compilation" means an aggregation of preexisting unclassified items of information.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(m) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(n) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(o) "Derivative classification" means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(p) "Document" means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.
(q) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(r) "File series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) "Foreign government information" means:
(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "foreign government information" under the terms of a predecessor order.

(t) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.

(u) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a "violation," as defined below.

(v) "Integral file block" means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

(w) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(x) "Intelligence" includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

(y) "Intelligence activities" means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(z) "Intelligence Community" means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

(aa) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(bb) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

(cc) "National security" means the national defense or foreign relations of the United States.
(dd) "Need-to-know" means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(ee) "Network" means a system of two or more computers that can exchange data or information.

(ff) "Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(gg) "Original classification authority" means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(hh) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ii) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(ll) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(mm) "Senior agency official" means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(nn) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(oo) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(pp) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(qq) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(rr) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(ss) "U.S. entity" includes:
(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(tt) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(uu) "Weapons of mass destruction" means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

Sec. 6.2 General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Director of National Intelligence may, with respect to the Intelligence Community and after consultation with the heads of affected departments and agencies, issue such policy directives and guidelines as the Director of National Intelligence deems necessary to implement this order with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director of National Intelligence. Any such policy directives or guidelines issued by the Director of National Intelligence shall be in accordance with directives issued by the Director of the Information Security Oversight Office under section 5.1(a) of this order.

(c) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(d) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. The foregoing is in addition to the specific provisions set forth in sections 1.1(b), 3.1(c) and 5.3(e) of this order.

(e) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.
(f) This order shall be implemented subject to the availability of appropriations.

(g) Executive Order 12958 of April 17, 1995, and amendments thereto, including Executive Order 13292 of March 25, 2003, are hereby revoked as of the effective date of this order.

Sec. 6.3. Effective Date. This order is effective 180 days from the date of this order, except for sections 1.7, 3.3, and 3.7, which are effective immediately.

Sec. 6.4. Publication. The Archivist of the United States shall publish this Executive Order in the Federal Register.

BARACK OBAMA

THE WHITE HOUSE,
December 29, 2009.
June 9, 2011

**Purpose**

This guidance implements Executive Order 13556 of November 4, 2010 (the Order).

Section 2(c) of the Order provides that the National Archives and Records Administration (NARA) shall serve as the Executive Agent (EA) to implement the Order and monitor agency implementation. Section 4(b) of the Order also requires the EA, in consultation with affected agencies, to develop and issue such directives as are necessary to implement the Order.

**Scope**

This guidance applies to agencies that create or handle unclassified information requiring safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, or Government-wide policy.

**General Provisions**

**Establishment and Management of a CUI Program**

Agency heads shall establish and manage an agency CUI program that develops and implements agency procedures, roles, and responsibilities regarding CUI in accordance with the Order and this guidance, provides for required training for affected personnel regarding implementation and maintenance of the agency’s CUI program in accordance with this guidance, creates a self-inspection program to ensure compliance with the Order and this guidance, and designates a senior agency official to assist the agency head in CUI implementation and ensure compliance with the Order and this guidance.

**Designation of Categories**

Designation of information as CUI shall be limited to unclassified information requiring safeguarding or dissemination controls as set forth in law, regulation, or Government-wide
policy. Per section 3(b) of the Order, if there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

The EA shall establish the initial CUI categories based on agency submissions in accordance with sections 3(a)(2) and 4(a) of the Order.

Following initial designations, an agency head or the designated senior agency official may submit a written request to the EA for addition to or revision of existing CUI categories for review and approval. The request shall include the type of information within the agency that may meet the requirements for designation as CUI, along with a proposed marking, definition, and applicable decontrol period. Each request shall reference the authority for safeguarding or dissemination controls pursuant to law, regulation, or Government-wide policy upon which the request is based.

No safeguarding measures or limits on dissemination may be placed upon unclassified information as part of the conduct or reporting of federally-funded scientific research, except as provided in applicable statutes.

**CUI Registry**

Per section 4(d) of the Order, the EA shall establish and maintain a CUI registry to contain authorized CUI categories; subcategories (if necessary); citation of law, regulation, or Government-wide policy for each category; associated markings; applicable safeguarding and dissemination controls per associated authorities; and applicable decontrol requirements.

The registry shall also list sanctions specified in applicable statute or regulation along with their associated CUI categories.

The CUI registry shall be available on the NARA website to ensure public accessibility. CUI categories may not be used until the phased implementation date for marking, and the marking is approved and made available in the CUI registry.

**Markings**

CUI markings are intended to facilitate consistency in information sharing and a common understanding of safeguarding and dissemination controls.

CUI markings are the only markings authorized to designate unclassified information that requires safeguarding or dissemination controls. Such markings shall only be authorized when controls are required pursuant to and consistent with applicable law, regulations, and Government-wide policies.

Approved CUI markings shall be listed in the CUI registry.
All CUI markings shall be clearly applied and easily identified using the format in this guidance. Should there be extraordinary circumstances that require flexible marking practices, an agency head, or the designated senior agency official, shall submit a written request to the EA for consideration and approval of alternative methods.

The following shall be the only approved overall marking format for CUI:

CUI//Authorized Category-Subcategory (if necessary)

The EA, in consultation with affected agencies, shall issue guidance regarding the appropriate CUI markings and placement for various types of media.

Commingling CUI with classified national security information is authorized and when performed shall adhere to this guidance, as well as 32 C.F.R. Part 2001, or other issuances pursuant to Executive Order 13526 or a successor executive order.

**Portion Markings**

Portion marking is encouraged to facilitate information sharing and proper application of controls for CUI. Should agencies employ portion marking as a part of their information protection program, portion markings shall be placed before each section of the document containing CUI.

The following format shall be the only approved portion marking format for CUI:

(CUI//Authorized Category-Subcategory (if necessary))

**Re-marking of Legacy Material**

Agencies are not required to redact or re-mark legacy material when transferred to the physical or legal custody of NARA.

When legacy material is re-used, in whole or in part, legacy markings shall not be carried forward.

If a legacy document is re-used in its entirety and the information meets the standards for designation as CUI, any legacy markings shall be either struck through with a single straight line, or removed via electronic measures. Should striking through or removing the legacy marking not be practicable, an accompanying statement will indicate the appropriate CUI marking, and specify that the former marking is invalid. When legacy material is incorporated, paraphrased, or restated in part, the appropriate CUI marking shall be applied only if the information meets the requirements for designation as CUI.
**Safeguarding**

Agencies shall employ safeguarding measures and controls to protect CUI from unauthorized access, and to manage the risks associated with the processing, storage, handling, transmission, and destruction of CUI. Agencies shall ensure that all safeguarding measures are consistent with existing federal requirements and guidelines for CUI, including Office of Management and Budget (OMB) policies and National Institute of Standards and Technology (NIST) standards and guidelines, per section 6(a)(3) of the Order.

When law, regulation, or Government-wide policy mandates specific requirements for the safeguarding of a particular category or subcategory of CUI, these requirements shall be published in the CUI registry.

All persons responsible for the processing, storage, handling, transmission, or destruction of CUI shall take appropriate measures to prevent unauthorized access or use.

Agency-specific safeguarding controls that exceed those published in the CUI registry shall not be imposed on users outside of the implementing agency.

**Dissemination**

Should a law, regulation, or Government-wide policy include dissemination controls, these specific instructions shall be followed and made available for reference in the CUI registry. In the absence of specific dissemination controls per associated authorities, agencies shall disseminate CUI only to individuals who require the information for an authorized mission purpose.

The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to the Freedom of Information Act (FOIA), or any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches, in accordance with section 2(b) of the Order.

**Decontrol**

CUI shall be decontrolled as soon as possible when it no longer requires safeguarding measures and dissemination controls pursuant to its associated authorities. CUI may not be controlled indefinitely unless law, regulation, or Government-wide policy so stipulates. Each category in the registry shall indicate a specific time frame or event for applicable decontrol.

No action is necessary when CUI is decontrolled unless the information has been incorporated, restated, paraphrased, or re-used. In these cases, the CUI marking shall be either struck through with a single straight line, or removed via electronic measures.
Decontrol does not constitute public release of CUI. Public release shall be in accordance with law, regulation, and agency-specific procedures. CUI shall be decontrolled before, or no later than, the time of authorized public release.

**Education and Training**

At a minimum, agencies shall ensure that their personnel who create or handle CUI have a satisfactory knowledge and understanding of relevant CUI categories and associated markings, as well as applicable safeguarding, dissemination, and decontrol policies and procedures.

Initial and refresher training shall be tailored to meet the specific needs of the agency and the activities that personnel are expected to perform as determined by the individual agency. Agency programs developed pursuant to this guidance shall include the means, methods, and frequency for providing CUI training.

**Agency Self-Inspections**

Agency heads shall create a self-inspection program that adheres to the principles and requirements of the Order and this guidance, develop self-inspection methods, including reviews and assessments, to evaluate program effectiveness, measure the level of compliance with the Order and this guidance, and monitor the progress of CUI implementation. Agency self-inspection programs shall also integrate lessons learned from reviews and assessments to improve operational policies, procedures, and training, establish a system for corrective action to prevent and respond to non-compliance with the Order and this guidance, and provide documentation that reflects the analysis and conclusions of the self-inspection program to the EA on an annual basis and as requested by the EA.

**Executive Agent Responsibilities**

**Implementation**

The EA shall review compliance plans submitted by the agencies per sections 5(a) and 5(b) of the Order to monitor progress towards proper implementation of the Order and this guidance. Following this review, and in consultation with affected agencies and OMB, the EA shall establish deadlines for phased implementation based on agency submissions per section 5(b) of the Order.

The EA shall issue additional notices and guidance as needed for implementation of the Order, as well as for establishing and maintaining agency CUI programs. Such additional notices and guidance shall be developed in consultation with affected agencies as well as representatives of the public and State, local, tribal, and private sector partners.
Oversight

The EA shall conduct oversight to ensure that agencies have comprehensive programs in place for implementation of and compliance with the Order and this guidance. Upon request of the EA, agencies shall provide an update of CUI implementation efforts for subsequent reporting as required by section 5(c) of the Order. EA oversight may include conducting formal reviews, on-site liaison visits, and audits throughout the executive branch to evaluate agency CUI implementation, identifying information handling procedures or issues that require corrective actions, providing guidance and assistance, and conducting inquiries in response to pertinent notifications or complaints.

Additional Information

Dispute Resolution

Agencies involved in a dispute arising from an agency’s implementation of the Order and this guidance shall make every effort to resolve the dispute expeditiously. Disputes should be resolved within a mutually-agreed upon time period, taking into consideration the mission, sharing, and protection requirements of the parties concerned.

If agencies party to a dispute cannot reach a mutually acceptable resolution, the dispute may be referred to the EA. The EA shall act as the impartial arbiter of the dispute. If a party to the dispute is a member of the Intelligence Community, the EA shall consult with the Office of the Director of National Intelligence.

If the EA and an agency cannot reach an agreement on an issue related to the implementation of the Order or this guidance, an appeal may be made to the President through the Director of OMB for resolution per section 4(c) of the Order.

Transfer of Records to NARA

When records, as defined by 44 U.S.C. 3301, containing CUI are transferred to the physical or legal custody of NARA, the agency shall inform NARA of the continued control of such records through an indicator on the Records Transmittal and Receipt (SF-135) or the Agreement to Transfer Records to The National Archives of The United States (SF-258). Additionally, when a physical transfer of records occurs, the appropriate CUI marking shall be placed on the outside of the box to indicate that information designated as CUI is enclosed.

If such an indication is not made on one of the aforementioned forms, the information shall be presumed to have been decontrolled prior to transfer, regardless of any CUI markings on the records.
Definitions

Agency means any “Executive agency,” as defined in 5 U.S.C. 105, and the United States Postal Service; any “Military Department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that uses, handles, or stores CUI.

Associated authority means any law, regulation, or Government-wide policy that requires safeguarding and/or dissemination controls for such information that has been categorized as CUI.

Controlled Unclassified Information (CUI) means unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, and Government-wide policy.

CUI categories means the exclusive designations for identifying and organizing types of unclassified information that meet the standard for CUI.

CUI registry means the public listing of authorized CUI categories and subcategories, citations of applicable law, regulation, and Government-wide policy for each category, associated markings, and applicable safeguarding, dissemination, and decontrol requirements.

Decontrolled means that the information is no longer subject to CUI safeguarding and/or dissemination controls.

Dissemination means the authorized sharing of CUI amongst parties to include executive branch agencies and State, local, tribal, and private sector partners, but does not include disclosure in response to a request under the Freedom of Information Act.

Government-wide policy means a formal, written issuance including, but not limited to, an Executive Order, OMB policy, or NIST standards and guidelines that explicitly applies to executive branch agencies.

Information means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.

Legacy material means sensitive unclassified material that was previously marked under agency-specific marking practices.

Portion marking means placing a parenthetical symbol immediately preceding those sections of a document containing CUI to indicate the applicable CUI category.
Public Release means the act of making information available to the general public through the approved processes of an agency.

Safeguarding means measures and controls that are prescribed to protect CUI from unauthorized access and to manage the risks associated with processing, storage, handling, transmission, and destruction of CUI.

Please direct any questions regarding this Controlled Unclassified Information Office Notice to: cui@nara.gov.
Exemption 1

Exemption 1 of the Freedom of Information Act protects from disclosure information that has been deemed classified "under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy" and is "in fact properly classified pursuant to such Executive order." The Supreme Court has recognized that Congress intended for the President to bear immediate responsibility for protecting national security, which includes the development of policy that establishes what information must be classified to prevent harm to national security. Exemption 1, in turn, is the provision of the FOIA which affords protection for such properly classified information. The role of the federal judiciary includes the de novo review of an agency's Exemption 1 claims in litigation, with appropriate deference given to the Executive Branch's special expertise in matters of national security.


2 See, e.g., Dep't of the Navy v. Egan, 484 U.S. 518, 527-30 (1988) (discussing responsibility for protecting national security entrusted in the President as Commander in Chief of the military and as head of Executive Branch) (non-FOIA case).

3 See, e.g., Larson v. Dep't of State, 565 F.3d 857, 861 (D.C. Cir. 2009) (acknowledging that Exemption 1 protects information properly classified under national security executive order); Morley v. CIA, 508 F.3d 1108, 1123-24 (D.C. Cir. 2007) (same); Wolf v. CIA, 473 F.3d 370, 373 & n.3 (D.C. Cir. 2007) (same); Campbell v. DOJ, 164 F.3d 20, 29 (D.C. Cir. 1998) (same).

4 See, e.g., Ctr. for Nat'l Sec. Studies v. DOJ, 331 F.3d 918, 926-27 (D.C. Cir. 2003) (discussing deference shown to Executive Branch in national security matters) (Exemption 7(A)); Ray v. Turner, 537 F.2d 1187, 1190-95 (D.C. Cir. 1978) (discussing role of three branches of federal government in determining national security sensitivity); Cozen O'Connor v. U.S. Dep't of Treasury, 570 F. Supp. 2d 749, 773 (E.D. Pa. 2008) (noting that courts have "neither the expertise nor the qualifications to determine the impact upon national security" and that a "court must not substitute its judgment for the agency's regarding national defense or foreign (continued...)
Each President, beginning with President Harry S. Truman in 1951, has established the uniform policy of the Executive Branch concerning the protection of national security information with the issuance of a new or revised national security classification executive order. This classification executive order provides the procedural and substantive legal framework for the classification decisions of the designated subject matter experts who have been granted classification authority by the President. Exemption 1 provides for protection from disclosure for all national security information that has been properly classified in accordance with the substantive and procedural requirements of the current executive order. As such, Exemption 1 does not protect information that is merely "classifiable"—that is, meets the substantive requirements of the current such executive order but has not been actually reviewed and classified under it. Accordingly, to qualify for Exemption 1 protection, the information must actually satisfy all of the requirements for classification under the executive order.

The executive order in effect as of June 2009 is Executive Order 12,958, as amended, which is an amendment of an executive order first issued by President William J. Clinton in

---

4(continued)

policy implications" (citing Halperin v. CIA, 629 F.2d 144, 148 (D.C. Cir. 1980)).


10 See Exec. Order No. 12,958, as amended, §§ 1.1-4; see also NARA Classification Directive, 32 C.F.R. § 2001 (outlining procedural requirements for classification).
1995 and then revised by President George W. Bush on March 25, 2003. The provisions of this executive order are discussed below. On May 27, 2009, President Barack Obama issued a memorandum directing the Assistant to the President for National Security Affairs to consult with the relevant Executive Branch departments and agencies and to submit to the President within ninety days recommendations and proposed revisions to Executive Order 12,958, as amended.\(^\text{12}\)

The issuance of each classification executive order, or the amendment of an existing executive order, raises the question of the applicability of successive executive orders to records that were in various stages of administrative or litigative handling as of the current executive order's effective date.\(^\text{13}\) The general rule is that the appropriate executive order to apply, with its particular procedural and substantive standards, depends upon when the responsible agency official takes the final classification action on the record in question.\(^\text{14}\)

Under the precedents established by the Court of Appeals for the District of Columbia Circuit, the accepted rule is that a reviewing court will assess the propriety of Exemption 1 withholdings under the executive order in effect when "the agency's ultimate classification decision is actually made."\(^\text{15}\) Only when "a reviewing court contemplates remanding the case to the agency to correct a deficiency in its classification determination is it necessary\(^\text{16}\) to apply the standards of a superseding executive order. It also is important to note that some courts

\(^\text{11}\) See Exec. Order No. 12,958, as amended; see also, e.g., Larson, 566 F.3d at 863 (applying Executive Order 12,958, as amended); ACLU v. FBI, 429 F. Supp. 2d 179, 188 (D.D.C. 2006) (same); Judicial Watch v. DOJ, 306 F. Supp. 2d 58, 64-65 (D.D.C. 2004) (same).

\(^\text{12}\) Presidential Memorandum for Heads of Executive Departments and Agencies Concerning Classified Information and Controlled Unclassified Information, 74 Fed. Reg. 26277 (May 27, 2009) (outlining six topics that shall be considered during revision process).


\(^\text{14}\) See Halpern v. FBI, 181 F.3d 279, 289-90 (2d Cir. 1999); Campbell, 164 F.3d at 29 ("[A]bsent a request by the agency to reevaluate an Exemption 1 determination based on a new executive order . . . the court must evaluate the agency's decision under the executive order in force at the time the classification was made."); cf. Summers v. DOJ, 140 F.3d 1077, 1082 (D.C. Cir. 1998) (remanding to district court because district court failed to articulate whether it was applying Executive Order 12,356 or Executive Order 12,958 to evaluate Exemption 1 withholdings), on remand, No. 87-3168, slip op. at 2 (D.D.C. Apr. 19, 2000) (applying Executive Order 12,958 to uphold Exemption 1 withholdings).

\(^\text{15}\) King v. DOJ, 830 F.2d 210, 217 (D.C. Cir. 1987).

\(^\text{16}\) Id.; see also Campbell, 164 F.3d at 31 n.11 (recognizing that when court remands to agency for rereview of classification, such review is performed under superseding executive order); Greenberg v. U.S. Dept of Treasury, 10 F. Supp. 2d 3, 12 (D.D.C. 1998) (applying Executive Order 12,356 to records at issue, but noting that Executive Order 12,958 would apply if court "[f]ound that the agencies improperly withheld information pursuant to (continued...)

\(205\)
have permitted agencies, as a matter of discretion, to reexamine their classification decisions under a newly issued or amended executive order in order to take into account "changed international and domestic circumstances." 17

**Standard of Review**

In an early case that considered Executive Branch classification decisions made pursuant to a classification executive order, the Supreme Court held that records classified under proper procedures were exempt from disclosure per se, without the allowance for any further judicial review or in camera inspection. 18 The Supreme Court recognized that a great amount of deference should be accorded to the agency’s decision to protect national security information from disclosure, 19 an accepted doctrine that continues to this day. 20 Thereafter, however, Congress amended the FOIA in 1974 to provide expressly for de novo review by the courts and for in camera review of documents, including classified documents, where

16(...continued)
Exemption 1”.

17 *Baez v. DOJ*, 647 F.2d 1328, 1233 (D.C. Cir. 1980) (upholding agency’s classification reevaluation under executive order issued during course of district court litigation); see, e.g., *Miller v. U.S. Dept of State*, 779 F.2d 1378, 1388 (6th Cir. 1985) (agency chose to reevaluate under new Executive Order 12,356); *Military Audit Project v. Casey*, 656 F.2d 724, 737 & n.41 (D.C. Cir. 1981) (agency chose to reevaluate under new Executive Order 12,065); *Nat’l Sec. Archive v. CIA*, No. 99-1160, slip op. at 7 (D.D.C. July 31, 2000) ("[E]ven though the existence of [subject] documents was originally classified under Executive Order 12,356, the fact that they were reevaluated under Executive Order 12,958 means that Executive Order 12,958 controls."); *Keenan v. DOJ*, No. 94-1909, slip op. at 7 (D.D.C. Mar. 24, 1997) (finding that although agency could "voluntarily reassess" its classification decision under Executive Order 12,958, issued during pendency of lawsuit, agency not required to do so). But see *Wiener v. FBI*, No. 82-1720, slip op. at 3 (C.D. Cal. Aug. 25, 2005) (denying FBI’s request to reevaluate classified information under amended executive order after court’s earlier decision, and finding that FBI’s decision not to conduct such review earlier suggests that such reconsideration "was not crucial to national security’), *appeal dismissed per stipulation*, No. 05-56652 (9th Cir. Jan. 3, 2007).


19 Id. at 84, 94.

appropriate. In so doing, Congress sought to ensure that agencies properly classify national security records and that reviewing courts remain cognizant of their authority to verify the correctness of agency classification determinations.

The Court of Appeals for the District of Columbia Circuit has refined the appropriate standard for judicial review of national security claims under Exemption 1, finding that summary judgment is entirely proper if an agency's affidavits are reasonably specific and there is no evidence of bad faith. This review standard has been adopted by other circuit courts as well.


23 See, e.g., Larson v. Dep't of State, 565 F.3d 857, 865 (D.C. Cir. 2009) (holding that if agency affidavit contains "reasonable specificity" and "information logically falls within claimed exemption," then "court should not conduct a more detailed inquiry to test the agency's judgment"); Pub. Citizen v. Dep't of State, 276 F.3d 634, 645 (D.C. Cir. 2002) (finding agency's affidavits sufficiently detailed to support Exemption 1 witholding and determining that subsequent release of some previously classified information was not evidence of bad faith); Halperin v. CIA, 629 F.2d 144, 147-48 (D.C. Cir. 1980) (finding that summary judgment was appropriate where agency affidavits are sufficient and there is no indication of bad faith); El Badrawi v. DHS, 583 F. Supp. 2d 285, 314 (D.Conn. 2008) (holding that summary judgment is appropriate where agency has provided "detailed and specific information demonstrating both why the material has been kept secret and why such secrecy is allowed by the terms of an existing executive order" (citing N.Y. Times Co. v. DOD, 499 F. Supp. 2d 501, 510 (S.D.N.Y. 2007))); Schoenman v. FBI, 575 F. Supp. 2d 136, 153 (D.D.C. 2008) (suggesting that Court of Appeals for District of Columbia Circuit rule on reviewing propriety of agency's Exemption 1 assertion is "that little proof or explanation is required beyond a plausible assertion that information is properly classified"); N.Y. Times Co. v. DOD, 499 F. Supp. 2d 501, 511 (S.D.N.Y. 2007) (concluding that multiple declarations provided by defendants together adequately support summary judgment by describing records withheld and demonstrating that records were properly classified); Makky, 489 F. Supp. 2d at 441 (approving agency declaration containing "specific categories of classified information that were redacted on each document" and demonstrating that disclosure could identify "specific type of intelligence activity directed at a specific target; targets of foreign counterintelligence investigation; and intelligence information about or from a foreign country"); Summers v. DOJ, 517 F. Supp. 2d 231, 238 (D.D.C. 2007) (approving agency declaration containing "an extremely detailed description of each document, its classification level, the location on the document of each deletion made, and a description (to the extent possible) of the content of the deleted material"); Edmonds v. DOJ, 405 F. Supp. 2d 23, 33 (D.D.C. 2005) (explaining that "this court must respect the experience of the agency and stay within the proper limits of the judicial role in FOIA review").

24 See, e.g., Tavakoli-Nouri v. CIA, No. 00-3620, 2001 U.S. App. LEXIS 24676, at *9 (3d Cir. Oct. 18, 2001) (recognizing that courts give "substantial weight to agency's affidavit regarding details of classified status of a disputed document"); Maynard v. CIA, 986 F.2d 547, 555-56 & n.7 (1st Cir. 1993) (recognizing that courts must accord "substantial deference" to agency withholding determinations and "uphold the agency's decision" so long as withheld (continued...)}
Despite the courts' general reluctance to "second-guess" agency decisions on national security matters, agencies still have the responsibility to justify classification decisions in supporting affidavits. See In Exemption 1 cases, courts are likely to require that the affidavit be provided by an agency official with direct knowledge of the classification decision. Where agency affidavits have been found to be insufficiently detailed, courts have withheld summary judgment in Exemption 1 cases. When an affidavit contains sufficient explanation, however,

24(...continued)
information logically falls into the exemption category cited and there exists no evidence of agency "bad faith"; Bowers, 930 F.2d at 357 (stating that "[w]hat fact or bit of information may compromise national security is best left to the intelligence experts").

25 See Badrawi, 583 F. Supp. 2d at 314 (noting that agency "must provide detailed and specific information" justifying classification decision); N.Y. Times Co., 499 F. Supp. 2d at 611 (concluding that multiple declarations provided by defendants together adequately describe records withheld and adequately demonstrate that it was properly classified); ACLU v. DOJ, 321 F. Supp. 2d 24, 35 (D.D.C. 2004) (declaring that "it is not a question of whether the Court agrees with the defendant's assessment of the danger, but rather, 'whether on the whole record the Agency's judgment objectively survives the test of reasonableness, good faith, specificity, and plausibility in this field of foreign intelligence in which the [agency] is expert and given by Congress a special role'" (quoting Gardels v. CIA, 689 F.2d 1100, 1105 (D.C. Cir. 1982))).


27 See Halpern v. FBI, 181 F.3d 279, 293 (2d Cir. 1999) (declaring that agency's "explanations read more like a policy justification" for Executive Order 12,356, that the "affidavit gives no contextual description," and that it fails to "fulfill the functional purposes addressed in Vaughn"); Campbell v. DOJ, 164 F.3d 20, 31, 37 (D.C. Cir. 1998) (remanding to district court to allow the FBI to "further justify" its Exemption 1 claim because its declaration failed to "draw any connection between the documents at issue and the general standards that govern the national security exemption"); on remand, 193 F. Supp. 2d 29, 37 (D.D.C. 2001) (finding declaration insufficient where it merely concluded, without further elaboration, that "disclosure of [intelligence information] . . . could reasonably be expected to cause serious damage to the national security"); Oglesby v. U.S. Dept of the Army, 79 F.3d 1172, 1179-84 (D.C. Cir. 1996) (rejecting as insufficient certain Vaughn Indexes because agencies must itemize each document and adequately explain reasons for nondisclosure); Rosenfeld v. DOJ, 57 F.3d 803, 807 (9th Cir. 1995) (affirming district court disclosure order based upon finding that government failed to show with "any particularity" why classified portions of several documents should be withheld); Wiener v. FBI, 943 F.2d 972, 978-79 (9th Cir. 1991) (rejecting as inadequate agency justifications contained in coded Vaughn affidavits, based upon view (continued...)
it is generally accepted that "the court will not conduct a detailed inquiry to decide whether it agrees with the agency's opinions."^28

Deference to Agency Expertise

As indicated above, courts generally have heavily deferred to agency expertise in national security cases. The Court of Appeals for the District of Columbia Circuit has articulated an expansive standard of deference in national security cases, noting that "little proof or explanation is required beyond a plausible assertion that information is properly

^27(...)continued

that they consist of "boilerplate" explanations not "tailored" to particular information being withheld pursuant to Exemption 1); Singh v. FBI, 574 F. Supp. 2d 32, 50 (D.D.C. 2008) (withholding summary judgment in part because defendants failed to justify all exemption claims); Pipko v. CIA, 312 F. Supp. 2d 669, 674 (D.N.J. 2004) (commenting that agency affidavits must provide more than "merely glib assertions" to support summary judgment); Coldiron v. DOJ, 310 F. Supp. 2d 44, 52 (D.D.C. 2004) (observing that courts do not expect "anything resembling poetry," but nonetheless expressing dissatisfaction with agency's "cut and paste" affidavits).

^28Edmonds, 405 F. Supp. 2d at 33; see also Larson v. Dept of State, No. 02-1937, 2005 WL 3276303, at *11 (D.D.C. Aug. 10, 2005) (explaining that "[g]iven the weight of authority counseling deference . . . in matters involving national security, this court must defer to the agency's judgment"); Fla. Immigrant Advocacy Ctr. v. NSA, 380 F. Supp. 2d 1332, 1334 (S.D. Fla. 2005) (declaring that Exemption 1, properly applied, serves as "absolute bar" to release of classified information); Judicial Watch, Inc. v. U.S. Dept of Commerce, 337 F. Supp. 2d 146, 162 (D.D.C. 2004) (ruling that "a reviewing court is prohibited from conducting a detailed analysis of the agency's invocation of Exemption 1" (citing Halperin, 629 F.2d at 148)); Wolf v. CIA, 357 F. Supp. 2d 112, 116 (D.D.C. 2004) (commenting that "this Circuit has required little more than a showing that the agency's rationale is logical"), aff'd in pertinent part & remanded, 473 F.3d 370, 376 (D.C. Cir. 2007) (concluding that "[i]n light of the substantial weight accorded agency assertions of potential harm made in order to invoke the protection of FOIA Exemption 1, the [agency affidavit is] both logically and plausibly sufficient").

^29See, e.g., Students Against Genocide v. Dept of State, 257 F.3d 828, 837 (D.C. Cir. 2001) (holding that because courts lack expertise in national security matters, they must give "substantial weight to agency statements" (quoting Halperin v. CIA, 629 F.2d 144, 148 (D.C. Cir. 1980))); Bowers v. DOJ, 350 F.2d 350, 357 (4th Cir. 1991) (observing that "[w]hat fact . . . may compromise national security is best left to the intelligence experts"); Doherty v. DOJ, 775 F.2d 49, 52 (2d Cir. 1985) (according "substantial weight" to agency declaration); Taylor v. Dep't of the Army, 684 F.2d 99, 109 (D.C. Cir. 1982) (holding that classification affidavits are entitled to "the utmost deference"); Azmy v. DOD, 562 F. Supp. 2d 590, 597 (S.D.N.Y. 2008) (reiterating that agencies have "unique insights" in area of national security); ACLU v. DOJ, 429 F. Supp. 2d 179, 188 (D.D.C. 2006) (holding that court must recognize "unique insights and special expertise" of Executive Branch concerning the kind of disclosures that may be harmful).
Such deference is based upon the "magnitude of the national security interests and potential risks at stake," and it is extended by courts because national security officials are uniquely positioned to view "the whole picture" and "weigh the variety of subtle and complex factors" in order to determine whether the disclosure of information would damage national security. Indeed, courts ordinarily are very reluctant to substitute their judgment in place of the agency's "unique insights" in the areas of national defense and foreign relations. This is because courts have recognized that national security is a "uniquely

---

30 Morley v. CIA, 508 F.3d 1108, 1124 (D.C. Cir. 2007); see Larson v. Dept of State, 565 F.3d 857, 862 (D.C. Cir. 2009) (noting that court need only examine whether agency's classification decision "appears 'logical' or 'plausible'" (citing Wolf v. CIA, 473 F.3d 370, 374-75 (D.C. Cir. 2007))); James Madison Project v. CIA, 605 F. Supp. 2d 99, 109 (D.D.C. 2009) (commenting that D.C. Circuit rule is "that little proof or explanation is required beyond a plausible assertion that information is properly classified" (citing Morley, 508 F.3d at 1124); Schoenman v. FBI, 575 F. Supp. 2d 136, 153 (D.D.C. 2008) (same); Summers v. DOJ, 517 F. Supp. 2d 231, 238 (D.D.C. 2007) (citing Wolf, 473 F.3d at 374-75, for proposition that court need only determine whether agency's classification decision is "logical or plausible").

31 Ctr. for Nat'l Sec. Studies v. DOJ, 331 F.3d 918, 928 (D.C. Cir. 2003) (quoting CIA v. Sims, 471 U.S. 159, 179 (1985)) (Exemption 7(A)); see also L.A. Times Comm'n's, LLC v. Dept of the Army, 442 F. Supp. 2d 880, 899-900 (C.D. Cal. 2006) (deferring to judgment of senior Army officers regarding risks posed to soldiers and contractors by enemy forces in Iraq); ACLU v. DOD, 406 F. Supp. 2d 330, 333 (D.D.C. 2006) (acknowledging that "one may criticize the deference extended by the courts as excessive," but holding that such deference is the rule).

32 Sims, 471 U.S. at 179-80; see also, e.g., Zadvydas v. Davis, 533 U.S. 678, 696 (2001) (commenting that "terrorism or other special circumstances" may warrant "heightened deference") (non-FOIA case); Dept of the Navy v. Egan, 484 U.S. 518, 530 (1988) (explaining that "courts traditionally have been reluctant to intrude upon the authority of the executive in national security affairs") (non-FOIA case); Ctr. for Nat'l Sec. Studies, 331 F.3d at 918 (rejecting "artificial limits" on deference, and explaining that "deference depends on the substance of the danger posed by disclosure -- that is, harm to the national security -- not the FOIA exemption invoked").

33 Larson, 565 F.3d at 864; see also Assassination Archives & Research Ctr. v. CIA, 334 F.3d 55, 58 (D.C. Cir. 2003).

34 See, e.g., Maynard v. CIA, 986 F.2d 547, 556 n.9 (1st Cir. 1993) (stating that court "not in a position to 'second-guess'" agency's determination regarding need for continued classification of material); Krikorian v. Dept of State, 984 F.2d 461, 464-65 (D.C. Cir. 1993) (acknowledging agency's "unique insights" in areas of national defense and foreign relations and further explaining that because judges "lack the expertise necessary to second-guess ... agency opinions in the typical national security FOIA case," they must accord substantial deference to an agency's affidavit (quoting Halperin v. CIA, 629 F.2d 144, 148 (D.C. Cir. 1980))); Cozen O'Connor v. U.S. Dept of Treasury, 570 F. Supp. 2d 749, 773 (E.D. Pa. 2008) (finding that courts have "neither the expertise nor the qualifications to determine the impact upon national security" and that "court must not substitute its judgment for the agency's regarding national defense or foreign policy implications"); Summers, 517 F. Supp. 2d at 238 (noting that (continued...)
executive purview\textsuperscript{35} and that "the judiciary is in an extremely poor position to second-guess the executive's judgment" on national security issues.\textsuperscript{35}

Nevertheless, some FOIA plaintiffs have argued -- and in some cases courts have agreed -- that the nature of judicial review should involve questioning the underlying basis for the agency's classification decision.\textsuperscript{37} However, the majority of courts have rejected the idea that judicial review is to serve as a quality-control measure to reassure a doubtful requester.\textsuperscript{38} Further, courts have overwhelmingly rejected the notion that additional judicial

\textsuperscript{34}(...continued)

assessing potential for harm to intelligence source from disclosure "is the duty of the agency, and not the court"); \textit{ACLU v. FBI}, 429 F. Supp. 2d 179, 188 (D.D.C. 2006) (reasoning that "while a court is ultimately to make its own decision, that decision must take seriously the government's predictions" of harm to national security); \textit{Aftergood v. CIA}, No. 98-2107, 1999 U.S. Dist. LEXIS 18135, at *9-10 (D.D.C. Nov. 12, 1999) (declaring that courts must respect agency predictions concerning potential national security harm from disclosure, and recognizing that these predictions "must always be speculative to some extent"). But see \textit{King}, 830 F.2d at 226 (holding that trial court erred in deferring to agency's judgment that information more than thirty-five years old remained classified when executive order presumed declassification of information over twenty years old and agency merely indicated procedural compliance with order); \textit{Coldiron v. DOJ}, 310 F. Supp. 2d 44, 53 (D.D.C. 2004) (cautioning that court's deference should not be used as "wet blanket" to avoid proper justification of exemptions); \textit{Lawyers Comm. for Human Rights v. INS}, 721 F. Supp. 552, 561 (S.D.N.Y. 1989) (reminding that such deference does not give agency "carte blanche" to withhold responsive documents without "valid and thorough affidavit"); subsequent decision, No. 87-Civ-1115, slip op. at 1-2 (S.D.N.Y. June 7, 1990) (upholding Exemption 1 excisions after in camera review of certain documents and classified \textit{Vaughn} affidavit).

\textsuperscript{35}\textit{Ctr. for Nat'l Sec. Studies}, 331 F.3d at 927; see also \textit{LA Times Comm'n}s, 442 F. Supp. 2d at 899 (echoing the belief that national security is "a uniquely executive purview" (citing \textit{Zadvydas}, 533 U.S. at 696)).


\textsuperscript{37} See \textit{ACLU}, 429 F. Supp. 2d at 186 (concluding that "the importance of the issues raised by this case" make in camera review necessary); \textit{Fla. Immigrant Advocacy Ctr. v. NSA}, 380 F. Supp. 2d 1332, 1338 (S.D. Fla. 2005) (granting in camera review "to satisfy an 'uneasiness' or 'doubt' that the exemption claim may be overbroad given the nature of Plaintiff's arguments"); \textit{Wiener v. FBI}, No. 83-1720, slip op. at 3 (C.D. Cal. Sept. 27, 2004) (rejecting FBI's articulation of harm that would result from disclosure of classified information); \textit{ACLU v. DOD}, 339 F. Supp. 2d 501, 504 (S.D.N.Y. 2004) (finding that "[i]n our view, simply raising national security concerns [cannot] justify unlimited delay," and considering "the public's right to receive information on government activity in a timely manner").

\textsuperscript{38} See, e.g., \textit{Nat'l Sec. Archive Fund, Inc. v. CIA}, 402 F. Supp. 2d 211, 221 (D.D.C. 2005) (declining to conduct in camera review merely "to verify the agency's descriptions and provide (continued...)}
review should be triggered by a requester’s unsupported allegations of wrongdoing against
the government.\footnote{39}

When reviewing the propriety of agency classification determinations, courts have
demonstrated deference to agency expertise by according little or no weight to opinions of
persons other than the agency classification authority,\footnote{40} including persons who may have
previously maintained some knowledge of the subject matter while employed within the
Executive Branch.\footnote{41}

\footnote{(...continued)}

assurances, beyond a presumption of administrative good faith, to FOIA plaintiffs that the
descriptions are accurate and as complete as possible”\footnote{See Bassiouni \textit{v. CIA}, 392 F.3d 244, 247 (7th Cir. 2004) (commenting that “Exemption 1
would not mean much if all anyone had to do, to see the full list of the CIA’s holdings, was
allege that the agency had some documents showing how he ‘exercises rights guaranteed by
classification officer’s national security determination even though more than 100
ambassadors did not initially classify information); Van Atta \textit{v. Def. Intelligence Agency}, No. 87-1508, 1988 WL 73856, at *1-2 (D.D.C. July 6, 1988) (rejecting opinion of requester about
willingness of foreign diplomat to discuss issue); Wash. Post \textit{v. DOD}, No. 84-2949, 1987 U.S.
document in official capacity as member of Committee on Foreign Relations); \textit{cf. Lawyers
Dec. 18, 1991) (rejecting requester’s contention that officials of former Soviet Union consented
(D.D.C. 1991) (adjudging that "non-official releases" contained in books by participants
involved in Iranian hostage rescue attempt -- including ground assault commander and former
President Carter -- have "good deal of reliability" and require government to explain "how
official disclosure" of code names "at this time would damage national security").

\footnote{See, e.g., Hudson River Sloop Clearwater, Inc. \textit{v. Dept of the Navy}, 891 F.2d 414, 421-22
(2d Cir. 1989) (rejecting opinion of former admiral); Gardels \textit{v. CIA}, 689 F.2d 1100, 1106 n.5
(D.C. Cir. 1982) (rejecting opinion of former CIA agent); Berman \textit{v. CIA}, 378 F. Supp. 2d 1209,
1219 (E.D. Cal. 2005) (rejecting opinions of retired member of CIA’s Historical Advisory
Committee and former Special Assistant to the President of the United States); Rush \textit{v. Dept
of State}, 748 F. Supp. 1548, 1554 (S.D. Fla. 1990) (rejecting opinion of former ambassador who
had personally prepared some of records at issue); Pfeiffer \textit{v. CIA}, 721 F. Supp. 337, 340-41
(D.D.C. 1989) (rejecting opinion of former CIA staff historian).}
Agencies that classify national security information are sometimes unable to explain the basis for the classification decision on the public record without divulging the classified information itself. In these instances, courts have permitted or sometimes required agencies to submit explanatory in camera affidavits in order to protect the national security information that could not be discussed in a public affidavit. In camera affidavits have also been employed when even acknowledging the existence of records at issue would pose a threat to national security and consequently the agency has used the "Glomar" response to neither confirm nor deny the existence of records. If an agency submits an in camera affidavit, however, it is under a duty to "create as complete a public record as is possible" before doing so. This public record is intended to provide a meaningful and fair opportunity for a plaintiff

[43] See, e.g., Patterson v. FBI, 893 F.2d 595, 598-99 (3d Cir. 1990) (allowing in camera affidavit in order to supplement public affidavit and describe national security harm); Simmons v. DOJ, 796 F.2d 709, 711 (4th Cir. 1986) (same); Ingle v. DOJ, 698 F.2d 259, 264 (6th Cir. 1983) (same); Salisbury v. United States, 690 F.2d 966, 973 n.3 (D.C. Cir. 1982) (same); Stein v. DOJ, 662 F.2d 1245, 1255-56 (7th Cir. 1981) (same); Robinson v. FBI, No. 06-3359, 2008 WL 2502134, at *2-3 (E.D. Pa. June 20, 2008) (commenting that FBI public affidavits may need to be supplemented with in camera affidavit to fully articulate withholdings for proper review by court); Elec. Frontier Found. v. DOJ, No. 07-00403, slip op. at 11 (D.D.C. Aug. 14, 2007) (noting that agency’s filing of ex parte classified affidavit was appropriate, and would likely have been required by court had “agency not fortuitously proffered the classified declaration on its own”); Edmonds v. FBI, 272 F. Supp. 2d 35, 46 (D.D.C. 2003) (approving the use of an in camera affidavit, noting that “extensive public justification would threaten to reveal the very information for which a FOIA exemption is claimed”); Pub. Citizen v. Dep’t of State, 100 F. Supp. 2d 10, 27-28 (D.D.C. 2000) (ordering submission of an in camera affidavit because further description in a public affidavit "would reveal the [very] information the agency is trying to withhold"); Pub. Educ. Ctr., Inc. v. DOD, 905 F. Supp. 19, 22 (D.D.C. 1995) (ordering in camera affidavit because "extensive public justification would threaten to reveal the very information for which . . . [Exemption 1 was] claimed" (quoting Lykins, 725 F.2d at 1463)).

[44] See Phillipi v. CIA, 546 F.2d 1009, 1013 (D.C. Cir. 1976) (dealing with request for records regarding Glomar Explorer submarine-retrieval ship, so "neither confirm nor deny" response is now known as a "Glomar" response or as "Glomarization"); see also Hunt v. CIA, 981 F.2d 1116, 1119 (9th Cir. 1992) (noting that court accepted in camera affidavits to explain basis for Glomar assertion); Cozen O’Connor v. U.S. Dep’t of Treasury, 570 F. Supp. 2d 749, 786-87 (E.D. Pa. 2008) (explaining that "court may examine classified affidavits in camera if the public record is not sufficient to justify the Glomar response"); cf. El Badrawi v. DHS, 583 F. Supp. 2d 285, 315 (D.Conn. 2008) (finding that FBI had not supported its Glomar response with regard to Exemptions 2 and 7(E), and directing it to submit in camera affidavit).

[44] Phillipi, 546 F.2d at 1013; see also Armstrong v. Executive Office of the President, 97 F.3d 575, 580 (D.C. Cir. 1996) (holding that when district court uses an in camera affidavit, even in national security cases, “it must both make its reasons for doing so clear and make as much as possible of the in camera submission available to the opposing party” (citing Lykins v. DOJ, 725 F.2d 1455, 1465 (D.C. Cir. 1984))); Patterson, 893 F.2d at 600; Simmons, 796 F.2d at 710; Elec. Frontier Found., No. 07-00403, slip op. at 12 (D.D.C. Aug. 14, 2007) (recognizing (continued...)
to challenge, and an adequate evidentiary basis for a court to rule on, an agency's invocation of Exemption 1.\textsuperscript{45}

Courts have found that counsel for plaintiffs are not entitled to participate in such in camera proceedings.\textsuperscript{46} This was the case even in one unusual situation where plaintiff's counsel had been issued a personnel security clearance for an unrelated purpose.\textsuperscript{47} Many years ago, one court took the unprecedented step of appointing a special master to review and categorize a large volume of classified records.\textsuperscript{48} In other instances involving voluminous records, courts have on occasion ordered agencies to submit samples of the documents at issue for in camera review.\textsuperscript{49}

\textsuperscript{44}(...continued)

need for full public record to allow operation of adversarial process, but accepting necessity of district court's review of in camera affidavits to protect sensitive national security data; \textit{Scott v. CIA}, 916 F. Supp. 42, 48-49 (D.D.C. 1996) (denying request for in camera review until agency "creates as full a public record as possible").

\textsuperscript{45} See \textit{Campbell v. DOJ}, 164 F.3d 20, 30 (D.C. Cir. 1999) (requiring defendant to provide plaintiff with "a meaningful opportunity to contest, and the district court [with] an adequate foundation to review, the soundness of the withholding" (quoting \textit{King v. DOJ}, 830 F.2d 210, 218 (D.C. Cir. 1987))); \textit{Coldiron v. DOJ}, 310 F. Supp. 2d 44, 49 (D.D.C. 2004) (finding that agency "must provide a basis for a FOIA requester to contest, and the court to decide, the validity of the withholding"); \textit{ACLU v. DOJ}, 265 F. Supp. 2d 20, 27 (D.D.C. 2003) (acknowledging that agency affidavits "are entitled to substantial weight," but finding that they "must nevertheless afford the requester an ample opportunity to contest" them); cf. \textit{Lion Raisins Inc. v. USDA}, 354 F.3d 1072, 1083 (9th Cir. 2004) (approving the "use of in camera affidavits in order to supplement prior public affidavits that were too general," but rejecting the district court's use of in camera affidavits as "the sole factual basis for a district court's decision").

\textsuperscript{46} See \textit{Salisbury}, 690 F.2d at 973 n.3; \textit{Weberman v. NSA}, 668 F.2d 676, 678 (2d Cir. 1982); \textit{Hayden}, 608 F.2d at 1385-86; see also \textit{Ellsberg v. Mitchell}, 709 F.2d 51, 61 (D.C. Cir. 1983) (holding that plaintiff's counsel not permitted to participate in in camera review of documents arguably covered by state secrets privilege).

\textsuperscript{47} See \textit{El Badrawi v. DHS}, 596 F. Supp. 2d 389, 400 (D. Conn. 2009) (finding that although plaintiff's counsel maintained personnel security clearance, he did not have a "need to know" the withheld information, and thus failed to satisfy second requirement for access to classified information).


\textsuperscript{49} See, e.g., \textit{Wilson v. CIA}, No. 89-3356, 1991 WL 226682, at *3 (D.D.C. Oct. 15, 1991) (ordering in camera submission of "sample" of fifty documents because it was "neither necessary nor practicable" for court to review all 1000 processed ones).
Waiver of Exemption Protection

Several courts have had occasion to consider whether agencies have a duty to disclose classified information that purportedly has found its way into the public domain.\(^{50}\) This issue most commonly arises when a plaintiff argues that an agency has waived its ability to invoke Exemption 1 as a result of prior disclosure of similar or related information.\(^{51}\) In this regard, courts have held that, in making an argument of waiver through some prior public disclosure, a FOIA plaintiff bears "the initial burden of pointing to specific information in the public domain that appears to duplicate that being withheld."\(^{52}\)

\(^{50}\) See, e.g., Frugone v. CIA, 169 F.3d 772, 774 (D.C. Cir. 1999) (finding that disclosure made by employee of agency other than agency from which information is sought is not official and thus does not constitute waiver); Azmy v. DOD, 562 F. Supp. 2d 590, 598-99 (S.D.N.Y. 2008) (finding that although much may now be known by the public about subject, there has been no indication that this specific information has been disclosed).

\(^{51}\) See, e.g., Assassination Archives & Research Ctr. v. CIA, 334 F.3d 55, 60 (D.C. Cir. 2003) (holding that FOIA plaintiff must show that previous disclosure duplicates specificity of withheld material to establish waiver of exemptions, and determining that CIA's prior disclosure of some intelligence methods employed in Cuba does not waive use of exemptions for all such methods); Elec. Privacy Info Ctr. v. DOJ, 584 F. Supp. 2d 65, 71 (D.D.C. 2008) (ruling against waiver and rejecting contention that public availability of some information about Terrorist Surveillance Program diminishes government's argument for classification of remaining information); Wheeler v. CIA, 271 F. Supp. 2d 132, 140 (D.D.C. 2003) (rejecting plaintiff's contention that foreign nation's knowledge of past U.S. intelligence activities creates general waiver of all intelligence activities related to that nation).

\(^{52}\) Afshar v. Dep't of State, 702 F.2d 1125, 1130 (D.C. Cir. 1983); see also Morley v. CIA, 508 F.3d 1108, 1124 (D.C Cir. 2007) (ruling against waiver because plaintiff can not "point to specific information that was previously released and is now withheld"); James Madison Project v. NARA, No. 02-5089, 2002 WL 31296220, at *1 (D.C. Cir. Oct. 11, 2002) (affirming that the "party claiming that public disclosure prevents withholding the same information bears the burden of showing that the specific information at issue has been officially disclosed"); Pub. Citizen v. Dep't of State, 276 F.3d 634, 645 (D.C. Cir. 2002) (reaffirming that burden is on requester and rejecting plaintiff's waiver claim as "speculation" where plaintiff failed to demonstrate that specific information had been released into public domain, even though records were publicly accessible in NARA reading room upon request); Nat'l Sec. Archive Fund, Inc. v. CIA, 402 F. Supp. 2d 211, 222 (D.D.C. 2005) (ruling that plaintiff's "bald assertions" of public disclosure do not satisfy waiver standard); Ctr. for Int'l Envtl. Law v. Office of the U.S. Trade Representative, 237 F. Supp. 2d 17, 20 (D.D.C. 2002) (holding that plaintiff failed to show that information was in public domain when it merely pointed to other publicly available documents dealing with same general subject matter); Pfeiffer v. CIA, 721 F. Supp. 337, 342 (D.D.C. 1989) (holding that plaintiff must do more than simply identify "information that happens to find its way into a published account" to meet this burden). But see Wash. Post v. DOD, 766 F. Supp. 1, 12-13 (D.D.C. 1991) (suggesting that agency has ultimate burden of proof when comparing publicly disclosed information with information being withheld, determining whether information is identical and, if not, determining whether release of slightly different information would harm national security).
Courts have carefully distinguished between a bona fide declassification action or official release on the one hand and unsubstantiated speculation lacking official confirmation on the other, refusing to consider classified information to be in the public domain unless it has been officially disclosed.\(^{33}\) While this yields an especially narrow concept of "waiver" in the national security context, courts have recognized the importance of protecting sensitive national security information through such an approach.\(^{34}\) Indeed, this approach comports

\(^{33}\) See, e.g., Frugone, 169 F.3d at 775 (holding that letter from OPM advising plaintiff that his employment records were in CIA custody is not "tantamount to an official statement of the CIA"); Pub. Citizen v. Dept' of State, 11 F.3d 198, 201 (D.C. Cir. 1993) (holding that "an agency official does not waive FOIA Exemption 1 by publicly discussing the general subject matter of documents which are otherwise properly exempt from disclosure under that exemption"); Hoch v. CIA, No. 88-5422, 1990 WL 102740, at *1 (D.C. Cir. July 20, 1990) (concluding that without official confirmation, "clear precedent establishes that courts will not compel [an agency] to disclose information even though it has been the subject of media reports and speculation"); Abbots v. NRC, 765 F.2d 604, 607-08 (D.C. Cir. 1985) (reasoning that even if the withheld data were the same as an estimate in the public domain, that is not the same as knowing the NRC's official policy as to the "proper level of threat a nuclear facility should guard against"); Afshar, 702 F.2d at 1130-31 (observing that a foreign government can ignore "[u]nofficial leaks and public surmise . . . but official acknowledgment may force a government to retaliate"); Gerstein v. CIA, No. 06-4643, 2008 WL 4415080, at *6 (N.D. Cal. Sept. 26, 2008) (finding that agency is not required to confirm which particular reports of leaked information about satellite capabilities were accurate); Hiken v. DOD, 521 F. Supp. 2d 1047, 1059 (N.D. Cal. 2007) (ruling that agency not required to give "official confirmation" that information in public domain is classified); Edmonds v. FBI, 272 F. Supp. 2d 35, 49 (D.D.C. 2003) (holding that anonymous leak of information concerning FBI counterterrorism activities did not prevent agency from invoking exemption, because disclosures in tandem would amount to official confirmation of authenticity); Rubin v. CIA, No. 01 CIV 2274, 2001 WL 1537706, at *5 (S.D.N.Y. Dec. 3, 2001) (finding that plaintiff's mere showing that some private publication alleged that CIA maintained files on subject was not evidence of official disclosure and, therefore, that agency's "Glomar" position was not defeated); Wash. Post Co. v. DOD, No. 84-3400, slip op. at 3 (D.D.C. Sept. 22, 1986) (refusing to find official disclosure through abandonment of documents in Iranian desert following tragic and aborted 1980 military mission to rescue American hostages or through government's introduction of them into evidence in espionage trial); Schlesinger v. CIA, 591 F. Supp. 60, 66 (D.D.C. 1984) (rejecting contention that CIA prepublication review of former employees' books and articles serves as an official disclosure); cf. Hudson River Sloop Clearwater, Inc. v. Dept' of the Navy, 891 F.2d 414, 422 (2d Cir. 1989) (commenting that retired senior naval officer who was "no longer serving with an executive branch department cannot continue to disclose official agency policy" and "cannot establish what is agency policy"). But see Lawyers Comm. for Human Rights v. INS, 721 F. Supp. 552, 569 (S.D.N.Y. 1989) (ruling that Exemption 1 protection is not available when same documents were disclosed by foreign government or when same information was disclosed to media in "off-the-record exchanges").

\(^{34}\) See Frugone, 169 F.3d at 774 (ruling that disclosure made by employee from agency other than one from which information was sought is not official and thus does not constitute waiver); Edmonds v. DOJ, 405 F. Supp. 2d 23, 29 (D.D.C. 2005) (finding that even agency's disclosure to plaintiff's counsel during meeting does not constitute declassification action that (continued...
Waiver of Exemption Protection

with the amended Executive Order 12,958, which allows agencies to classify or reclassify information following an access request if it "has not previously been disclosed to the public under proper authority."\(^8\) (For a discussion of the requirements for such belated classification, see Exemption 1, Executive Order 12,958, as Amended, below.)

Courts have rejected the view that widespread reports in the media about the general subject matter involved are sufficient to overcome an agency's Exemption 1 claim for related records.\(^6\)

Another issue that has arisen in this regard has been the possible argument for waiver created when a government agency releases limited information on a subject while retaining additional information on the same subject as classified.\(^5\) The Court of Appeals for the District of Columbia Circuit has held that for information to be "officially acknowledged" in the context of Exemption 1, it must: (1) be as "specific" as the information previously released; (2) "match" the information previously disclosed; and (3) have been made public through an "official and documented" disclosure.\(^5\) Applying these criteria, the D.C. Circuit reversed the

\(^{54}\) (continued)

waives Exemption 1); Nat'l Sec. Archive v. CIA, No. 99-1160, slip op. at 12-13 (D.D.C. July 31, 2000) (ruling that Exemption 1 can be waived only through "the stamp of truth that accompanies official disclosure," even where requested information is otherwise "common knowledge in the public domain," and that "[d]isclosure by other agencies of CIA information does not preempt the CIA's ability to withhold that information").

\(^{55}\) Exec. Order No. 12,958, as amended, § 1.7(d).

\(^{56}\) See Azmy, 562 F. Supp. 2d at 598-99 (finding that although much may now be known by the public about former detainee, there has been no indication that this specific information has been officially disclosed); Elec. Frontier Found. v. DOJ, 532 F. Supp. 2d 22, 24 (D.D.C. 2009) (holding that newspaper article generally referring to existence of records on subject is not specific enough to waive exemptions); cf. Simmons v. DOJ, 796 F.2d 709, 712 (4th Cir. 1986) (ruling that there had been no "widespread dissemination" of information in question).

\(^{57}\) See, e.g., Elec. Privacy Info Ctr., 584 F. Supp. 2d at 71 (rejecting contention that public availability of some information about classified Terrorist Surveillance Program diminishes government's argument for classifying remaining information); Whalen v. U.S. Marine Corps, 407 F. Supp. 2d 54, 57 (D.D.C. 2005) (holding that the defendant agency's prior disclosures on a subject did not constitute a waiver of all information on that subject, and noting that "it seems equally as likely that the government's prior voluminous disclosures indicate diligent respect by the coordinate agencies to Executive Order 12,958 and bolster the defendant's position that it has withheld only that information which it must under the applicable exemptions").

\(^{58}\) Fitzgibbon v. CIA, 911 F.2d 755, 765 (D.C. Cir. 1990); see also Morley, 508 F.3d at 1124 (ruling against waiver because plaintiff did not "point to specific information that was previously released and is now withheld"); Wolf v. CIA, 473 F.3d 370, 378 (D.C. Cir. 2007) (reaffirming the rule in Fitzgibbon and the necessity of an "insistence on exactitude" when considering potential waiver of national security information and holding that in that case the
lower court's disclosure order and held that information published in a congressional report did not constitute "official acknowledgment" of the purported location of a CIA station, because the information sought related to an earlier time period than that discussed in the report.\footnote{59}

In so ruling, the D.C. Circuit did not address the question of whether congressional release of the identical information relating to intelligence sources and methods could ever constitute "official acknowledgment," thus requiring disclosure under the FOIA.\footnote{60} However, the D.C. Circuit had previously considered this question and had concluded that congressional publications do not constitute "official acknowledgment" for purposes of the FOIA.\footnote{61}

In a later decision, the D.C. Circuit had another opportunity to consider the issue of whether an agency had "waived" its ability to properly withhold records pursuant to Exemption 1. The case involved the question of whether the public congressional testimony of the U.S. Ambassador to Iraq constituted such a "waiver" so as to prevent the agency from invoking the FOIA's national security exemption to withhold related records.\footnote{62} The district court had held -- after reviewing the seven documents at issue in camera -- that the public testimony had not "waived" Exemption 1 protection because the "context" of the information

\footnote{58}{(...continued)}

"specific information at issue," i.e. the existence of particular records, had been officially acknowledged by the agency during congressional testimony); \textit{Students Against Genocide v. Dep't of State}, 257 F.3d 828, 835 (D.C. Cir. 2001) (holding that a prior release of photographs similar to those withheld did not waive Exemption 1, because the fact that "some information resides in the public domain does not eliminate the possibility that further disclosures can cause harm to [national security]" (quoting \textit{Fitzgibbon}, 911 F.2d at 766)); \textit{Elec. Frontier Found.}, 532 F. Supp. 2d at 24 (ruling against waiver because information in public domain is not as specific as information requested). \textit{But see Nat'l Sec. Archive, No. 99-1160, slip op. at 15-16 (D.D.C. July 31, 2000) (ordering CIA to disclose fact that it kept biographies on seven former East European heads of state because "Glomar" response was waived by CIA's 1994 admission that it kept biographies on all "heads of state" -- a "clear and narrowly defined term that is not subject to multiple interpretations," but noting that CIA's "Glomar" response otherwise would have been appropriate), reconsideration denied (D.D.C. Feb. 26, 2001).}

\footnote{59}{\textit{Fitzgibbon}, 911 F.2d at 765-66.}

\footnote{60}{\textit{Id}.}


\footnote{62}{\textit{Pub. Citizen v. Dep't of State}, 11 F.3d 198, 199 (D.C. Cir. 1993).}
in the documents was sufficiently "different" so as to not "negate" their "confidentiality." 63 Before the D.C. Circuit, the requester contended first that the court's prior decisions concerned attempts by FOIA requesters to compel agencies to confirm or deny the truth of information that others had already publicly disclosed. 64 The plaintiff then argued that the Ambassador's public statements about her meeting with the Iraqi leader prior to the invasion of Kuwait were far more detailed than those that the D.C. Circuit had found did not constitute "waiver" in previous cases. 65 The D.C. Circuit repudiated both of the requester's points and, in affirming the district court's decision, grounded its own decision in the fact that the requester "conceded" it could not "meet [the] requirement that it show that [the Ambassador's] testimony was 'as specific as' the documents it [sought] in this case, or that her testimony 'match[e[d]' the information contained in the documents. 66 Acknowledging that such a stringent standard is a "high hurdle for a FOIA plaintiff to clear," the D.C. Circuit concluded that the government's "vital interest in information relating to the national security and foreign affairs dictates that it must be." 67

The D.C. Circuit reasoned that to hold otherwise in a situation where the government had affirmatively disclosed some information about a classified matter would, in the court's view, give the agency "a strong disincentive ever to provide the citizenry with briefings of any kind on sensitive topics." 68 Indeed, in an opinion following this D.C. Circuit decision, the Court of Appeals for the Seventh Circuit reasoned that the public "is better off under a system that permits [the agency] to reveal some things without revealing everything; if even a smidgen of disclosure required [the agency] to open its files, there would be no smidgens." 69

In a case decided nearly a decade later, the D.C. Circuit once again visited the issue of claimed public disclosure of classified information. The district court earlier had rejected the plaintiff's waiver argument because the documents, while accessible, were not maintained

64 Pub. Citizen, 11 F.3d at 201-03.
65 Id. at 203.
66 Id.
67 Id.
68 Id.
69 Bassiouni v. CIA, 392 F.3d 244, 247 (7th Cir. 2004); see also ACLU v. DOD, 584 F. Supp. 2d 19, 25-26 (D.D.C. 2008) (holding that general public comment by agency officials on same topic did not waive Exemption 1 protection for more specific information on this topic); N.Y. Times Co. v. DOD, 499 F. Supp. 2d 501, 512-14 (S.D.N.Y. 2007) (affirming agency classification of Terrorist Surveillance Program information despite official acknowledgment that program exists). But see Wolf, 473 F.3d at 379-80 (remanding for determination of whether CIA Director's 1948 testimony before Congress, which was found to constitute "official acknowledgment" of "existence" of requested records, had also waived exemption protection for their "contents").
in a public access area and were not likely to have been accessed by a researcher.\textsuperscript{70} The district court had explained that such a "remote possibility of very limited disclosure" was not the type of "widespread" official dissemination capable of defeating an Exemption 1 claim.\textsuperscript{71} Agreeing with this, the D.C. Circuit ruled that the party claiming prior disclosure must point to "specific information in the public domain that appears to duplicate that being withheld,"\textsuperscript{72} to prevent the defendant agency from unrealistically having to bear 'the task of proving the negative.'\textsuperscript{73} The D.C. Circuit concluded that the plaintiff had failed to meet this burden, and it dismissed the public disclosure claim as nothing more than "speculation."\textsuperscript{74} (For a further discussion of this issue, see Discretionary Disclosure and Waiver, below.)

Finally, as one court has phrased it, classified information will not be released under the FOIA even to a requester of "unquestioned loyalty."\textsuperscript{75} In another decision concerning this issue, a court specifically held that a government employee who requested information and who also held a current "Top Secret" security clearance was properly denied access to classified records concerning himself because Exemption 1 protects 'information from disclosure based on the nature of the material, not on the nature of the individual requester.'\textsuperscript{76}

\textbf{Executive Order 12,958, as Amended}

As mentioned above, as of June 2009, Executive Order 12,958, which was amended on March 25, 2003,\textsuperscript{77} sets forth the standards governing national security classification and the mechanisms for declassification. As with prior executive orders, the amended Executive Order 12,958 recognizes both the right of the public to be informed about activities of its government and the need to protect national security information from unauthorized or

\begin{itemize}
\item \textsuperscript{70} Pub. Citizen v. Dept of State, 100 F. Supp. 2d 10, 29 (D.D.C. 2000).
\item \textsuperscript{71} Id. at 28-29.
\item \textsuperscript{72} Pub. Citizen, 276 F.3d at 645 (quoting Afshar, 702 F.2d at 1129).
\item \textsuperscript{73} Id. (quoting Davis v. DOJ, 968 F.2d 1276, 1279 (D.C. Cir. 1992)).
\item \textsuperscript{74} Id.
\item \textsuperscript{75} Levine v. DOJ, No. 83-1685, slip op. at 6 (D.D.C. Mar. 30, 1984) (concluding that regardless of a requester's loyalty, the release of documents to him could "open the door to secondary disclosure to others").
\item \textsuperscript{76} Martens v. U.S. Dept of Commerce, No. 88-3334, 1990 U.S. Dist. LEXIS 10351, at *10 (D.D.C. Aug. 6, 1990); see also Miller v. Casey, 730 F.2d 773, 778 (D.C. Cir. 1984) (accepting that plaintiff's security clearance was not an issue in denying access to requested information); cf. DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 771 (1989) (stating that "the identity of the requester has no bearing on the merits of his or her FOIA request") (Exemption 7(C)).
\end{itemize}
untimely disclosure. Accordingly, under Executive Order 12,958, as amended, information may not be classified unless "the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism." Courts have consistently recognized that an agency's articulation of the threatened harm to national security must always be speculative to some extent and that to require a showing of actual harm would be judicial "overstepping." Courts have routinely accepted that certain types of information have national security sensitivity. In the area of intelligence sources and methods, for example, courts are strongly inclined to accept the agency's position that disclosure of this type of information will cause damage to national security interests because this is "necessarily a region for forecasts in which [the agency's] informed judgment as to potential future harm should be respected."

Section 1.4 of Executive Order 12,958, as amended, specifies the types of information that may be considered for classification. No other types of information may be classified pursuant to the executive order. The information categories identified as proper bases for classification in the amended Executive Order 12,958 consist of:

(1) foreign government information;

---

78 See Exec. Order No. 12,958, as amended (commenting in introductory statement that "our Nation's progress depends on the free flow of information").

79 Id. § 1.1(a)(4); see also NARA Classification Directive, 32 C.F.R. § 2001.10(c) (2008) (explaining that ability of agency classifier to identify and describe damage to national security caused by unauthorized disclosure is critical aspect of classification system).

80 Halperin v. CIA, 629 F.2d 144, 149 (D.C. Cir. 1980); see Aftergood v. CIA, No. 98-2107, 1999 U.S. Dist. LEXIS 18135, at *9 (D.D.C. Nov. 12, 1999) (declaring that "the law does not require certainty or a showing of harm" that has already occurred); cf. ACLU v. DOJ, 265 F. Supp. 2d 20, 30 (D.D.C. 2003) (reiterating that "[t]he test is not whether the court personally agrees in full with the [agency's] evaluation of the danger -- rather, the issue is whether on the whole record the Agency's judgment objectively survives the test of reasonableness, good faith, specificity, and plausibility in this field of foreign intelligence in which the [agency] is expert" (quoting Gardels v. CIA, 689 F.2d 1100, 1105 (D.C. Cir. 1982))).

81 Gardels v. CIA, 689 F.2d 1100, 1106 (D.C. Cir. 1982); see also Bassiouni v. CIA, 392 F.3d 244, 245 (7th Cir. 2004) (commenting that to protect sources, intelligence agencies must often protect "how" a document came to its records system, because "in the intelligence business, 'how' often means 'from whom'"); Wash. Post v. DOD, 766 F. Supp. 1, 7 (D.D.C. 1991) (observing that disclosure of the working files of a failed Iranian hostage rescue attempt containing intelligence planning documents would "serve as a model of 'do's and don't's" for future counterterrorist missions "with similar objectives and obstacles").

82 See Exec. Order No. 12,958, as amended, § 1.4(a)-(g).

83 See id.

84 See id. § 1.4(b); see also Peltier v. FBI, 218 F. App'x 30, 31 (2d Cir. 2007) (holding that disclosure of foreign government information "would breach express promises of (continued...)
(2) vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security;\(^{85}\)

(3) intelligence activities, sources, or methods;\(^{86}\)

\(^{84}(...continued\)

confidentiality made to a foreign government, on which the provision of the information was expressly contingent); Miller v. DOJ, 562 F. Supp. 2d 82, 102 (D.D.C. 2008) (finding that disclosure of foreign government information would show that government's cooperation, capabilities and vulnerabilities, and would lead to negative diplomatic consequences and diminished intelligence capabilities); Azmy v. DOD, 562 F. Supp. 2d 590, 600 (S.D.N.Y. 2008) (holding that agency properly classified foreign government information and that disclosure could be expected to "impair DOD's ability to obtain information from foreign governments in the future, who will be less likely to cooperate with the United States if they cannot be confident that the information they provide will remain confidential").


\(^{86}\) See Exec. Order No. 12,958, as amended, § 1.4(c); see also Schrecker v. DOJ, 254 F.3d 162, 166 (D.C. Cir. 2001) (protecting intelligence sources because release would harm national security by "dissuading current and future sources from cooperating"); Jones v. FBI, 41 F.3d 238, 244 (6th Cir. 1994) (protecting "numerical designators" assigned to national security sources) (decided under Executive Order 12,356); Patterson v. FBI, 893 F.2d 595, 597, 601 (3d Cir. 1990) (protecting information concerning intelligence sources and methods FBI used in investigation of student who corresponded with 169 foreign nations) (decided under Executive Order 12,356); Singh v. FBI, 574 F. Supp. 2d 32, 42-43 (D.D.C. 2008) (holding that FBI properly classified "numerical designator, which serves as a singular identifier for an intelligence source" because disclosure could permit hostile intelligence operation to glean source's identity); Schoenman v. FBI, 575 F. Supp. 2d 136, 153, 156 (D.D.C. 2008) (noting that intelligence sources "can be expected to furnish information only when confident that they are protected from retribution," and finding that disclosure of source information "regardless of whether they are active or inactive, alive or deceased, can reasonably be expected to jeopardize' the safety of the source or his or her family"); Cozen O'Connor v. U.S. Dept of Treasury, 570 F. Supp. 2d 749, 774 (E.D. Pa. 2008) (agreeing that agency had properly classified information received through confidential sources because disclosure of source-provided data could "circumvent current and future investigations of known and suspected terrorists"); Azmy, 562 F. Supp. 2d at 599 (finding that agency properly withheld "intelligence (continued...)}
(4) cryptology;\footnote{\textit{...continued}}

(5) foreign relations or foreign activities, including confidential sources;\footnote{\textit{...continued}}

\footnote{assessments and conclusions" because disclosure would reveal which sources they find credible and which sources they discredit, and how they reach their intelligence conclusions); \textit{Miller}, 562 F. Supp. 2d at 105 (finding that FBI properly classified detailed information provided by human intelligence source, and noting that "[i]n certain parts of the world, the consequences of public disclosure to an individual that has served as a U.S. source are often swift and far reaching, from economic reprisals to possible harassment, imprisonment, or even death"); \textit{Rubin v. CIA}, No. 01-CIV-2274, 2001 WL 1537706, at *3 (S.D.N.Y. Dec. 3, 2001) (holding that CIA properly refused to confirm or deny existence of records concerning two deceased British poets, because "intelligence collection may be compromised if sources are not confident that . . . their cooperation will remain forever secret"); \textit{cf. Schrecker v. DOJ}, 14 F. Supp. 2d 111, 117-18 (D.D.C. 1998) (observing that identities of intelligence sources are protectible pursuant to Exemption 1 regardless of whether individuals are alive or deceased), summary judgment granted, 74 F. Supp. 2d 26 (D.D.C. 1999), aff'd, 254 F.3d 162 (D.C. Cir. 2001).

\footnote{See Exec. Order No. 12,958, as amended, § 1.4(c); \textit{see also McDonnell v. United States}, 4 F.3d 1227, 1244 (3d Cir. 1993) (upholding classification of cryptographic information dating back to 1934 when release "could enable hostile entities to interpret other, more sensitive documents similarly encoded") (decided under Executive Order 12,356); \textit{Gilmore v. NSA}, No. C92-3646, 1993 U.S. Dist. LEXIS 7694, at *18-19, *22-23 (N.D. Cal. May 3, 1993) (finding mathematical principles and techniques in agency treatise protectible under this executive order category) (decided under Executive Order 12,356).

\footnote{See Exec. Order No. 12,958, as amended, § 1.4(d); \textit{see also Pelier}, 218 F. App'x at 31 (finding that disclosure would "reveal an intelligence relationship and could threaten the flow of information" between governments); \textit{Bassiouni}, 392 F.3d at 246 (observing that ",even allies could be unpleasantly surprised" by disclosure of CIA espionage information involving one of its citizens); \textit{Schoeneman}, 575 F. Supp. 2d at 153 (holding that intelligence agency properly classified "deliberative descriptions, commentary, and analysis on [foreign] government and defense establishment" because disclosure would damage "working relationship" and lead to less effective foreign intelligence collection); \textit{Miller}, 562 F. Supp. 2d at 102-04, 107 (finding that declarants had properly demonstrated potential for harm to foreign relations in disclosing information concerning foreign cooperation in plans to evacuate American citizens and an assessment of that foreign government's military and police capabilities); \textit{Wheeler v. DOJ}, 403 F. Supp. 2d 1, 12 (D.D.C. 2005) (holding that "foreign relations between Cuba and the United States remain tenuous at best," and that it would follow that information about persons in Cuba who provided information to the United States could still be very dangerous and, if disclosed, result in "embarrassment or imprisonment, if not death"); \textit{ACLU v. DOD}, 389 F. Supp. 2d 547, 561 (S.D.N.Y. 2005) (reasoning that "even if the only question was whether to recognize officially which was informally or unofficially believed to exist, the niceties of international diplomacy sometimes make it important not to embarrass a foreign country or its leaders, and exemptions from FOIA protect that concern as well"); \textit{Wolf v. CIA}, 357 F. Supp. 2d 112, 116 (D.D.C. 2004) (reasoning that the fact of the CIA's covert interest in a foreign (continued...)}
(6) military plans, weapons, or operations; 89

(7) scientific, technological, or economic matters relating to national security; 90 and

(8) government programs for safeguarding nuclear materials and facilities. 91

The amendment of Executive Order 12,958 also added a new classification category protecting information concerning "weapons of mass destruction," 92 and it further expanded two previously existing categories to include information regarding "defense against transnational

89(...continued)
citizen "could adversely affect relations with a foreign government because that government might believe that the CIA has collected intelligence information on a recruited one of its citizens or resident aliens"), aff'd in pertinent part & remanded on other grounds, 473 F.3d 370, 377-80 (D.C. Cir. 2007); Linn v. DOJ, No. 92-1406, 1995 WL 631847, at *26 (D.D.C. Aug. 22, 1995) (finding Exemption 1 withholdings proper because the agency demonstrated that it has "a present understanding" with the foreign government that any shared information will not be disclosed) (decided under Executive Order 12,356). But see Keenan v. DOJ, No. 94-1909, slip op. at 9-11 (D.D.C. Dec. 16, 1997) (ordering release of document segments withheld by the agency pursuant to Exemption 1, because the agency failed to show that the foreign governments named in documents more than thirty years old "still wish to maintain the secrecy of their cooperative efforts with the U.S.").


90 See Exec. Order No. 12,958, as amended, § 1.4(e).

91 See id. § 1.4(f); see also Weinberger v. Catholic Action of Haw., 454 U.S. 139, 144-45 (1981) (protecting "information relating to the storage of nuclear weapons"); Abbots v. NRC, 766 F.2d 604, 607 (D.C. Cir. 1985) (protecting "the NRC's determination as to the number of attackers a nuclear facility should be able to defend against successfully," because release of this information would allow potential attackers to "compute the size of the assault force needed for optimum results") (decided under Executive Order 12,356); Loomis v. DOE, No. 96-149, 1999 WL 33541935, at *6 (N.D.N.Y. Mar. 9, 1999) (protecting nuclear containment layout plan and referenced document on propagation of radiological requirements and procedures) (decided under original version of Executive Order 12,958), summary affirmance granted, 21 F. App'x 80 (2d Cir. 2001).

92 See Exec. Order No. 12,958, as amended, § 1.4(h).
Executive Order 12,958, as Amended, also established a presumption of harm to national security from the release of information provided by or related to foreign governments.\textsuperscript{94}

As with prior orders, the amended Executive Order 12,958 contains a number of distinct limitations on classification.\textsuperscript{95} Specifically, information may not be classified in order to:

1. conceal violations of law, inefficiency, or administrative error;\textsuperscript{96}
2. prevent embarrassment to a person, organization, or agency;\textsuperscript{97}
3. restrain competition;\textsuperscript{98}
4. prevent or delay the disclosure of information that does not require national security protection;\textsuperscript{99} or
5. protect basic scientific research not clearly related to the national security.\textsuperscript{100}

Additionally, the amendment of Executive Order 12,958 removed the requirement in the original version of the order that agency classification authorities not classify information if

\textsuperscript{93} See id. § 1.4(e), (g); see also id. § 1.1(a)(4) (incorporating "defense against transnational terrorism" into classification standards).

\textsuperscript{94} See id. § 1.1(c).

\textsuperscript{95} See id. § 1.7.

\textsuperscript{96} See id. § 1.7(a)(1); see also Billington, 11 F. Supp. 2d at 57-58 (dismissing plaintiff's "unsubstantiated accusations" that information should be disclosed because FBI engaged in illegal "dirty tricks" campaign).

\textsuperscript{97} See Exec. Order No. 12,958, as amended, § 1.7(a)(2); see also Billington, 11 F. Supp. 2d at 58-59 (rejecting plaintiff's argument that information was classified by FBI to shield agency and foreign government from embarrassment); Canning v. DOJ, 848 F. Supp. 1037, 1047-48 (D.D.C. 1994) (finding no credible evidence that the FBI improperly withheld information to conceal the existence of "potentially inappropriate investigation" of a French citizen, and noting that "if anything, the agency released sufficient information to facilitate such speculation") (decided under Executive Order 12,356).

\textsuperscript{98} See Exec. Order No. 12,958, as amended, § 1.7(a)(3).

\textsuperscript{99} See id. § 1.7(a)(4).

\textsuperscript{100} See id. § 1.7(b).
there is "significant doubt" about the national security harm.  

Following the amendment of Executive Order 12,958, and subject to strict conditions, agencies may reclassify information after it has been declassified and released to the public. The action must be taken under the "personal authority of the agency head or deputy agency head," who must determine in writing that the reclassification is necessary to protect national security. Further, the information previously declassified and released must be "reasonably recovered" by the agency from public holders, and it must be withdrawn from public access in archives. Finally, the agency head or deputy agency head must report any agency reclassification action to the Director of the Information Security Oversight Office within thirty days, along with a description of the agency's recovery efforts, the number of public holders of the information, and the agency's efforts to brief any such public holders. Similarly, the amended Executive Order 12,958 also authorizes the classification of a record after an agency has received a FOIA request for it, although such belated classification is permitted only through the "personal participation" of designated high-level officials and only on a "document-by-document basis." (For a further discussion of official disclosure, see Exemption 1, Waiver of Exemption Protection, above, and Discretionary Disclosure and Waiver, below.)

Executive Order 12,958, as amended, also contains a provision establishing a mechanism through which classification determinations can be challenged within the federal government. Furthermore, agencies are required to set up internal procedures to implement this program, in order to ensure that holders are able to make such challenges without fear of retribution and that the information in question is reviewed by an impartial official or panel. Additionally, an agency head or designee may authorize an "emergency" disclosure

---

101 See id.

102 See id. § 1.7(c).

103 Id. § 1.7(c)(1); see also NARA Classification Directive, 32 C.F.R. § 2001.13(a) (2008) (directive issued by Information Security Oversight Office describing procedures for reclassifying information pursuant to section 1.7(c) of Executive Order 12,958, as amended).

104 Exec. Order 12,958, as amended, § 1.7(c)(2); see also NARA Classification Directive, 32 C.F.R. § 2001.13(a)(1).

105 See Exec. Order 12,958, as amended, § 1.7(c)(3); see also NARA Classification Directive, 32 C.F.R. § 2001.13(b).

106 Exec. Order No. 12,958, as amended, § 1.7(d); see also NARA Classification Directive, 32 C.F.R. § 2001.13(a); see, e.g., Pub. Citizen v. Dept. of State, 100 F. Supp. 2d 10, 26 (D.D.C. 2000) (finding that agency official had "power to classify documents" following receipt of FOIA request) (decided under original version of Executive Order 12,958), aff'd on other grounds, 276 F.3d 674 (D.C. Cir. 2002).

107 See Exec. Order No. 12,958, as amended, § 1.8.

108 See id. § 1.8(b); see also id. § 5.3(b) (authorizing Interagency Security Classification Appeals Panel to "decide on [sic] appeals by persons who have filed classification (continued...)
of information to individuals who are not eligible for access to classified information, as may be necessary under exceptional circumstances "to respond to an imminent threat to life or in defense of the homeland."\(^\text{109}\)

In addition to satisfying the substantive criteria outlined in the applicable executive order, information also must adhere to the order's procedural requirements to qualify for Exemption 1 protection.\(^\text{109}\) In other words, the information has to be more than "classifiable" under the executive order -- it has to be actually classified under the order.\(^\text{111}\) This requirement recognizes that proper classification is actually a review process to identify potential harm to national security.\(^\text{112}\) Executive Order 12,958, as amended, prescribes the current procedural requirements that agencies must employ.\(^\text{113}\) These requirements include such matters as the proper markings to be applied to classified documents,\(^\text{114}\) as well as the manner in which agencies designate officials to classify information in the first instance.\(^\text{115}\)

Regarding proper national security markings, Executive Order 12,958, as amended,

\(^{108}\) (...continued)

challenges"; NARA Classification Directive, 32 C.F.R. § 2001.14 (describing procedures that agencies must establish in order to consider classification challenges).

\(^{109}\) See Exec. Order No. 12,958, as amended, § 4.2(b) (providing that an emergency disclosure does not constitute declassification); see also NARA Classification Directive, 32 C.F.R. § 2001.51 (describing transmission and reporting procedures for disclosure "in emergency situations, in which there is an imminent threat to life or in defense of the homeland").

\(^{110}\) See, e.g., Schoenman, 575 F. Supp. 2d at 151-52 (holding that agencies asserting Exemption 1 are required to "show both that the information was classified pursuant to the proper procedures, and that the withheld information substantively falls within the scope of [the applicable] Executive Order").

\(^{111}\) See, e.g., Exec. Order No. 12,958, as amended, §§ 1.1-.4, 1.6; see also NARA Classification Directive, 32 C.F.R. § 2001.10-.11, .20-.21, .23.

\(^{112}\) See, e.g., Hayden v. NSA, 608 F.2d 1381, 1386-87 (D.C. Cir. 1979) (finding that information must have been classified according to procedures outlined in national security classification executive order).

\(^{113}\) See, e.g., Exec. Order No. 12,958, as amended, §§ 1.5, 1.6, 2.1; see also NARA Classification Directive, 32 C.F.R. § 2001.20-.24.

\(^{114}\) See Exec. Order No. 12,958, as amended, § 1.6; see also Cohen v. FBI, No. 93-1701, at 5-6 (D.D.C. Oct. 11, 1994) (rejecting plaintiff's argument that subsequent marking of two documents during agency's second classification review rendered FBI's classification action ineffective; to require agencies "to perform every classification review perfectly on the first attempt" would be "a very strict and unforgiving standard") (decided under Executive Order 12,356).

\(^{115}\) See Exec. Order No. 12,958, as amended, § 1.3.
requires that each classified document be marked with the appropriate classification level, the identity of the original classification authority, the identity of the agency and office classifying the document, as well as with "a concise reason for classification" that cites the applicable classification category or categories. It also requires that a date or event for declassification be specified on the document. In addition, amended Executive Order 12,958 requires agencies to use portion markings to indicate levels of classification within documents, and it advocates the use of classified addenda in cases in which classified information comprises only "a small portion of an otherwise unclassified document." The Information Security Oversight Office (ISOO) has issued governmentwide guidelines on these marking requirements.

Executive Order 12,958 also establishes a government entity to provide oversight of agencies' classification determinations and their implementation of the order. The Interagency Security Classification Appeals Panel consists of senior-level representatives of the Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs. Among other things, this body adjudicates classification challenges filed by agency employees and decides appeals from persons who have filed requests under the mandatory declassification review provisions of the order.

---

116 See id. § 1.6(a)(1); see also id. § 1.2 (authorizing classification at the following levels, and using these descriptive terms only: (1) "Top Secret" level, when disclosure could be expected to cause "exceptionally grave damage" to the national security; (2) "Secret" level, when disclosure could be expected to cause "serious damage" to the national security; and (3) "Confidential" level, when disclosure could be expected to cause "damage" to the national security).

117 See id. § 1.6(a)(2).

118 See id. § 1.6(a)(3).

119 Id. § 1.6(a)(5).

120 See id. § 1.6(a)(4).

121 See id. § 1.6(c).

122 Id. § 1.6(g).


125 See Exec. Order No. 12,958, as amended, § 5.3(b); see also id. § 3.5 (establishing mandatory declassification review program as non-FOIA mechanism for persons to seek access to classified information generated or maintained by agencies, including papers (continued...))
Agencies with questions about the proper implementation of the substantive or procedural requirements of Executive Order 12,958, as amended, may consult with the Information Security Oversight Office, located within the National Archives and Records Administration, which holds governmentwide oversight responsibility for classification matters under Executive Order 12,958, as amended, by telephone at (202) 357-5250.126

**Duration of Classification and Declassification**

Other important provisions of amended Executive Order 12,958 are those that establish (1) limitations on the length of time information may remain classified,127 and (2) procedures for the declassification of older government information.128 The order requires agencies to "attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity."129 The order also limits the duration of classification to no longer than is necessary in order to protect national security.130 If the agency is unable to determine a date or event that will trigger declassification, however, then amended Executive Order 12,958 instructs the original classification authority to set a ten-year limit on new classification actions.131 The classification authority alternatively may determine that the sensitivity of the information justifies classification for a period of twenty-five years.132

The amendment of Executive Order 12,958 also continues the automatic declassification mechanism that was established by the original version of the order in 1995.133 The automatic declassification mechanism applies to information currently classified under any predecessor

---

126 (...continued) maintained by presidential libraries not yet accessible under FOIA).

127 See id. § 5.2.


129 id. § 1.5(a).

130 See id.; see also NARA Classification Directive, 32 C.F.R. § 2001.12(a)(1) (2008) (establishing guidelines for the duration of the classification, and requiring that a "classification authority shall attempt to determine a date or event that is less than ten years from the date of the original classification and which coincides with the lapse of the information's national security sensitivity").

131 See Exec. Order No. 12,958, as amended, § 1.5(b); see also NARA Classification Directive, 32 C.F.R. § 2001.12(a)(1).

132 See Exec. Order No. 12,958, as amended, § 1.5(b).

133 Compare Exec. Order No. 12,958, as amended, § 3.3 (current version), with Exec. Order No. 12,958, § 3.4 (original version).
executive order\textsuperscript{134} and is intended to ultimately lead to the creation of a governmentwide declassification database within NARA.\textsuperscript{135} For records that fall within any exception to amended Executive Order 12,958’s automatic declassification mechanism, agencies are required to establish "a program for systematic declassification review" that focuses on any need for continued classification of such records.\textsuperscript{136}

As did prior executive orders, amended Executive Order 12,958 provides for a "mandatory declassification review" program.\textsuperscript{137} This mechanism allows any person -- entirely apart from the FOIA context -- to request that an agency review its national security records for declassification.\textsuperscript{138} Unlike under the FOIA, though, such requesters do not have the right to judicial review of the agency's action.\textsuperscript{139} Instead, amended Executive Order 12,958 authorizes persons to appeal an agency's final decision under this program to the Interagency Security Classification Appeals Panel.\textsuperscript{140} To alleviate some of the burden of this program, Executive Order 12,958 contains a provision that allows an agency to deny a mandatory review request if it has already reviewed the information for declassification within the past two years.\textsuperscript{141}

For declassification decisions, amended Executive Order 12,958 authorizes agencies to apply a balancing test -- i.e., to determine "whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure."\textsuperscript{142} Though Executive Order 12,958, as amended, specifies that this provision is implemented solely as a matter of administrative discretion and creates no new right of

\textsuperscript{134} See Exec. Order No. 12,958, as amended, § 3.3(a).

\textsuperscript{135} See id. § 3.7 (directing Archivist to establish database of information that has been declassified by agencies, and instructing agency heads to cooperate in this governmentwide effort); see also Presidential Memorandum for Heads of Executive Departments and Agencies Concerning Classified Information and Controlled Unclassified Information, 74 Fed. Reg. 26277 (May 27, 2009) (directing Assistant to the President for National Security Affairs to address, in revisions to Executive Order 12,958, as amended, the creation of a National Declassification Center within NARA).

\textsuperscript{136} See Exec. Order No. 12,958, as amended, § 3.4(a).

\textsuperscript{137} Id. § 3.5.

\textsuperscript{138} See id.

\textsuperscript{139} See id.; cf. Miller v. Casey, 730 F.2d 773, 778 (D.C. Cir. 1984) (refusing to review CIA decision to deny access to records under agency's discretionary "historical research program").

\textsuperscript{140} See Exec. Order No. 12,958, as amended, § 3.5(b)(4), (d).

\textsuperscript{141} See id. § 3.5(a)(3).

\textsuperscript{142} Id. § 3.1(b).
judicial review, it is significant that no such provision existed under prior orders.\footnote{143} Although a few courts have attempted to apply the balancing test to the review of classification decisions in litigation,\footnote{144} most have held that national security officials are responsible for applying this balancing test at the time of the original classification decision, and that these officials are in the best position to weigh the public interest in disclosure against the threat to national security.\footnote{145}

Glomar Response and Mosaic Approach

Two additional considerations addressed initially by the original version of Executive Order 12,958, and then continued in the amended version, have already been recognized by the courts. First, the "Glomar" response is explicitly incorporated into the order: "An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the very fact of their existence or nonexistence is itself classified under this order."\footnote{146} The use of this response has been routinely upheld by the courts.\footnote{147}

\footnote{143 See FOIA Update, Vol. XVI, No. 2, at 11 ("Executive Order Comparison Chart") (providing chart comparing provisions of original version of Executive Order 12,958 with those of predecessor Executive Order 12,356).

\footnote{144 See, e.g., L.A. Times Commc'n, LLC v. Dep't of the Army, 442 F. Supp. 2d 880, 902 (C.D. Cal. 2006) (explaining that the court was attempting to achieve the "balance Congress sought to preserve between the public's right to know and the government's legitimate interest in keeping certain information confidential").

\footnote{145 See, e.g., ACLU v. DOJ, 265 F. Supp. 2d 20, 32 (D.D.C. 2003) (holding that even a "significant and entirely legitimate" public desire to view classified information "simply does not, in an Exemption 1 case, alter the analysis"); Kelly v. CIA, No. 00-2498, slip op. at 15 (D.D.C. Aug. 8, 2002) (observing that agency should factor in public interest at time that classification decision is made, and further noting that requester's asserted public interest in disclosure of requested information will not undermine proper classification because it certainly is in public interest to withhold information that would damage national security), modified in other respects, No. 00-2498, slip op. at 1 (D.D.C. Sept. 25, 2002), appeal on adequacy of search dismissed on procedural grounds, No. 02-5384, 2003 WL 21804101 (D.C. Cir. July 31, 2003).

\footnote{146 Exec. Order No. 12,958, as amended, § 3.6(a), 68 Fed. Reg. 15,315 (Mar. 28, 2003), reprinted in 50 U.S.C. § 435 note (2006); see also Hogan v. Huff, No. 00-6753, 2002 WL 1369722, at *7 (S.D.N.Y. June 21, 2002) (ruling that the executive order "authorizes agencies to refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence is itself classified") (decided under original version of Executive Order 12,958).

Second, the "mosaic" or "compilation" approach -- the concept that apparently harmless pieces of information, when assembled together, could reveal a damaging picture -- is recognized in amended Executive Order 12,958.\textsuperscript{146} It is also a concept that has been widely recognized by courts in Exemption 1 cases.\textsuperscript{149} Compilations of otherwise unclassified information may be classified if the "compiled information reveals an additional association or relationship that: (1) meets the [order's classification] standards, and (2) is not otherwise revealed in the individual items of information."\textsuperscript{150} This "mosaic" approach has been

\textsuperscript{147}(...continued)

request for records concerning plaintiff's activities as journalist in Cuba during 1960s); \textit{Marrera v. DOJ}, 622 F. Supp. 51, 53-54 (D.D.C. 1985) (applying "Glomar" response to request for any record which would reveal whether requester was target of surveillance pursuant to Foreign Intelligence Surveillance Act); cf. \textit{Bassiouni v. CIA}, No. 02-C-4049, 2004 WL 1125919, at *7 (N.D. Ill. Mar. 31, 2004) (allowing agency to give "no number, no list" response -- i.e., admission that records existed, coupled with refusal to further describe them -- to protect classified national security information even though agency previously acknowledged existence of records), aff'd, 392 F.3d 244 (7th Cir. 2004). But see \textit{ACLU v. DOD}, 389 F. Supp. 2d 547, 591 (S.D.N.Y. 2005) (commenting that the "danger of Glomar responses is that they encourage an unfortunate tendency of government officials to over-classify information, frequently keeping secret that which the public already knows, or that which is more embarrassing that revelatory of intelligence sources or methods").

\textsuperscript{148} Exec. Order No. 12,958, as amended, § 1.7(e).

\textsuperscript{149} See \textit{Bassiouni}, 392 F.3d at 246 (recognizing properly that "[w]hen a pattern of responses itself reveals classified information, the only way to keep secrets is to maintain silence uniformly"); \textit{Edmonds v. DOJ}, 405 F. Supp. 2d 23, 33 (D.D.C. 2005) (upholding the agency's mosaic argument, and finding that it "comports with the legal framework"); \textit{Berman v. CIA}, 378 F. Supp. 2d 1209, 1215-17 (E.D. Cal. 2005) (observing that "numerous courts have recognized the legitimacy of the mosaic theory in the context of the FOIA," and holding that CIA's Presidential Daily Briefs could fairly be viewed as "an especially large piece of the 'mosaic' because it is the only finished intelligence product that synthesizes all of the best available intelligence" for the President (citing \textit{CIA v. Sims}, 471 U.S. 159, 178 (1985))); \textit{ACLU v. DOJ}, 321 F. Supp. 2d 24, 37 (D.D.C. 2004) (affirming that "this Circuit has embraced the government's 'mosaic' argument in the context of FOIA requests that implicate national security concerns"); \textit{Edmonds v. FBI}, 272 F. Supp. 2d 35, 47-48 (D.D.C. 2003) (accepting that "some information required classification because it was intertwined with the sensitive matters at the heart of the case" and "would tend to reveal matters of national security even though the sensitivity of the information may not be readily apparent in isolation") (decided under original version of Executive Order 12,958); \textit{ACLU v. DOJ}, 265 F. Supp. 2d 20, 29 (D.D.C. 2003) (allowing the agency to withhold statistical intelligence-collection data, commenting that "even aggregate data is revealing," and concluding that disclosure "could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities") (decided under original version of Executive Order 12,958).

\textsuperscript{150} See Exec. Order No. 12,958, as amended, § 1.7(e); see also \textit{Billington v. DOJ}, 11 F. Supp. 2d 45, 55 (D.D.C. 1998) (applying cited provision of executive order to rule that "aggregate result" does not need to be "self-evident" to qualify for Exemption 1 protection), summary (continued...
consistently endorsed by the courts. The Court of Appeals for the District of Columbia Circuit has also reaffirmed that even if there is other information that if released "would pose a greater threat to the national security," Exemption 1 "bars the court from prying loose from the government even the smallest bit of information that is properly classified." The court held that situations may exist, in the national security context particularly, where even "bits and pieces" of data may aid in piecing together bits of other information even when the individual piece is not of obvious importance itself. As with other agency decisions regarding harm to national security, it is also reasonable for courts to grant an agency the appropriate degree of deference with regard to the practical applicability of their mosaic analysis.


See, e.g., Am. Friends Serv. Comm. v. DOD, 831 F.2d 441, 444-45 (3d Cir. 1987) (recognizing validity of "compilation" theory, and ruling that certain "information harmless in itself might be harmful when disclosed in context"); Salisbury v. United States, 690 F.2d 966, 971 (D.C. Cir. 1982) (explicitly acknowledging "mosaic-like nature of intelligence gathering"); Taylor v. Dept of the Army, 684 F.2d 99, 105 (D.C. Cir. 1982) (upholding classification of compilation of information on army combat units); Halperin v. CIA, 629 F.2d 144, 150 (D.C. Cir. 1980) (observing that ")each individual piece of intelligence information, much like a piece of a jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"); Loomis v. DCE, No. 96-149, 1999 WL 33541935, at *7 (N.D.N.Y. Mar. 9, 1999) (finding that safety measures regarding nuclear facilities set forth in manuals and lay-out plans contain highly technical information and that "such information in the aggregate could reveal sensitive aspects of operations"); summary affirmation granted, 21 F. App'x 80 (2d Cir. 2001); Nat'l Sec. Archive v. FBI, 759 F. Supp. 872, 877 (D.D.C. 1991) (adjudging that disclosure of code names and designator phrases could provide hostile intelligence analyst with "common denominator" permitting analyst to piece together seemingly unrelated data into snapshot of specific FBI counterintelligence activity).

Abbotts v. NRC, 766 F.2d 604, 608 (D.C. Cir. 1985) (quoting Afshar v. Dep't of State, 702 F.2d 1125, 1130 (D.C. Cir. 1983)).

ACLU, 321 F. Supp. 2d at 37 (quoting Sims, 471 U.S. at 178).

Id. (quoting Ctr. for Nat'l Sec. Studies v. DOJ, 331 F.3d 918, 928 (D.C. Cir. 2003)).

See Berman, 378 F. Supp. 2d at 1217 (holding, in context of Exemption 3, that agency's decision to employ a mosaic analysis is entitled to deference); see also Larson v. Dep't of State, No. 02-1937, 2005 WL 3276303, at *12 (D.D.C. Aug. 10, 2005) (allowing that "the CIA has the right to assume that foreign intelligence agencies are zealous ferrets" (citing Gardels v. CIA, 689 F.2d 1100, 1106 (D.C. Cir. 1982))).
Exclusion Considerations

Additionally, agencies should also be aware of the FOIA's "(c)(3) exclusion.\textsuperscript{156} This special records exclusion applies to certain especially sensitive records maintained by the Federal Bureau of Investigation, which concern foreign intelligence, counterintelligence or international terrorism matters: Where the existence of such records is itself a classified fact, the FBI may, so long as the existence of the records remains classified, treat the records as not subject to the requirements of the FOIA.\textsuperscript{157} (See the discussion of this provision under Exclusions, below.)

\textsuperscript{156} 5 U.S.C. § 552(c)(3).

\textsuperscript{157} Id.; see also Attorney General's Memorandum on the 1986 Amendments to the Freedom of Information Act 24-25 (Dec. 1987).
Balkinization
an unanticipated consequence of
Jack M. Balkin

Monday, November 05, 2007

Our Classification Pathologies

Marty Lederman

One of the high-level CIA detainees, Majid Khan, recently met over eight days with his attorneys from the Center for Constitutional Rights, and told them of the "time he spent in CIA custody." In connection with the Mukasey confirmation vote, his attorneys quite understandably wish to let Congress know how our government has treated their client. But as a condition of being able to speak to their client in the first place, the government required them to agree not to reveal what their client told them, because (as they explained in a letter to Senators today) "everything we learned from our client is presumptively classified."

I've said this before but it's worth saying again: This is absurd, and, assuming that Khan or his attorneys have any First or Sixth Amendment rights (a hard question, perhaps), it's likely unconstitutional, too. Even if it made sense to classify the CIA techniques in the first place, once the government "reveals" its classified information to private persons outside the government, the classification has been compromised. Classification rules restrict what government officials may say. And they restrict what can be said by those (e.g., judges, opposing counsel) who are given the information only on the condition that they not disclose it. But Khan himself did not "ask for" this "information," or agree to any conditions on disclosure before "receiving" it. Therefore, the only reason he cannot publish an account of what the CIA did to him on the front page of the New York Times (or ask his lawyers to do so) is not that he is subject to classification restrictions, but instead that the government has gagged him as part of its detention practice.

If Khan were ever freed -- either because he was wrongly detained, or because the conflict ends, etc.; or if he were put inside the criminal justice system; or if he were detained in the United States; or if he were a U.S. person; he would be able, as a practical and as a legal matter, to publicly reveal what the CIA did to him. (Imagine a criminal defendant raising a defense about being tortured by the state and the state responding that the methods of interrogation were classified . . . .)

Why should that fact change just because Khan is an alien being held in a wholly-
U.S.-controlled facility a few miles off the coast of Florida? Here's what I wrote about this previously. It is still relevant -- except that now the Senators have the ability to call a halt to this absurd classification nonsense:

[Even if the classification [of the techniques] were itself valid, can it really be the case that the persons against whom the CIA employed its methods may be prevented from disclosing such historical facts to the public?

There is not, to my knowledge, any statute purporting to restrict such publication. Indeed, at least to the extent that the writer's audience includes the U.S. public, I would assume that the victim of U.S. government actions has a First Amendment right to publish the story, even if he is an alien abroad (see Lamont). (Perhaps there's a Sixth Amendment right to counsel implicated, too, but I'm less interested in that just now.)

So, for example, if and when Khan is released from U.S. custody, he will be free -- both legally and as a practical matter -- to publicly describe his treatment at the hands of the CIA, even though a CIA employee, or Senator overseeing the agency, might not be likewise free to do so because of the classification. Indeed, several CIA detainees have publicly told the stories of their detention and interrogation, including the book-length treatment by Moazzam Begg and the declaration, in the Khan case itself, of Khaled al-Masri, who was held with Khan in the "Salt Pit." We could not detain Khan because he threatened to reveal what the CIA did to him -- that would be an impermissible prior restraint. (This information does not, in other words, fall within one of the small handful of categories of information -- such as the direction of future troop movements (see Near v. Minnesota) -- whose publication the government may unconditionally prohibit.)

Therefore, even if Khan is legally detained for other, valid reasons, it seems to me that we cannot use the fact -- the fortuity -- of his detention as an excuse for preventing his public speech that would otherwise be constitutionally privileged.

Posted 5:30 PM by Marty Lederman [link]
More on al-Aulaqi and Transparency

by Jack Goldsmith

In response to some push back, and at the risk of some repetition, I would like to clarify a bit more why I think there is no serious bar to the government revealing more about the legal basis for its action against al-Awlaki in Yemen.

There are very good reasons why the government might not want to officially and openly talk about a covert operation despite the fact that, as Ben says, everyone in the world knows about it. As Abe Shulsky and Gary Schmitt gingerly say of covert actions in their excellent (though somewhat outdated) book on intelligence:

[T]here may be cases in which a good deal of information about operations becomes public, but for diplomatic or other reasons, governments involved avoid officially acknowledging their connection with them. ... [I]t is less provocative and less disruptive to diplomatic relations not to acknowledge an operation even if the country adversely affected by it is well aware of one's involvement. The target country, either in the interests of good relations or because it cannot effectively prevent it, may ignore the covert action; it is much harder for it to do so if the government conducting it publicly acknowledges what it is doing.

I accept this and related explanations as reasons not to acknowledge the action officially. But maintaining technical covertness is not an absolute value or an absolute bar to more transparency. There are at least two competing factors to consider:

First, it is wrong, as Ben notes, for the government to maintain technical covertness but then engage in continuous leaks, attributed to government officials, of many (self-serving) details about the covert operations and their legal justifications. It is wrong because it is illegal. It is wrong because it damages (though perhaps not destroys) the diplomatic and related goals of covertness. And it is wrong because the Executive branch seems to be trying to have its cake (not talking about the program openly in order to serve diplomatic interests and perhaps deflect scrutiny) and eat it too (leaking promiscuously to get credit for the operation and to portray it as lawful). I do not know if the leaks are authorized in some sense or not, or where in the executive branch they come from, or what if anything the government might be doing to try to stop them. But of course the president is ultimately responsible for the leaks. One might think -- I am not there yet, but I understand why someone might be -- that the double standard on discussing covert actions disqualifies the government from invoking technical covertness to avoid scrutiny.

Second, there is no bar grounded in technical covertness, or in concerns about revealing means and methods of intelligence gathering, to revealing (either in a redacted opinion or in a separate document) the legal reasoning supporting a deadly strike on a U.S. citizen. John Brennan and Harold Koh have already talked about the legality of strikes outside Afghanistan in abstract terms, mostly focusing on international law. I don't think much more detail on the international law basis is necessary; nor do I think that more disclosure on international law would do much to change the minds of critics who believe the strikes violate international law. But there has been practically nothing said officially (as opposed through leaks and gestures and what is revealed in between the lines in briefs) about the
executive branch processes that lie behind a strike on a U.S. citizen, or about what constitutional rights the U.S. citizen target possesses, or about the limitations and conditions on the president’s power to target and kill a U.S. citizen. This information would, I think, matter to American audiences that generally support the president on the al-Aulaqi strike but want to be assured that it was done lawfully and with care. The government could easily reveal this more detailed legal basis for a strike on a U.S. citizen without reference to particular operations, or targets, or means of fire, or countries.

This was written by Jack Goldsmith. Posted on Wednesday, October 5, 2011, at 2:17 pm. Tagged Al Awlaki, Harold Koh, John Brennan. Bookmark the permalink. Follow comments here with the RSS feed.

Filed in Covert Action | Targeted Killing | Targeted Killing: Drones.

Both comments and trackbacks are currently closed.
The WikiLeaks Illusion

by Alasdair Roberts

WikiLeaks’ tsunami of revelations from U.S. government sources last year did not change the world, but it did change WikiLeaks.

Late last November, the antisecrecy group WikiLeaks achieved the greatest triumph in its short history. A consortium of major news media organizations—including The New York Times, The Guardian, Der Spiegel, Le Monde, and El País—began publishing excerpts from a quarter-million cables between the U.S. State Department and its diplomatic outposts that WikiLeaks had obtained. The group claimed that the cables constituted “the largest set of confidential documents ever to be released into the public domain.” The Guardian predicted that the disclosures would trigger a “global diplomatic crisis.”

This was the fourth major disclosure orchestrated by WikiLeaks last year. In April, it had released a classified video showing an attack in 2007 by U.S. Army helicopters in the streets of Baghdad that killed 12 people, including two employees of the Reuters news agency. In July, it had collaborated with the news media consortium on the release of 90,000 documents describing U.S. military operations in Afghanistan from 2004 through 2009. These records included new reports of civilian casualties and “friendly fire” incidents. In October came a similar but larger set of documents—almost 400,000—detailing U.S. military operations in Iraq.

WikiLeaks’ boosters said that the group was waging a war on secrecy, and by the end of 2010 it seemed to be winning. The leaks marked “the end of secrecy in the old-fashioned, Cold War–era sense,” claimed Guardian journalists David Leigh and Luke Harding. A Norwegian politician nominated WikiLeaks for the Nobel Peace Prize, saying that it had helped “redraw the map of information freedom.” “Like him or not,” wrote a Time magazine journalist in December, WikiLeaks founder Julian Assange had “the power to impose his judgment of what should or shouldn’t be secret.”

Did the leaks of 2010 really mark the end of “old-fashioned secrecy?” Not by a long shot. Certainly, new information technologies have made it easier to leak sensitive information and broadcast it to the world. A generation ago, leaking was limited by the need to physically copy and smuggle actual documents. Now it is a matter of dragging, dropping, and clicking Send. But there are still impressive barriers to the kind of “radical
transparency” WikiLeaks says it wants to achieve. Indeed, the WikiLeaks experience shows how durable those barriers are.

Let's begin by putting the leaks in proper perspective. A common way of showing their significance is to emphasize the sheer volume of material. In July 2010, The Guardian described the release of the Afghan war documents as “one of the biggest leaks in U.S. military history.” Assange, an Australian computer programmer and activist who had founded WikiLeaks in 2006 (and is currently in Britain facing extradition to Sweden on rape and sexual molestation charges), compared it to perhaps the most famous leak in history. “The Pentagon Papers was about 10,000 pages,” he told the United Kingdom’s Channel 4 News, alluding to the secret Pentagon history of America’s involvement in Vietnam that was leaked in 1971. By contrast, there were “about 200,000 pages in this material.”

The Afghan war logs did not hold the record for long. In October, they were supplanted by the Iraq disclosures, “the greatest data leak in the history of the United States military,” according to Der Spiegel. Within weeks, WikiLeaks was warning that this record too would soon be shattered. It boasted on Twitter that its next release, the State Department cables, would be “7x the size of the Iraq War Logs.” Indeed, it was “an astonishing mountain of words,” said the two Guardian journalists. “If the tiny memory stick containing the cables had been a set of printed texts, it would have made up a library containing more than 2,000 sizable books.”

Gauging the significance of leaks based on document volume involves a logical fallacy. The reasoning is this: If we are in possession of a larger number of sensitive documents than ever before, we must also be in possession of a larger proportion of the total stockpile than ever before. But this assumes that the total itself has not changed over time.

In fact, the amount of sensitive information held within the national security apparatus is immensely larger than it was a generation ago. Technological change has caused an explosion in the rate of information production within government agencies, as everywhere else. For example, the leaked State Department cables might have added up to about two gigabytes of data—one-quarter of an eight-gigabyte memory card. By comparison, it has been estimated that the outgoing Bush White House transferred 77 terabytes of data to the National Archives in 2009. That is almost 10,000 memory cards for the White House alone. The holdings of other agencies are even larger.

The truth is that a count of leaked messages tells us nothing about the significance of a breach. Only six percent of the State Department cables that were leaked last year were classified as secret. And the State Department has said that the network from which the cables were extracted was not even the primary vehicle for disseminating its information. In the period in which most of the quarter-million WikiLeaks cables were distributed within the U.S. government, a State Department official said, “we disseminated 2.4 million cables, 10 times as many, through other systems.”

The 2010 disclosures also revealed fundamental problems with the WikiLeaks project. The logic that initially motivated Assange and his colleagues was straightforward: WikiLeaks would post leaked information on the Internet and rely on the public to interpret it, become outraged, and demand reform. The antisecrecy group, which at the start of last year had a core of about 40 volunteers, had great faith in the capacity of the public to do the right thing. Daniel Domscheit-Berg, who was WikiLeaks’ spokesman until he broke with Assange last fall, explained the reasoning in Inside WikiLeaks, a book published earlier this year: “If you provide people sufficient background information, they are capable of behaving correctly and making the right decisions.”
This proposition was soon tested and found wanting. When WikiLeaks released a series of U.S. military counterinsurgency manuals in 2008, Domscheit-Berg thought there would be “outrage around the world, and I expected journalists to beat down our doors.” The manuals described techniques for preventing the overthrow of governments friendly to the United States. In fact, the reaction was negligible. “No one cared,” writes Domscheit-Berg, “because the subject matter was too complex.”

As the British journalist John Lanchester recently observed, WikiLeaks’ “release of information is unprecedented: But it is not journalism. The data need to be interpreted, studied, made into a story.” WikiLeaks attempted to do this itself when it released the Baghdad helicopter video. Assange unveiled the video at a news conference at the National Press Club in Washington, D.C., and packaged it so that its significance would be clear. He titled it Collateral Murder. The edited video, WikiLeaks said, provided evidence of “indiscriminate” and “unprovoked” killing of civilians.

Even with this priming, the public reaction was muted. Many people turned on WikiLeaks itself, charging that it had manipulated the video to bolster its allegations of military misconduct. “This strategy for stirring up public interest was a mistake,” Domscheit-Berg agrees. “A lot of people [felt] . . . that they were being led around by the nose.”

The release of the Afghan war documents in July 2010 gave WikiLeaks further evidence of its own limitations. The trove of documents was “vast, confusing, and impossible to navigate,” according to The Guardian’s Leigh and Harding, “an impenetrable forest of military jargon.” Furthermore, the logs contained the names of many individuals who had cooperated with the American military and whose lives could be threatened by disclosure. WikiLeaks recognized the need for a “harm minimization” plan but lacked the field knowledge necessary to make good decisions about what should be withheld.

By last summer, all of these difficulties had driven WikiLeaks to seek its partnership with news media organizations. The consortium that handled the disclosures last fall provided several essential services for the group. It gave technical assistance in organizing data and provided the expertise needed to decode and interpret records. It opened a channel to government officials for conversation about the implications of disclosing information that WikiLeaks itself was unable to establish. Finally, of course, the news media organizations had the capacity to command public attention. They were trusted by readers and possessed a skill in packaging information that WikiLeaks lacked.

By the end of 2010, it was clear that WikiLeaks’ modus operandi had fundamentally changed. It had begun with an unambiguous conception of its role as a receiver and distributor of leaked information. At year’s end, it was performing a different function: It still hoped to serve as a trusted receiver of leaks, but it was now working with mainstream news media to decide how—or if—leaked information ought to be published. For WikiLeaks, this involved difficult concessions. “We were no longer in control of the process,” Domscheit-Berg later wrote. The outflow of leaked information was now constrained by the newspapers’ willingness to invest money and time in sifting through more documents.

For the newspapers that participated in the consortium, the rationale for publishing leaked information was simple. As The New York Times explained in an editorial note when the State Department cables were released in November, Americans “have a right to know what is being done in their name.” The cables “tell the unvarnished story of how the government makes its biggest decisions.” This is the conventional journalistic argument in defense of disclosure, and there is no doubt that the WikiLeaks revelations provided vivid and sometimes disturbing illustrations of the ways in which power is wielded by the United States and its allies.
WikiLeaks itself wanted bigger things to flow from its work. It continued to expect outrage and political action. Assange told Britain’s Channel 4 News last July that he anticipated that the release of the Afghan war documents would shift public opinion against the war. There was a similar expectation following release of the Iraq war documents. But these hopes were again disappointed. In some polls, perceptions about the conduct of the Afghan war actually became more favorable after the WikiLeaks release. Meanwhile, opinion about American engagement in Iraq remained essentially unchanged, as it had been for several years.

There are good reasons why disclosures do not necessarily produce significant changes in policy or politics. Much depends on the context of events. When the Pentagon Papers came out in 1971, they contributed to policy change because a host of other forces were pushing in the same direction. The American public was exhausted by the Vietnam War, which at its peak involved the deployment of almost four times as many troops as are now in Iraq and Afghanistan. Many Americans were also increasingly skeptical of all forms of established authority. The federal government’s status was further tarnished by other revelations about abuses of power by the White House, CIA, and FBI.

We live in very different times. There is no popular movement against U.S. military engagement overseas, no broad reaction against established authority in American society, no youth rebellion. The public mood in the United States is one of economic uncertainty and physical insecurity. Many Americans want an assurance that their government is willing and able to act forcefully in the pursuit of U.S. interests. In this climate, the incidents revealed by WikiLeaks—spying on United Nations diplomats, covert military action against terrorists, negotiations with regimes that are corrupt or guilty of human rights abuses—might not even be construed as abuses of power at all. On the contrary, they could be regarded as proof that the U.S. government is prepared to get its hands dirty to protect its citizens.

Indeed, it could be said that WikiLeaks was doing the one thing Americans least wished for: increasing instability and their sense of anxiety. The more WikiLeaks disclosed last year, the more American public opinion hardened against it. By December, according to a CNN poll, almost 80 percent of Americans disapproved of WikiLeaks’ release of U.S. diplomatic and military documents. In a CBS News poll, most respondents said they thought the disclosures were likely to hurt U.S. foreign relations. Three-quarters affirmed that there are “some things the public does not have a right to know if it might affect national security.”

As WikiLeaks waited fruitlessly for public outrage, it began to see another obstacle to the execution of its program. WikiLeaks relies on the Internet for the rapid dissemination of leaked information. The assumption, which seemed plausible in the early days of cyberspace, is that the Internet is a vast global commons—a free space that imposes no barrier on the flow of data. But even online, commercial and political considerations routinely compromise the movement of information.

This reality was quickly illustrated after the release of the State Department cables on November 28. Three days later, Amazon Web Services, a subsidiary of Amazon.com that rents space for the storage of digitized information, stopped acting as a host for WikiLeaks’ material, alleging that the group had violated its terms of service. The same day, a smaller firm that provides online graphics capabilities, Tableau Software, discontinued its support. The firm that managed WikiLeaks’ domain name, EveryDNS.net, also suspended services, so that the domain name wikileaks.org was no longer operable. On December 20, Apple removed an application from its online store that offered iPhone and iPad users access to the State Department cables.

All of these actions complicated WikiLeaks’ ability to distribute leaked information. Decisions by other organizations also undermined its financial viability. Five days after the State Department disclosures, PayPal, which manages online payments, announced that it would no longer process donations to WikiLeaks, alleging
that the group had violated its terms of service by encouraging or facilitating illegal activity. MasterCard and Vise Europe soon followed suit.

Critics alleged that these firms were acting in response to political pressure, and many American legislators did in fact call on businesses to break with WikiLeaks. But direct political pressure was hardly necessary; cold commercial judgment led to the same decision. WikiLeaks produced little revenue for any of these businesses but threatened to entangle all of them in public controversy. A public-relations specialist told Seattle’s KIRO News that it was “bizarre” for Amazon to assist WikiLeaks during a holiday season: “I don’t think you mix politics with retail.” Worse still, businesses were exposed to cyberattacks by opponents of WikiLeaks within the hacker community that disrupted their relationships with other, more profitable clients.

These business decisions hurt WikiLeaks significantly. Assange said they amounted to “economic censorship” and claimed that actions by these financial intermediaries were costing WikiLeaks $650,000 per week in lost donations.

The leaks also provoked a vigorous reaction by the U.S. government. The Army came down hard on Private Bradley Manning, the apparent source of all four of the 2010 disclosures, bringing 34 charges against him. The most serious of these, aiding the enemy, could result in a death sentence, although prosecutors have said they will not seek one. The government is also investigating other individuals in connection with the leaks. Some in Congress have used the episodes to argue for strengthening the law on unauthorized disclosure of national security information, and federal agencies have tightened administrative controls on access to sensitive information. These steps, which may well produce a result precisely the opposite of what WikiLeaks intends by reducing citizens’ access to information about the government, have been taken by an administration that promised on its first day in office to “usher in a new era of open government.”

WikiLeaks is predicated on the assumption that the social order—the set of structures that channel and legitimate power—is both deceptive and brittle: deceptive in the sense that most people who observe the social order are unaware of the ways in which power is actually used, and brittle in the sense that it is at risk of collapse once people are shown the true nature of things. The primary goal, therefore, is revelation of the truth. In the past it was difficult to do this, mainly because primitive technologies made it difficult to collect and disseminate damming information. But now these technological barriers are gone. And once information is set free, the theory goes, the world will change.

We have seen some of the difficulties with this viewpoint. Even in the age of the Internet, there is no such thing as the instantaneous and complete revelation of the truth. In its undigested form, information often has no transformative power at all. Raw data must be distilled and interpreted, and the attention of a distracted audience must be captured. The process by which this is done is complex and easily influenced by commercial and governmental interests. This was true before the advent of the Internet and remains true today.

Beyond this, there is a final and larger problem. It may well be that many of the things WikiLeaks imagines are secrets are not really secrets at all. It may be that what WikiLeaks revealed when it drew back the curtain is more or less what most Americans already suspected had been going on, and were therefore prepared to tolerate.

To put it another way, much of what WikiLeaks has released might best be described as open secrets. It would have been no great shock to most Americans, for example, to learn about the United States’ covert activities against terrorists in Yemen. “The only surprising thing about the WikiLeaks revelations is that they contain no surprises,” says the noted Slovenian philosopher Slavoj Zizek, a professor at the European Graduate School.
“The real disturbance was at the level of appearances: We can no longer pretend we don’t know what everyone knows we know.”

In a sense, it was odd to expect that there would be great surprises. The diplomatic and national security establishment of the U.S. government employs millions of people. Most of the critical decisions about the development of foreign policy, and about the apparatus necessary to execute that policy, have been made openly by democratically elected leaders, and sanctioned by voters in national elections over the course of 60 years. In broad terms, Americans know how U.S. power is exercised, and for what purpose. And so there are limits to what WikiLeaks can unveil. Even New York Times executive editor Bill Keller conceded that the disclosures did not “expose some deep, unsuspected perfidy in high places.” They provide only “texture, nuance, and drama.”

None of this is an argument for complacency about government secrecy. Precisely because of the scale and importance of the national security apparatus, it ought to be subjected to close scrutiny. Existing oversight mechanisms such as freedom of information laws and declassification policies are inadequate and should be strengthened. The monitoring capacity of news media outlets and other nongovernmental organizations must be enhanced. And citizens should be encouraged to engage more deeply in debates about the aims and methods of U.S. foreign policy. All of these steps involve hard work. There is no technological quick fix. A major difficulty with the WikiLeaks project is that it may delude us into believing otherwise.

You can download PDF file


Reprinted with the permission of The Woodrow Wilson International Center for Scholars.
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

NASSER AL-AULAQI, on his own behalf and as next
friend acting on behalf of ANWAR AL-AULAQI,

Plaintiff,

v.

BARACK H. OBAMA, President of the United States;
ROBERT M. GATES, Secretary of Defense; LEON E.
PANETTA, Director of the Central Intelligence Agency,

Defendants.

Civ. A. No. 10-cv-1469

PUBLIC DECLARATION AND ASSERTION OF MILITARY
AND STATE SECRETS PRIVILEGE BY
ROBERT M. GATES, SECRETARY OF DEFENSE

I, Robert M. Gates, do hereby state and declare as follows:

1. I am the Secretary of Defense and have served in this capacity since
December 18, 2006. As such, I am the head of the Department of Defense ("DoD") and
the principal assistant to the President in all matters relating to the Department of
Defense. The Secretary of Defense has authority, direction, and control over DoD and all
its components and activities. See 10 U.S.C. § 113(b). Prior to serving as the Secretary
of Defense, I served as Director of Central Intelligence from 1991 to 1993, as Deputy
Director of Central Intelligence from 1986 until 1989, and as Assistant to the President and Deputy National Security Adviser from 1989 until 1991.

2. Through the exercise of my official duties, I have been advised of this litigation and have reviewed the complaint in this case. I make the following statements based upon my personal knowledge and on information made available to me in my official capacity.

3. The purpose of this declaration is to formally assert the military and state secrets privilege in order to protect highly sensitive information of DoD and U.S. armed forces implicated by the allegations in this case. As summarized in this public declaration and described further in my classified declaration submitted for the Court's in camera, ex parte review, public disclosure of the information covered by my privilege assertion reasonably could be expected to cause harm, up to and including exceptionally grave harm, to the national security of the United States.

4. As the Secretary of Defense, pursuant to Executive Order 13256, I hold original classification authority up to the TOP SECRET level. This means that I have been authorized by the President to make original classification decisions.

I. ASSERTION OF THE STATE SECRETS PRIVILEGE

5. The allegations of this case put at issue sensitive intelligence information about al Qaida in the Arabian Peninsula ("AQAP"), disclosure of which would cause exceptionally grave harm to national security. The allegations of this case also put at issue sensitive military information concerning whether or not U.S. armed forces are engaged in particular operations in Yemen and the circumstances of any such operations.
Without confirming or denying any allegation in this case, information concerning whether or not U.S. armed forces are planning to undertake military actions in a foreign country, against particular targets, under what circumstances, for what reasons, and pursuant to what procedures or criteria, constitutes highly sensitive and classified military information that cannot be disclosed without causing serious harm to the national security of the United States. Accordingly, as set forth further below, I am asserting the military and state secrets privilege over information that falls within the following categories and that may be implicated by the allegations in this lawsuit:

A. Intelligence information DoD possesses concerning AQAP and Anwar al-Aulaqi, including intelligence concerning the threat AQAP or Anwar al-Aulaqi pose to national security, and the sources, methods, and analytic processes on which any such intelligence information is based;

B. Information concerning possible military operations in Yemen, if any, and including criteria or procedures DoD may utilize in connection with such military operations; and

C. Information concerning relations between the United States and the Government of Yemen, including with respect to security, military, or intelligence cooperation, and that government's counterterrorism efforts.

II. HARM OF DISCLOSURE OF THE PRIVILEGED INFORMATION.

6. First, I am asserting privilege over intelligence information DoD possesses concerning AQAP and Anwar al-Aulaqi, including intelligence concerning the threat AQAP or Anwar al-Aulaqi pose to national security, and the sources, methods, and analytic processes on which any such intelligence information is based. The United States, in a July 16, 2010 press release issued by the Department of Treasury, has
publicly indicated that AQAP is a Yemen-based terrorist group that has claimed
responsibility for numerous terrorist acts against United States and other targets,
including targets in Yemen itself, and that Anwar al-Aulaqi is a key operational AQAP
leader who assisted in preparations for the attempted bombing of Northwest Airlines
Flight 253 as it was landing in Detroit on December 25, 2009. See Declaration of Ben
Wizner, Exhibit T. The allegations in this case put at issue the nature and imminence of
the threat posed by AQAP and Anwar al-Aulaqi. My privilege assertion extends to
additional intelligence information that DoD may possess related to this threat, as well as
to the sources and methods by which that intelligence information was collected. The
disclosure of intelligence information concerning AQAP and Anwar al-Aulaqi that DoD
possesses would reveal not only DoD’s state of knowledge with respect to that group and
Anwar al-Aulaqi, and the threat they pose, but would tend to reveal sources and methods
by which such intelligence was obtained. For obvious reasons, DoD cannot reveal to a
foreign terrorist organization or its leaders what it knows about their activities and how it
obtained that information. Such disclosures could not only allow foreign terrorist
organizations to adjust their plans based on the state of U.S. knowledge, but alter their
communications and activities and thereby shield information that could prove critical to
assessing the threat they pose to the United States and other nations. I concur with
Director of National Intelligence Clapper’s assessment that the disclosure of intelligence
information related to AQAP and Anwar al-Aulaqi would cause exceptionally grave
harm to national security.
7. Second, I am asserting privilege over any information concerning possible military operations in Yemen and any criteria or procedures DoD may utilize in connection with such military operations. The disclosure of any operational information concerning actions U.S. armed forces have or may plan to take against a terrorist organization overseas would risk serious harm to national security and foreign relations. Official confirmation or denial of any operations could tend to reveal information concerning operational capabilities that could be used by adversaries to evade or counter any future strikes. The disclosure of such operations would allow such targets to act accordingly, including by altering their behavior to evade military action and continue to plot attacks against the United States. In addition, the disclosure of any criteria or procedures that may be utilized by DoD in planning or undertaking military action overseas would plainly compromise the United States’ capability to take such action not only in a particular case but in future cases by providing terrorist adversaries with insights into military planning. Finally, as discussed below, public confirmation or denial of either prior or planned operations could seriously harm U.S. foreign relations.

8. Third, I am asserting privilege over information concerning relations between DoD and the Government of Yemen, including on security, military or intelligence cooperation, and that government’s counterterrorism efforts. The disclosure of information concerning cooperation between the United States and a foreign state, and specifically regarding any possible military operations in that foreign country, could lead to serious harm to national security, including by disrupting any confidential relations with a foreign government.
III. CONCLUSION

9. In sum, as the Secretary of Defense, I formally assert the military and state secrets privilege in order to protect our nation's security from damage, up to and including exceptionally grave damage. In connection with this assertion of the military and state secrets privilege, I have considered the extent to which the bases for my assertion could be filed on the public record. I have determined that no further information concerning these matters beyond what is in this unclassified declaration can be disclosed on the public record without revealing the very classified information I seek to protect. As noted, my separate classified declaration provides a more detailed explanation of the information and harms to national security. Should the Court require additional information concerning my claims of privilege, I respectfully request an opportunity to provide that information prior to the Court's ruling on my privilege assertion.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 25th day of September 2010.

Robert M. Gates
Secretary of Defense
The Honorable Eric Holder  
Attorney General  
United States Department of Justice  
Washington, D.C. 20530

Dear Attorney General Holder:

As you know, we have been concerned for some time that the U.S. government is relying on secret interpretations of surveillance authorities that—in our judgment—differ significantly from the public’s understanding of what is permitted under U.S. law.

We believe that policymakers can have legitimate differences of opinion about what types of domestic surveillance should be permitted, but we also believe that the American people should be able to learn what their government thinks that the law means, so that voters have the ability to ratify or reject decisions that elected officials make on their behalf.

Unfortunately, however, the decision to classify the government’s interpretations of the law itself makes an informed debate on this issue impossible. Moreover, the absence of publicly available information about the government’s understanding of its authorities increases the risk of the public being misled or misinformed about the official interpretation of public laws.

While we are sure that you would agree that government officials should not describe government authorities in a way that misleads the public, during your tenure Justice Department officials have—on a number of occasions—made what we believe are misleading statements pertaining to the government’s interpretation of surveillance law.

The first set of statements that concern us are the repeated claims by Justice Department officials that the government’s authority to obtain business records or other “tangible things” under section 215 of the USA Patriot Act is analogous to the use of a grand jury subpoena. This comparison—which we consider highly misleading—has been made by Justice Department officials on multiple occasions, including in testimony before Congress. As you know, Section 215 authorities are not interpreted in the same way that grand jury subpoena authorities are, and we are concerned that when Justice Department officials suggest that the two authorities are “analogous” they provide the public with a false understanding of how surveillance law is interpreted in practice.

More recently, we were troubled to learn that a Justice Department spokesman stated that “Section 215 [of the Patriot Act] is not a secret law, nor has it been implemented under secret legal opinions by the Justice Department.” This statement is also extremely misleading. As the NSA General Counsel testified in July of this year, significant
interpretations of section 215 of the Patriot Act are contained in classified opinions of the Foreign Intelligence Surveillance Court and these opinions — and the legal interpretations they contain — continue to be kept secret. In our judgment, when the government relies on significant interpretations of public statutes that are kept secret from the American public, the government is effectively relying on secret law.

Again, we hope you will agree that misleading statements of this nature are not in the public interest and must be corrected. Americans will eventually and inevitably come to learn about the gap that currently exists between the public’s understanding of government surveillance authorities and the official, classified interpretation of these authorities. We believe that the best way to avoid a negative public reaction and an erosion of confidence in US intelligence agencies is to initiate an informed public debate about these authorities today. However, if the executive branch is unwilling to do that, then it is particularly important for government officials to avoid compounding the problem by making misleading statements such as the ones we have described here.

We urge you to correct the public record with regard to these statements, and ensure that everyone who speaks for the Justice Department on this issue is informed enough about it to avoid similarly misleading statements in the future.

Thank you for your attention to this matter.

Sincerely,

Ron Wyden
United States Senator

Mark Udall
United States Senator
Reducing Government Secrecy: Finding What Works

Steven Aftergood

INTRODUCTION

Sunlight is the best disinfectant, Justice Brandeis famously declared, praising publicity as a remedy for corruption. But sunlight is more than that; it is an indispensable precondition of life. And to extend the Brandeis metaphor, sunlight in the form of robust public access to government information is essential to the vitality of democratic governance, even in the absence of corruption. Our political institutions cannot function properly without it.

Whether it concerns matters of high policy, such as the decision to go to war, or the smallest allocation of taxpayer funds, the free flow of information to interested members of the public is a prerequisite to their participation in the deliberative process and to their ability to hold elected officials accountable. Of course, public disclosure of government information is not the only ingredient needed to sustain a vital democracy, and disclosure has always been conditioned on security, privacy, and other considerations. But without it, citizens are deprived of a meaningful role in the political process, and the exercise of authority is insulated from public oversight and control.

Ensuring appropriate public access to government information, while establishing proper boundaries around the exercise of official secrecy, has proved to be an elusive goal. The expansive secrecy practices of recent years appear to have enhanced the case for a new approach by illustrating the unintentional costs of secrecy, as well as its corrosive effects on government performance and public confidence. For example, as former Justice Department official Jack L.

* Director of the Project on Government Secrecy at the Federation of American Scientists. Mr. Aftergood writes and edits the online publication Secrecy News, which reports on new developments in secrecy policy. Research for this Essay was supported by grants from the Open Society Institute, the CS Fund, the Herb Block Foundation, the HKH Fund, the Rockefeller Family Fund, and the Stewart R. Mott Charitable Trust.

1. Louis D. Brandeis, What Publicity Can Do, Harper’s Wkly., Dec. 20, 1913, reprinted in Louis D. Brandeis, Other People’s Money and How the Bankers Use It 92, 92 (1932) (“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”).
Goldsmith told Congress: "There's no doubt that the extreme secrecy [associated with the Bush Administration's Terrorist Surveillance Program] . . . led to a lot of mistakes." More prosaically, even agency telephone directories have been removed from public access, along with numerous other categories of useful and formerly public information. Not only civil libertarians and public interest activists, but also defense and intelligence officials, now say that secrecy has gone too far and must be restrained. In particular, the classification system that restricts access to government information on national security grounds clearly is not serving its intended purpose. It has become an unwarranted obstacle to information-sharing inside and outside the government, to the detriment of public policy.

The "classification system is broken and is a barrier (and often an excuse) for not sharing pertinent information with homeland security partners," according to the Homeland Security Advisory Council, chaired by former FBI Director and former Director of Central Intelligence (DCI) William Webster. Others have independently reached identical conclusions. Stephen E. Flynn of the Council on Foreign Relations opined at a 2008 congressional hearing that "on the classification issue, there is just no question that the system is broken, fundamentally broken." Mr. Flynn observed further that "[b]ecause things get routinely overclassified, they can't get to the people who need [them]."

Concerns about excessive government secrecy have accompanied the national security classification system for decades. An official review in 1956 complained that, "overclassification has reached serious proportions." Entire shelves of commission reports, congressional hearings, and independent critiques since then have blasted official secrecy for improperly shielding govern-

---


6. *Id.*

ment operations from the public, impeding oversight, covering up rashness, and, ultimately, undermining national security itself.8

Successive waves of critics have rarely succeeded in devising effective solutions or strategies to mitigate the defective secrecy practices that they oppose. The persistent failure to achieve significant reforms over half a century suggests that these critics have not properly formulated their critiques or articulated recommendations in a way that would enable systemic changes. In recent years, in fact, classification—specifically overclassification—has increased, not diminished.

On the other hand, despite the fairly dismal record of the past fifty years, a small number of secrecy reform initiatives have yielded measurable differences in official secrecy policy, reducing the scope of classification activity, and increasing the pace of declassification. Why did those isolated efforts succeed? Can they be distinguished from the other well-intentioned initiatives that ultimately failed? Do they hold lessons for today’s potential reformers? This Essay seeks to identify the salient characteristics of successful secrecy reform programs in order to explain their successes and to inform future reform efforts. The following Part introduces national security secrecy, including its structure and operation, along with an explanation of its problematic features. Part II reviews the singularly unproductive history of efforts to reform and rationalize secrecy policy. Parts III and IV examine exceptions to this otherwise dismal history, in which significant reforms were accomplished with meaningful results. The remainder of the Essay proposes lessons for the future that may be derived from these successes.

I. THE BASICS OF NATIONAL SECURITY SECRECY

The purpose of the classification system is to prevent disclosure of information that could damage our national security. This straightforward definition, however, begs several questions: What is national security, if not the vitality of its democratic institutions that would be hobbled by secrecy? What constitutes damage? Who decides?

Even the architects and devotees of national security secrecy implicitly acknowledge that it represents a departure from the norms of democratic governance. In his 2003 executive order on classification policy, President George W. Bush affirmed both the norm and the departure:

Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security remains a priority.9

The presidential "nevertheless," which qualifies and limits the "free flow of information," has by now justified an enormous bureaucracy that implements and sustains the government secrecy system. By 2008, classification activity had increased to a total of more than 23 million classification actions per year.10 The most recent reported cost of protecting classified information in government and industry was a record annual high of $9.9 billion in 2007.11 "Unheard billions of pages of government records, some dating back to World War I, have remained inaccessible to the public on asserted national security grounds, and fateful government deliberations on questions of war and peace, human rights, and domestic surveillance have increasingly moved beyond public ken."

In practice, it is possible to distinguish at least three distinct categories of government secrecy. The first, "genuine national security secrecy," works to protect information that would pose an identifiable threat to the security of the nation by compromising its defense or the conduct of its foreign relations. Such information could include design details of weapons of mass destruction and other advanced military or intelligence technologies, current military operational plans, identities of intelligence sources, confidential diplomatic initiatives, and similarly sensitive matters. Protection of such information is not controversial. These safeguards are the raison d'être of the classification system, and the public interest is served when this type of information remains secure.

A second category that often masks itself as genuine national security secrecy, however, is actually something quite different. One might deem this version "bureaucratic secrecy." It reflects that natural tendency of bureaucracies, famously identified by Max Weber, to hoard information.12 Whether out of convenience or a dim suspicion that disclosure is intrinsically riskier than non-

12. Max Weber, Bureaucracy, in Essays in Sociology 196, 233-34 (H.H. Gerth & C. Wright Mills eds. & trans., Oxford Univ. Press 1946) ("Every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret.").
disclosure, government agencies always seem to err on the side of secrecy even when there is no obvious advantage to doing so.

When asked how much defense information in government is overclassified or unnecessarily classified, former Under Secretary of Defense for Intelligence Carol A. Haave told a House subcommittee in 2004 that it could be as much as fifty percent, an astonishingly high figure.\textsuperscript{13} Former Information Security Oversight Office Director J. William Leonard added: "I would put it almost even beyond 50/50... [T]here's over 50 percent of the information that, while it may meet the criteria for classification, really should not be classified..."\textsuperscript{14} "It may very well be that a lot of information is classified that shouldn't be," admitted Defense Secretary Donald Rumsfeld in a 2004 news conference, "or it's classified for a period longer than it should be."\textsuperscript{15} Yet these official acknowledgments of unnecessary secrecy have not prompted any reversal of course. In fact, the pace of classification activity has continued to increase each year, a tribute to the bureaucratic impulse.

The third category of secrecy, "political secrecy," uses classification authority for political advantage. While probably the smallest in quantitative terms, this form of secrecy is actually the most problematic and objectionable. It exploits the generally accepted legitimacy of genuine national security interests in order to advance a self-serving agenda, to evade controversy, or to thwart accountability. In extreme cases, political secrecy conceals violations of law and threatens the integrity of the political process itself.

In one unusually explicit example of the practice, a 1947 Atomic Energy Commission memorandum concerning "Medical Experiments on Humans" instructed as follows: "It is desired that no document be released which refers to experiments with humans and might have adverse effect on public opinion or result in legal suits. Documents covering such work... should be classified 'secret.'"\textsuperscript{16} This is by no means the only example of political secrecy. The CIA notoriously concealed the use of hallucinogens and other behavior-altering substances on unsuspecting persons in a behavior modification program code-named MKULTRA, and the Department of Energy hid the deliberate exposure of unwitting subjects to radiation in the early Cold War era. More recently, the Bush Administration secretly conducted domestic surveillance outside the

\textsuperscript{13} Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on Nat'l Sec, Emerging Threats and Int'l Relations of the H. Comm. on Gov't Reform, 108th Cong. 83 (2005) (statement of Carol A. Haave, Under Secretary of Defense for Intelligence).

\textsuperscript{14} Id. 83 (2005) (statement of J. William Leonard, Director, Information Security Oversight Office).


statutory framework and performed interrogations subjecting suspected enemy combatants to extreme mental and physical pain. As these examples show, political secrecy is often used to circumvent the institutions of law rather than to protect them.

If all government secrecy actions were uniformly bad or abusive, the public policy solution would be simple: to eliminate secrecy. If all government secrecy actions were necessary or prudent, no solution would be required, since there would be no problem. But in practice, government secrecy seems to be comprised of a shifting mix of the legitimate and the illegitimate. Genuine national security secrecy is diluted in an ocean of unnecessary bureaucratic secrets and defamed from time to time by abuse in the form of political secrecy. The enduring public policy problem is to disentangle the legitimate from the illegitimate, preserving the former and exposing the latter.

II. A BRIEF HISTORY OF SECRECY REFORM

Over the past fifty years, generations of critics have risen to attack, bemoan, lampoon, and correct the excesses of government secrecy. Only rarely have they had a measurable and constructive impact.

The 1956 Coolidge Committee, led by Assistant Secretary of Defense Charles Coolidge, identified widespread overclassification that it attributed to vague classification standards and lack of any associated accountability or punishment. The Coolidge Committee recommended the creation of a Director for Declassification within the Office of the Secretary of Defense and a reduction in the number of authorized classifiers.7 There is no record that these suggestions were ever adopted.

The 1970 Defense Science Board Task Force on Secrecy concluded that the amount of scientific and technical information that is classified "could profitably be decreased perhaps as much as 90 percent . . . ."8 The Task Force recommended a maximum classification lifetime of five years for most scientific and technical information and declassification of most currently classified technical information within two years.9 These recommendations were ignored.

The 1985 Stilwell Commission, chaired by the late Army General Richard G. Stilwell, again found that "too much information appears to be classified and much at higher levels than is warranted."10 From this commission's optimistic perspective, "[t]he remedy is straightforward: disciplined compliance with the

---

17. COMMITTEE ON CLASSIFIED INFORMATION REPORT, supra note 7 at 6, 13-14.
19. Id. at 2.
rules."²¹ Straightforward or not, however, the Commission’s advice had no discernable impact on the problem.

The 1994 Joint Security Commission reported to the Secretary of Defense and the DCI that, “the classification system, largely unchanged since the Eisenhower administration, has grown out of control.”²² Not only that, but “the classification system is not trusted on the inside any more than it is trusted on the outside. Insiders do not trust it to protect information that needs protection. Outsiders do not trust it to release information that does not need protection.”²³ The Joint Security Commission recommended adoption of a single classification level (offering two degrees of protection) to replace the existing three-level system.²⁴ This recommendation was not accepted.

The 1997 Moynihan Commission, chaired by the late Senator Daniel P. Moynihan, found that the secrecy system “is used too often to deny the public an understanding of the policymaking process . . . . There needs to be some check on the unrestrained discretion to create secrets.”²⁵ Toward that end, the Moynihan Commission recommended adopting legislation that would clearly define what may or may not be classified.²⁶ Such legislation was introduced in Congress, but it expired without a vote.

The 9/11 Commission also singled out secrecy as a problem, created to investigate the terrorist attacks of September 11, 2001 and to derive the public policy lessons that might be learned from them. The Commission explained in its 2004 final report that, “[c]urrent security requirements nurture overclassification and excessive compartmentation of information among agencies.”²⁷ The Commission recommended legislation to disclose the budgets of intelligence agencies and called for new incentives to reward information sharing.²⁸ In this case, the recommendations were largely accepted. Legislation to require disclosure of the intelligence budget total (though not the budgets of individual agencies) was enacted, and effective steps were taken to improve information shar-

21. Id. at 50.
23. Id.
24. Id. at 77.
26. Id. at xxii.
28. Id. at 416-17.
ing among government agencies. But the problem of systemic overclassification was unaffected.

Of course, not even the briefest account of secrecy reform's history could fail to mention the Freedom of Information Act (FOIA), which gave legal force to public requests for government information. The Act mandated the release of classified information upon request unless it was "properly classified." FOIA has been used successfully over the years to challenge the classification of particular records and to dislodge mountains of government documents (classified and unclassified) that would otherwise not have been released. But at its best, FOIA only facilitates access to specific records; it does not and cannot alter the practices and procedures that make them inaccessible in the first place. Thus, indispensable as it was and remains, FOIA did not provide an effective remedy for the excesses of government secrecy that were identified by the various secrecy reform efforts that preceded and followed the Act's passage in 1966.

Other targeted initiatives have likewise fallen short of systemic reform but did generate some success. The John F. Kennedy Assassination Records Collection Act and the Nazi War Crimes Disclosure Act each led to the declassification of significant bodies of historical records. President Clinton's 1995 executive order, which aimed to set a twenty-five-year lifetime for most classified documents, led to the declassification of approximately a billion pages of historically valuable records.

Yet these achievements, while intrinsically valuable and a boon to historians, did nothing to restrain the scope of current classification activity or to promote public access to contemporary records that were unnecessarily withheld. In that respect, the continuity of the complaints voiced by critics of government secrecy over the period reviewed in this Part is striking. Despite the intellectual firepower brought to bear and the political effort that was invested, very little has changed with respect to classification policy. The 1997 Moyhian Report stated with unusual self-awareness: "We started our work with the knowledge that many commissions and reports on government secrecy have preceded us, with little impact on the problems we still see and on the new

ones we have found." More than a decade later, the same may unfortunately be said of that commission and its report.

And yet, there are some remarkable exceptions to this discouraging record, namely secrecy reform proposals that produced results that were both tangible and instructive. Closer consideration of these exceptions provides practical guidance for contemporary efforts to control government secrecy.

III. The Interagency Security Classification Appeals Panel

One example of a successful secrecy reform was an unexpectedly effective new procedure for reconsidering agency decisions not to declassify and release a document. Executive Order 12,958 established a little-known Interagency Security Classification Appeals Panel (ISCAP) to consider appeals from members of the public whose requests for declassification review had been denied. Even those who devised the ISCAP scheme did not anticipate how well it would perform its assigned task.

The ISCAP is composed exclusively of executive branch officials, including representatives of the major national security agencies that are the most prolific classifiers: the Departments of Defense, State, and Justice; the CIA; the National Security Council; and the National Archives and Records Administration. Bringing these classifiers together to review individual agency classification decisions did not appear to be a radical innovation. But to the surprise of many observers, the ISCAP has proved to be an exceptionally independent and effective check on individual executive branch agency classification practices.

Incredibly, the ISCAP has voted more often than not to declassify records that the originating agency had refused to declassify. Between May 1996 and September 2008, the ISCAP considered appeals concerning 769 documents, and voted to declassify, in whole or in part, 495 of them. In other words, the Panel overruled the classification position of one of its own member agencies in a clear majority (64%) of the cases that were presented to it.

By comparison, one may note that federal courts, which have adopted a deferential posture to the executive branch on national security matters, almost never overturn agency classification decisions. There are no more than a few dozen FOIA cases over the past thirty years in which an agency's assertion of a classification exemption has been overruled by a court. Even then the decision was reached primarily on technical rather than substantive grounds.

35. MONTNINH COMMISSION REPORT, supra note 8, at xxii.
38. A Department of Justice tally identified only eighteen cases from 1979 to 1995 in which a court ordered disclosure of classified information, and several of those were reversed on appeal. Office of Info. Policy, U.S. Dep't of Justice, Litigation Review: History of Exemption 1 Disclosure Orders, 16 FOIA UPDATE 4 (1995).
Reflecting on the ISCAP’s record of granting appeals to declassify agency records, ISCAP Chair Roslyn A. Mazer averred in 1998: “I am confident that had just about all of these appeals been brought before the federal courts under the Freedom of Information Act, the appellant would not have prevailed, and the information would have remained classified unless the agency itself decided to declassify it.”

But under its own much more forthcoming procedures, ISCAP declassified the contested information.

The ISCAP soon became such a potent tool for challenging classification errors that one member agency, the CIA, sought relief from its jurisdiction. At first the CIA was unsuccessful. In 1999, the Justice Department Office of Legal Counsel produced an opinion that concluded that, contrary to the CIA’s position, “the DCl’s [classification] determinations are subject to substantive ISCAP review.”

But then in 2003, the CIA requested and received the authority from President George W. Bush to veto ISCAP decisions declassifying and disclosing CIA information. Such CIA vetoes of ISCAP decisions have been exercised in two reported cases. In recent years, the Panel has amassed a backlog of pending appeals, and it has never had the capacity to address more than a handful of classification challenges. But the ISCAP still retains its overall track record of voting to release information in the majority of classified documents presented to it.

What does the success of this program tell us? I believe that the actions of the ISCAP can best be understood in terms of the three categories of classified information described above: genuine national security secrecy, bureaucratic secrecy, and political secrecy. The ISCAP structure offers a way to winnow out the latter illegitimate forms of secrecy, while preserving its legitimate applications to justifiable ends.

All member agencies within the ISCAP share a commitment to genuine national security secrecy, i.e., the use of classification authority to protect legitimate secrets, and they have affirmed such secrecy whenever they encountered it. Former ISCAP Chair Mazer noted, for example, that, “[the ISCP?] member-

---

40. Id.
43. See 2008 OVERSIGHT OFFICE REPORT, supra note 10, at 20.
44. Id. at 19-20.
ship has consistently voted to retain classification of information that would identify a human intelligence source, even after thirty-plus years.\textsuperscript{45} But even though all of the member agencies may also practice their own illegitimate bureaucratic and political forms of secrecy, they evidently have no self-interest at stake in the bureaucratic or political uses of secrecy by other individual agencies. It turns out that they also have no patience for these activities. No federal judge or other external oversight body has been as ruthlessly effective in overturning unjustified classification actions as the ISCAP.\textsuperscript{46}

Essentially, the ISCAP process extended declassification authority beyond the agency that classified the information. In doing so, it removed bureaucratic and political self-interest from the equation, making it possible to distinguish legitimate national security secrecy from its impostors and to strip away the latter. This extension of declassification authority, though it may offend the autonomy of individual agencies, has improved the functioning of the overall classification system and is likely to have many other applications.

IV. The Fundamental Classification Policy Review

Another rare innovation in government secrecy policy that produced exceptional results was the Fundamental Classification Policy Review (FCPR) undertaken by the Department of Energy (DoE) in 1995.\textsuperscript{47} This process represented a dedicated effort to review, revise, and update the department’s classification guides—the templates for applying classification controls—with the declared intention of reducing the scope of DoE classification.\textsuperscript{48}

The FCPR emerged from the “Openness Initiative” led by Energy Secretary Hazel O’Leary. It was a bold effort to reverse the excesses of Cold War secrecy, to modernize the department’s security policies, and to rebuild flagging public confidence in DoE management of the troubled nuclear weapons complex. Secretary O’Leary declassified the complete list of U.S. nuclear explosive tests, released information on the history of U.S. production of plutonium and highly

\textsuperscript{45} Roslyn A. Mazer, Chair, Interagency Sec. Classification Appeals Panel, Remarks at the Joint Intelligence Community Information and Classification Management Conference (Nov. 2, 1998), available at http://www.fas.org/sgp/advisory/isicap/mazer98.html.

\textsuperscript{46} Courts have been reluctant to challenge executive branch secrecy judgments “for separation of powers reasons, for fear of becoming enmeshed in political questions, and out of concern that the judiciary lacks the expertise to reach appropriate decisions in these areas.” Meredith Fuchs, \textit{Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy}, \textit{58 Admin. L. Rev.} 131, 158 (2006). But these concerns are not well founded. See, e.g., \textit{id.} (arguing that the courts’ concerns lack a strong basis).


\textsuperscript{48} \textit{id}. at 3-4.
enriched uranium, and authorized release of previously classified aspects of inertial confinement fusion technology.

One of the more interesting aspects of the FCPR was the way in which it tackled the agency's entire classification infrastructure through an unprecedented systematic critical examination. The mission of the FCPR was to determine "what information must continue to be protected ... [and] which information no longer requires protection and should be made available to the public ..."49 Among the guiding principles was the view that, "[c]lassification must be based on explainable judgments of identifiable risk to national security and no other reason."50 Thus, "an identified benefit or need is not required to justify declassification and release to the public. Rather, the federal government must establish the reason for classification."51

The FCPR was conducted over a one-year period by fifty technical experts from the DoE, national laboratories, and other agencies, divided into seven topical working groups. The reviewers examined thousands of topics in hundreds of DoE classification guides, evaluated their continued relevance, and formulated recommendations for change. Significantly, public input was actively solicited at every stage of the process, from identification of the issues to review of the final draft recommendations. Following their year-long deliberations, the reviewers concluded that hundreds of categories of classified DoE information should be declassified. In some cases, they recommended increased protection for particularly sensitive categories of information. In large part, the reviewers' recommendations were adopted in practice.52

Other attempted secrecy reform initiatives tended to use general terms in outlining desired outcomes (e.g., more openness or less classification) or intermediate steps (e.g., legislation or a new executive order). But the FCPR distinguished itself by directly examining the decision to classify thousands of specific categories of information. The reviewers essentially queried: Were those decisions justifiable on genuine national security grounds? If so, they would be upheld. If not, the reviewer would eliminate them.

But perhaps the most remarkable feature of this exercise was that it mobilized the DoE bureaucracy itself as an agent of secrecy reform and not merely as its object. The defense mechanisms that would normally be triggered in response to legislative intervention or FOIA litigation—delay, defiance, or mere pro forma compliance—for the most part did not materialize. Instead, the DoE secrecy bureaucracy was effectively reprogrammed with a new mission: reduce secrecy

50. Id. at 17.
51. Id. at 17 n.12.
to the minimum necessary. That objective was satisfied to an unprecedented extent.

V. The Secrets of Effective Secrecy Reform

Against the desolate backdrop of futile criticism of government secrecy policy that has persisted for decades, the comparatively successful initiatives described above allow some inferences to be drawn regarding the elements of successful secrecy reform that could be applied in the future.

A. Secrecy Reform Is Best Pursued at the Agency Level

Practical secrecy reform is most effectively pursued at the agency level, where secrecy is actually implemented, rather than through abstract or hortatory government-wide statements of policy. The classification issues that arise in each major national security agency are substantively different, as are the associated security cultures. Intelligence agencies are concerned above all with the protection of sources and methods. Military agencies, for example, focus on the security of weapons technology and operational plans. Foreign policy agencies, on the other hand, must weigh the international impacts of classification and declassification.

Each agency that classifies information maintains its own classification guides, specifying in detail exactly what information may be classified and at what level. Furthermore, each agency is prone to overclassify different types of material. It follows that a successful retooling of the classification system must be undertaken where the real classification activity takes place: at the agency level, as the Energy Department’s PCSR shows. It is true that revisions to an executive order on classification can signal new directions for the entire executive branch and impose new limits, which are both desirable and necessary. But all such revisions will still need to be translated into concrete procedures.

Despite the centrality of individual agency secrecy procedures, they have been seriously neglected by overseers and reformers. A large fraction of agency classification guides have not been reviewed or updated for years, dating back to before the Bush administration’s 2003 revisions to classification policy. “Overall, 67 percent of the guides agencies reported as being currently in use had not been updated within the past five years,” according to the Information Security Oversight Office.53 This means that obsolete secrecy practices are being perpetuated automatically. Therefore, the single most productive secrecy reform action that could now be undertaken would be to conduct the equivalent of the Fundamental Classification Policy Review at each one of the major classifying agencies. In other words, the president could achieve a systematic reduction in government secrecy by directing each agency that classifies information to conduct a detailed public review of its classification policies with the objective of reducing secrecy to the essential minimum and declassifying everything that does not

53. 2008 OVERSIGHT OFFICE REPORT, supra note 10, at 23.
meet the standard for classification. Crucially, as with the DoE’s FCPR, the agencies themselves would be tasked to lead the secrecy reform process, not simply to endure it passively. Harnessing the bureaucracy in this way minimizes the likelihood of institutional foot-dragging or even sabotage. It could also produce some constructive tension among agencies, as they compete to see which can implement the president’s directive most effectively and which can generate the most significant reforms.

B. Extend Declassification Authority Beyond the Originating Agencies

If the task of secrecy reform is to disentangle legitimate from illegitimate secrecy and to uphold genuine national security secrecy while reducing and eliminating bureaucratic and political secrecy, then the track record of the ISCAP suggests that the most practical and effective method is to extend declassification authority beyond the agency in which it originated. This is the best way to nullify agency self-interest and purge it from the classification process.

This notion is generally abhorrent to most agencies, which doubt that other federal agencies can truly appreciate the sensitivity of “their” information. The CIA felt so strongly about the possibility that other agencies might order release of its information that it successfully petitioned the President for the authority to veto ISCAP decisions requiring the CIA to declassify information against its will. Nonetheless, something along these lines is essential to break down the self-serving barriers to disclosure produced by bureaucratic, illegitimate secrecy. If one executive branch agency cannot successfully explain to a senior official from another executive branch agency why the national security requires that a certain item be classified, then there is reason to doubt the necessity of its continued secrecy.

There is a dawning awareness that the days of unilateral agency control of information must come to a close. At his 2007 confirmation hearing to become Under Secretary of Defense for Intelligence, Lieutenant General James R. Clapper concurred with the statement that “the information gathered by the various [intelligence] collection agencies, such as CIA, NSA, and DIA, is not ‘owned’ by those agencies, and those agencies [should] not control decisions about who should get access to collected information.” But, he added, those decisions should be controlled by the Director of National Intelligence (DNI). Such change would constitute real progress, though it stops short of addressing over-classification in the Office of the DNI.

C. Encourage Experimentation and Pilot Projects

A qualitatively new twenty-first century information security policy that truly serves the national interest will not emerge spontaneously. Rather, it must

be approached incrementally in order to win acceptance and to correct initial errors. The process likely will start modestly in one corner of the government and then expand. The possibility of such innovations in security policy should be actively cultivated and encouraged through an officially sanctioned pilot program.

Security policy thus far has tended to be something of an intellectual backwater, where conformity and obedience are prized above all. These qualities have their place, but they need to be leavened by innovation and alertness to the lessons of experience. Small-scale tests of new approaches to information security could be explored at the individual program and agency level, and could be overseen and nurtured by the Obama Administration’s new Chief Technology Officer, who is charged with, among other things, promoting transparency.55

Almost by definition, innovation cannot be prescribed or institutionalized easily, but it can be rewarded and emulated where appropriate. Successful secrecy reform initiatives such as the FCPR and the ISCAP both began on a limited scale as experiments whose outcomes were uncertain. The FCPR was a one-year process within a single agency. The ISCAP is a low-activity operation that usually meets no more than once per month to consider only one or two dozen cases per year. More experiments and pilot projects in modifying classification policy are needed.

A fundamental transformation of the entire government secrecy system may be out of reach, at least as long as there is no consensus about what form it should take. But a series of small-scale experiments could help shape such a consensus and point to a new direction for the future. What if an agency or a program manager decided to treat documents marked “Confidential” (the lowest of the three classification levels) as unclassified? What if the inspector general at each agency were granted authority to declassify or downgrade any classified document in the agency that he or she concluded no longer required classification? What if all newly declassified documents in one agency were immediately scanned and placed on the agency’s website? Tests along these lines could be conducted on a limited scale and in such a way that, even if they went astray, would not incur much damage or expense. No matter the outcome, however, such efforts should provide valuable new insight into the process of innovation in security policy. Many such experiments are possible, and a few might succeed.

D. The Importance of Leadership

The last lesson that emerges from the intermittent success of secrecy reform is the essential role of high-level leadership. Any agency head might have undertaken an initiative akin to the FCPR, but only Secretary O’Leary did so. The Openness Initiative that she launched seems to have been attributable to idio-

syncratic factors as much as any others. It was true, as she said, that President Clinton had declared: "The more the American people know about their government the better they will be governed." Though Clinton directed that message to the entire executive branch, Secretary O'Leary was the only one of all the Clinton Administration agency heads who acted on it in a serious and systematic way.

Her actions reflect the Reagan-era maxim: "personnel is policy." In other words, the choice and placement of competent, motivated government employees is at least as important and influential as the wording of any particular policy statement. Dedicated and skillful personnel can flourish even in a policy vacuum, while obstructionist or incompetent persons can frustrate the most carefully conceived plans. We live in a democracy, but not all of us are "democrats" by instinct or inclination. That is to say, not all of us are equally committed to open, accountable government or to constructive engagement with members of the public. Indeed, some are actually quite hostile to such interaction.

A year ago, I requested a copy of a specific unclassified document from the CIA under FOIA. Despite repeated inquiries, the CIA FOIA staff would not acknowledge receipt of the request for six months. Even months later, this simple request remained open—neither granted nor denied. By contrast, a member of the FOIA staff at the Office of the DNI recently alerted me to the availability of a document that I had not even requested, because she knew I was interested in the subject. The basic difference in orientation reflected in these two encounters cannot be located in specific agency regulations or guidelines. It is a matter of personal characters and attitudes. And so, to a large extent, good personnel will produce good results. This is more easily stated than implemented. Improving the quality of the government workforce is a challenge for many reasons, including financial, educational, and demographic considerations.

When it comes to secrecy reform, though, improvements can be encouraged through employee performance evaluations that reward proper disclosure and through care in the nomination and confirmation process to select those individuals who truly value open government and limited secrecy. Fortunately, the most senior official of all—the President of the United States—has embraced open government as a guiding principle. "Starting today," President Obama remarked on his first full day in office, "every agency and department should know that this administration stands on the side not of those who seek to withhold information, but those who seek to make it known." As a result of this confluence of circumstances and personal commitments, there is now fertile ground for a transformation of inherited secrecy practices.

56. FCP Report, supra note 47, at 3.
Conclusion

Even in the inner chambers of the national security bureaucracy, it is now acknowledged that the secrecy system is dysfunctional and that its basic concepts are open to question. Remarkably, after more than fifty years of implementing national security classification policy, an internal Intelligence Community study admitted that, "[t]he definitions of 'national security' and what constitutes 'intelligence'—and thus what must be classified—are unclear." And so, unsurprisingly, the application of those definitions in practice produces murky results.

There is no disagreement in any domain that robust public access to government information is an essential characteristic of a vital democracy. Nor, on the other hand, is there any dispute that some types of government information require protection on national security grounds. Beyond these points, however, consensus gives way to confusion, inertia, and the weight of past practice. In 2007 and 2008, for example, the total budget for the National Intelligence Program was declassified, pursuant to legislation recommended by the 9/11 Commission. But earlier this year, the DNI rejected a request for disclosure of the 2006 intelligence budget total, declaring that it is properly classified. How can that be, when more recent information is freely disclosed? No sensible answer is forthcoming.

As a result of this incoherence and the mounting dissatisfaction with classification policy, the government secrecy system is now ripe for reform. The Obama Administration’s emphatic commitment to “creating an unprecedented level of openness in Government” provides the needed impetus for the reform process. If current reform efforts are to succeed, this Essay has argued that today’s reformers must recognize the failures of the past and learn the lessons of our occasional successes. Rhetorical statements of principle are fine and necessary. In order to change classification practice, though, it will be necessary to revise the classification process itself.

The alternative to indiscriminate secrecy is not indiscriminate openness. Rather, the new Administration should undertake a thoughtful, critical, and open review of individual agency classification guides to redefine the scope of national security secrecy in light of current geopolitical and technological realities. Nothing should ever be classified in the absence of an identifiable threat to national security. Declassification authority must be extended beyond the origi-


nating agency so as to mitigate the tendency toward bureaucratic secrecy. Other checks and balances on classification could be added to provide opportunities to identify and correct classification errors. Innovations and experiments in security policy should be promoted to identify fruitful directions for system-wide reform. "[T]here is a tendency to use the classification system to protect information which is not related to the national security," the Coolidge Committee observed in 1956, offering a familiar complaint that might have been uttered yesterday. According to its members, "[t]his constitutes an abuse of the classification system . . . and tends to destroy public confidence in the system." A solution to such classification abuse is long overdue, and now is finally within reach. The benefits of renewed sunlight for the health of our democracy are likely to be abundant.

63. Id.
Intelligence and the National Security Strategist: Enduring Issues and Challenges

edited by Roger Z. George and Robert D. Kline

PUBLISHED FOR THE SHERMAN KENT CENTER FOR INTELLIGENCE STUDIES
NATIONAL WAR COLLEGE
BY NATIONAL DEFENSE UNIVERSITY PRESS
WASHINGTON, D.C.
2004
Chapter 30

How Leaks of Classified Intelligence Help U.S. Adversaries: Implications for Laws and Secrecy

James B. Bruce

It is "obvious and inarguable" that no governmental interest is more compelling than the security of the Nation.

—U.S. Supreme Court in Haig v. Agee (1981)

To succeed, intelligence requires secrets. And secrecy is under assault. The future of U.S. intelligence effectiveness depends to a very significant degree on keeping its secrets about collection sources and methods and analytical techniques. When secrecy is breached, foreign targets of U.S. intelligence—such as adversary countries and terrorists—learn about intelligence techniques and operations, and then often develop denial and deception countermeasures to them. As a result, the effectiveness of intelligence declines, to the detriment of the national security policymakers and warfighters and the citizenry that it is meant to serve.

For years, the U.S. press has been an open vault of classified information on U.S. intelligence collection sources and methods. But now the problem is worse than ever before, given the scope and seriousness of leaks coupled with the power of electronic dissemination and search engines. The principal sources of intelligence information for U.S. newspapers, magazines, television, books, and the Internet are unauthorized disclosures of classified information. Press leaks reveal, individually and cumulatively, much about how secret intelligence works—and, by extension, how to defeat it.

This significant issue—the unauthorized disclosure of classified intelligence—has been extraordinarily resistant to correctives. It will never be solved without a frontal assault on many levels, and an essential one is U.S. law. This chapter addresses key legal issues in gaining better control over unauthorized disclosures that appear in

Source: This chapter is a slightly revised version of James B. Bruce, "Laws and Leaks of Classified Intelligence: The Consequences of Permissive Neglect," Studies in Intelligence 47, no. 1 (March 2003), 39–49.
the press. It advocates a range of legal solutions that have not been tried before, some of which are controversial. The views expressed here are my own.

Importantly, I would not hold these views had I not come to them from the vantage point of 21 years in the intelligence business, and particularly my last 8 with the Foreign Denial and Deception Committee. This committee represents an interagency effort to understand how foreign adversaries learn about, then try to defeat, our secret intelligence collection activities. I have come to appreciate that unauthorized disclosures of classified intelligence pose a serious, seemingly intractable, problem for U.S. national security. The Director of Central Intelligence (DCI), George Tenet, made the point in an interview that unauthorized disclosures "have become one of the biggest threats to the survival of U.S. Intelligence." A skeptical public can rightly question whether the DCI might not be exaggerating the seriousness of the problem. Unfortunately, he is not, and no intelligence specialist who is knowledgeable about the damage caused by leaks would disagree.

This presents an important anomaly in public discourse: Nearly all of the compelling evidence supporting the argument that leaks cause serious damage is available only in the classified domain. It thus seems daunting to make a persuasive public case for legal correctives to address unauthorized disclosures when so little of the evidence for it can be discussed publicly. Proponents for better laws—it will soon become clear why I am one of these—sometimes feel that this is not a fair fight. Freedom-of-the-press advocates and professional journalists exert disproportionate influence on this debate, at least when compared to advocates of criminal penalties for the leaking and publishing of sensitive classified intelligence. But I have come to believe that First Amendment objections to criminal penalties for disclosing classified intelligence now demand a more critical reconsideration than we have given them to date. When we can link these important constitutional issues in a balanced and dispassionate way, it will be more of a fair fight, a more reasoned debate.

**The Seriousness of Unauthorized Disclosures**

*Any sources and methods of intelligence will remain guarded in secret. My administration will not talk about how we gather intelligence, if we gather intelligence, and what the intelligence says. That's for the protection of the American people.*

—President George W. Bush, following the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon.

It is a myth, too commonly held outside the Intelligence Community (IC), that leaks really do not do much harm. The genealogy of this erroneous view traces to the publication of the *Pentagon Papers* in 1971. After much Government carping about all the damage that those top-secret revelations in the press would do to U.S. national security, few today would claim that any damage was done at all. And I am unaware of any that was done to intelligence. The *Pentagon Papers* flap took us off the scent. The view that leaks are harmless is further nourished by other popular myths that the Government overclassifies everything—including intelligence—and classifies way too much.
This seduction has become a creed among anti-secrecy proponents without clearances. But I would argue that this, too, at least in regard to intelligence, is wrong.

A recent classified study of media leaks has convincingly shown that leaks do cause a great deal of harm to intelligence effectiveness against priority national security issues, including terrorism. This is principally because the press has become a major source for sensitive information for our adversaries about U.S. intelligence—what it knows, what it does, and how it does it. Unfortunately, serious leaks of U.S. intelligence cumulatively provide substantial information to foreign adversaries. At the Central Intelligence Agency (CIA) alone, since 1995 there have been hundreds of investigations of potential media leaks of agency information, and a significant number of these have been referred to the Department of Justice for follow-up action. Leaks that have damaged the National Security Agency (NSA) signals intelligence sources and methods also number in the hundreds in recent years; dozens of these cases have also been referred to Justice. The National Imagery and Mapping Agency (NIMA) has experienced roughly a hundred leaks just since 2000 that have damaged U.S. imagery collection effectiveness. Many dozens of leaks on the activities and programs of the National Reconnaissance Office (NRO) have also helped foreign adversaries develop countermeasures to spaceborne collection operations. The Defense Intelligence Agency (DIA) and the military services, too, have suffered collection losses as a result of media leaks.

It is impossible to measure the damage done to U.S. intelligence through these leaks, but knowledgeable specialists assess the cumulative impact as truly significant. Some losses are permanent and irreversible; others can be recovered, though sometimes only partially, and with the expenditure of substantial resources that could well be spent elsewhere.

While leaks of classified information are often intended to influence or inform U.S. audiences, foreign intelligence services and terrorists are close and voracious readers of the American press. They are keenly alert to revelations of U.S. classified information. For example, Stanislav Lunev, a former Russian military intelligence officer, wrote:

I was amazed—and Moscow was very appreciative—at how many times I found very sensitive information in American newspapers. In my view, Americans tend to care more about scooping their competition than about national security, which made my job easier.5

I call this the Lunev Axiom: Classified intelligence disclosed in the press is the effective equivalent of intelligence gathered through foreign espionage. Several reported examples of Cold War-era intelligence losses due to press leaks concerned:

- Soviet ICBM testing, 1958. A New York Times story on January 31, 1958, reported that the United States was able to monitor the 8-hour countdown broadcasts for Soviet missile launches from Tyuratam (now Baykonur), Kazakhstan, which provided enough lead time to dispatch U.S. aircraft to observe the splashdowns and, thus, collect data used to estimate the accuracy of the intercontinental ballistic missiles. Following publication of the article,
Moscow cut the countdown broadcasts to 4 hours, too little time for U.S. aircraft to reach the landing area. Occurring in the midst of the missile-gap controversy, the publication of the press item left President Dwight Eisenhower livid. Reportedly, some intelligence was lost forever, and, to recoup the remainder, the U.S. Air Force had to rebuild an Alaskan airfield at a cost of millions of dollars.6

- Politburo conversations, 1971. In a September 16, 1971, column in The Washington Post, Jack Anderson wrote that U.S. intelligence was successfully intercepting telephone conversations from limousines used by members of the Soviet Politburo in Moscow. British historian Christopher Andrew says that this U.S. collection program producing highly sensitive information ended abruptly after Anderson’s revelations.7

- Soviet submarines, 1975. The Los Angeles Times published a story on February 7, 1975, that the CIA had mounted an operation to recover a sunken Soviet submarine from the Pacific Ocean floor. The New York Times ran its own version the next day. After this story broke, Jack Anderson further publicized the secret operation on national television on March 18. In his memoir, former DCI William Colby wrote: "There was not a chance that we could send the Glomar [Explorer] out again on an intelligence project without risking the lives of our crew and inciting a major international incident. . . . The Glomar project stopped because it was exposed."8

Importantly, not only Russian intelligence officers understand this. Key adversaries of the United States, such as China and al Qaeda, derive a significant amount of their information on the United States and U.S. intelligence from the media, including the Internet. What we need to understand are the legal implications of this key principle.

How Leaks Hurt: Some Post-Soviet Examples

The Intelligence Community faces improved foreign countermeasures as adversaries use leaks to expand their understanding of U.S. intelligence. Some more recent examples will illustrate the point.

M-11s in Pakistan. In the mid-1990s, dozens of press articles covered the issue of whether Chinese M-11 missiles had been covertly transferred to Pakistan. If missiles had been acquired, Pakistan could be found in violation of the Missile Technology Control Regime (MTCR), to which it was a signatory. Under the National Defense Authorization Act, U.S. law mandates sanctions against proven MTCR violators.

Reports in the Washington press claimed that U.S. intelligence had indeed found missiles in Pakistan but that the information apparently was not solid enough to trigger sanctions. Based on numerous leaks, readers of both the Washington Times and the Washington Post learned that intelligence had failed to convince the Department of State of the missiles’ existence. “Spy satellites,” the press announced, were unable to “confirm” the presence of such missiles. The message from the press coverage was, in effect, that any nation—such as Pakistan or other signatories to the MTCR who sought to circumvent its terms—could avert U.S. sanctions if they neutralized intelligence by
shielding missiles from satellite observation. These articles not only suggested to Pakistan and China that some key denial measures were succeeding but also spelled out specific countermeasures that other potential violators could take to prevent U.S. intelligence from satisfying the standards needed for sanctions under the MTCR.

**Indian nuclear testing.** U.S. imaging capabilities are a favorite press topic. An example is leaked intelligence about India's nuclear program in the mid-1990s. Unauthorized disclosures about issues such as this have revealed to our adversaries, directly and indirectly, unique elements that underpin our analytic tradecraft. Thoughtful manipulation by adversaries, as well as friends, of such knowledge exposed in the press impairs our ability to provide policymakers with timely intelligence before they are taken by surprise—as happened when the Intelligence Community failed to warn of the Indian nuclear tests in May 1998.⁹

**Liaison relationships.** Effective intelligence depends on cooperative relationships with friendly governments and individuals who trust the United States to protect their confidences. Press disclosures can—and sometimes do—undermine these relationships, making both governments and individuals reluctant to share information, thereby inhibiting intelligence support crucial to informed policymaking, counterterrorist efforts, and, when necessary, military operations.

**Iraqi weapons of mass destruction.** In 1998, newspaper reports provided lengthy coverage of the United Nations Special Commission charged with inspecting Iraq's weapons of mass destruction (WMD) facilities following the Gulf War. These reports were widely cited in subsequent worldwide media coverage. Although the articles contained many inaccuracies, information in them interfered with the U.S. Government's ability to aggressively pursue its policy on Iraqi weapons inspections. Other serious leaks clearly have degraded Washington's ability to obtain intelligence on Iraq. Damaging press disclosures based on imagery-derived intelligence on Iraq have included the movement of missile systems, construction of a new command and control network, and the dispersal of WMD equipment following the September 11, 2001, terrorist attacks in New York and Washington.

**Al Qaeda terrorism.** Terrorists feed on leaks. Through their investigations into whether the September 11 attacks resulted from intelligence failure, Congress and the special commission will learn that important intelligence collection capabilities against Osama bin Laden and al Qaeda were lost in the several years preceding September 2001. With the concurrence of NSA, the White House officially released just one example of these leaks. As press spokesman Ari Fleischer explained:

> And let me give you a specific example why, in our democracy and in our open system, it is vital that certain information remain secret. In 1998, for example, as a result of an inappropriate leak of NSA information, it was revealed about NSA being able to listen to Osama bin Laden on his satellite phone. As a result of the disclosure, he stopped using it. As a result of the public disclosure, the United States was denied the opportunity to monitor and gain information that could have been very valuable for protecting our country.¹⁰

276
What the public cannot easily know, because the overwhelming bulk of this intelligence must necessarily remain classified, is that the bin Laden example cited here is just the tip of the iceberg. In recent years, all intelligence agencies—CIA, NSA, NIMA, NRO, and DIA, to cite just the larger ones—have lost important collection capabilities, including against high-value terrorist targets. These losses have impaired human operations, signals intelligence, and imagery collection. And they have deprived U.S. analysts and policymakers of critical information, unavailable elsewhere, that they should have had.

**Weak Enforcement**

*The seriousness of the [unauthorized disclosures] issue has outpaced the capacity of extant administrative and law enforcement mechanisms to address the problem effectively.*

—Attorney General John Ashcroft

Logic and facts reveal a highly inverse correlation between law enforcement and leaks: the less the enforcement, the greater the leaks of classified information—and probably the other way around as well. A statistical approach is impossible, however, because there has been only a single example of any prosecution for an intelligence leak—Navy analyst Samuel Loring Morison in 1985. The glaring absence of criminal penalties for leaking and publishing classified intelligence establishes a law enforcement climate of utter indifference—actually permissive neglect. The unofficial message seems to be: Leak all you want, and no matter how much, or how serious, nothing will happen to you.

Perversely, for perpetrators there seem to be only benefits to leaking. Anonymous Government officials seek to skew public debate in their favor by selectively leaking intelligence that supports their favored policy positions. Journalists and book publishers can gain policy influence, brandishing relevant intelligence that their opponents may not have seen, and cannot easily refute—at least not in the press, without more leaks. But also, over time, journalists and writers can gain public renown and recognition—better newspaper, magazine, and book sales—as well as bigger incomes and profits, merely by exploiting the classified materials that law-breaking Government officials provide to them. This unholy alliance works exceedingly well as long as the legal climate remains indifferent to it.

**Laws on Leaks**

Is leaking classified intelligence against the law? Probably—but one would not know it from the prosecution data: only Morison would know for certain, and he was pardoned as President Bill Clinton was leaving office. President Clinton also vetoed the Shelby Amendment, an anti-leaks law written into the fiscal year 2001 Intelligence Authorization Act.

It is precisely the legal ambiguity of leaking that is the heart of this problem. Certainly there are laws against it—chiefly the 1917 espionage law (Title 18 USC §§ 793 (d)–(e) and 798) and the narrower Intelligence Identities Protection Act (Title
50 USC § 421). One could devote a whole legal seminar to what is wrong with these laws—and I urge legal experts to address this. But suffice it here to offer a non-lawyer's view that a law that is almost never enforced is either unneeded or useless. I contend that effective anti-leaks laws are urgently needed—but since the present ones are not enforced and virtually unenforceable, they are useless. Worse, consistent conspicuous failure to enforce these laws actually encourages the very crimes that they proscribe.

This problem is not new. The Willard Report (after its chairman Richard K. Willard, then-Deputy Assistant Attorney General) drew an unsettling conclusion two decades ago:

In summary, past experience with leak investigations has been largely unsuccessful and uniformly frustrating for all concerned.... This whole system has been so ineffectual as to perpetuate the notion that the Government can do nothing to stop the leaks.\(^{12}\)

Legal correctives proposed in the Willard Report resulted in draft legislation in 1984. Although supported by the Office of Management and Budget and the Reagan administration, the Intelligence Community later withdrew the draft legislation due to a perceived lack of support.

Twelve years later, responding to a request from the Assistant to the President for National Security Affairs, the National Counterintelligence Policy Board completed another study and reported no discernible change in the Government's ability to control leaks. The 1996 report explained the continuing failure to control leaks as a result of three key factors:

- a lack of political will to deal firmly and consistently with unauthorized executive branch and congressional leakers
- the use of unauthorized disclosures as a vehicle to influence policy
- the difficulty of prosecuting cases under existing statutes. Notably, not one of the five efforts to obtain legislation on unauthorized disclosures between 1981 and 1995 succeeded.\(^{13}\)

Why are press leaks so hard to investigate? In brief, the Government sources for classified information that is disclosed in the U.S. press are enormously difficult to identify. Intelligence that is disseminated to more than a few dozen officials will rarely be investigated if leaked because the list of potential offenders is already too long. Any intelligence that is disseminated electronically—as volumes are today—is largely shielded from any leaks investigations because identifying a single guilty leaker among hundreds or even thousands of innocent readers as a practical matter is extremely difficult.

Further, investigations within the intelligence agencies can rarely extend to consumers of their intelligence products—most of whom have policy equities to defend or oppose but have little discernible incentive to protect sources and methods or little understanding of the risks to them that leaking poses. And, unlike most of their intelligence-producer counterparts, intelligence consumers will probably never have to face a routine polygraph examination.
Moreover, because intelligence agencies are for the most part not law enforcement agencies, Federal press leak investigations require high-level authorization that is not routinely granted and must compete with other national security priorities, such as terrorism or espionage, for limited investigative resources. Also, long-standing enforcement policy (not law) has, to date, not sought to target journalists as a means of identifying their Government sources.

Finally, Government officials who provide classified information to the press are sometimes believed to be very senior, and thus more politically insulated from investigations, while lower-ranking officials who leak may be responding to higher-level direction, thus rationalizing a disclosure as “authorized.” Even as this kind of disclosure averts the formal declassification review process, it also complicates the legal issue by adding ambiguity over whether such a disclosure is authorized or not.

Given the palpable history of failure to protect classified intelligence information from press disclosures—and given the epidemic proportions of leaks and the deleterious consequences they wreak in foreign D&D countermeasures that reduce the effectiveness of U.S. collection—it is fair to question why past failed approaches should be expected to work today. They will not.

There has never been a general criminal penalty for unauthorized disclosures of classified intelligence. Although intelligence leaks technically can be prosecuted under the espionage statutes (18 U.S.C. §§ 793 and 798), only the single case, United States v. Morison, ever has been. Given that literally thousands of press leaks have occurred in recent years—many serious and virtually all without legal penalty—it is clear that current laws do not provide an effective deterrent to leakers or to journalists and their media outlets that knowingly publish classified intelligence.

Federal law enforcement officers would probably agree that bad laws are hard to enforce. A penetrating critique of what passes for anti-leak laws is provided in a comprehensive note in the June 1985 Virginia Law Review by Eric Ballou and Kyle McSlarrow. Although written before the Morison prosecution, the chief points remain as valid today as when written. A key passage highlights the responsibility of Congress:

The disjointed array of statutes shows that Congress does not have a comprehensive scheme to deal with the problem of leaks. The existing statutes either prohibit those disclosures with a specific intent to harm the United States or to advantage a foreign nation, or they apply only to a few narrowly defined categories of disclosures. The specific intent statutes do not apply to information leaks because of their high culpability standard. Those statutes are more appropriate to the problem of classic espionage. As a result, persons who leak [classified] information to further public debate may do so with impunity, as long as the information they disclose is not protected by one of the more narrowly directed statutes. A second infirmity of the specific intent statutes is that they only protect information relating to the national defense. These statutes do not cover diplomatic secrets, nonmilitary technology, and other nonmilitary secrets that affect the country's security. The more narrowly directed statutes, although protecting some of this information, nonetheless constitute an incomplete solution to the problem of leaks.
Congress has ignored large categories of information that should not be disclosed with impunity. In summary, Congress has not constructed a principled and consistent scheme of criminal sanctions to punish the disclosure of vital government secrets. Moreover, persons who leak government secrets are but one side of the problem; the government must also pursue remedies against those who publish secrets. Like the disclosure provisions, however, the statutes relevant to the publication of government secrets are vaguely drafted and incomplete.¹⁴

A Call for New Laws

Given the intractable nature of controlling leaks, we need to try remedies that have not been tried before. I defer to the drafting skills of competent attorneys to translate any promising ideas here into workable legislation. My suggestions are grouped into three categories: Write new laws. Amend old ones. And enforce them all—new or old.

Given the fact that many thousands of leaks of classified intelligence in recent years have seriously damaged intelligence effectiveness, thereby jeopardizing the Nation's security—and that existing penalties provide no effective deterrent to leaking—we urgently need a comprehensive anti-leaks statute to empower law enforcement and investigators to better protect intelligence. A new law should:

- unambiguously criminalize unauthorized disclosures of classified intelligence
- hold Government leakers accountable for providing classified intelligence to persons who do not have authorized access to that information, irrespective of intent; and hold unauthorized recipients accountable for publishing information that they know to be classified
- define intelligence information—including substantive content, activities, operations, sources and methods—distinctly from defense information, creating a discrete protected category for intelligence that does not require proof that it is related to military defense
- provide better protection to especially sensitive and highly classified intelligence information in trials and other judicial proceedings than is presently afforded through the Classified Information Procedures Act.

Congress can ensure that such legislation is drafted in a manner that is consistent with constitutional requirements.

In addition, a separate new law should be crafted to provide the same protection to technical sensors deployed on any platform (space, air, land, and sea) that is now afforded to human operations. Such a law would constitute a technical counterpart to the Intelligence Identities Protection Act (50 USC § 421).

Accountability

Should journalists have legal accountability? Absolutely, in my view. Few would dispute that the first line of enforcement must be drawn at offending Government officials who unlawfully steal and disclose classified intelligence. Like citizens everywhere, Government officers have different opinions on the propriety of holding
journalists legally accountable for publishing it. Still, I believe that to be fully effective, a worthy law should also hold cleared publicists—that is, journalists, writers, publishing companies, media networks, and Web sites that traffic in classified information—accountable for intelligence disclosures. Specifically, media representatives should be held responsible for publicizing—thus, making available to terrorists and other U.S. adversaries—intelligence information that they know to be classified.\textsuperscript{15} Whether journalists understand it or not—and many probably do not—the public exposure of significant intelligence often damages intelligence effectiveness by compromising valuable U.S. sources and methods. Journalists should also be held responsible under present criminal statutes for unlawful possession of classified documents when they have them.

Legal accountability for journalists is necessary because declassification authority is assigned by law exclusively to Government officials, elected and appointed, through lawful procedures. Journalists who publish classified intelligence arrogate to themselves an authority legally vested in Government that they do not by right possess. In publishing classified intelligence, no journalist can convincingly claim the constitutional right to do so. Any journalist’s First Amendment right to publish information does not appear to—and should not—extend to disclosing lawfully classified intelligence information. In any case, a constitutional claim of the right to publish classified intelligence remains to be established.

A close reading of Title 18 USC § 798 (sometimes referred to as the signals intelligence [SIGINT] statute) and 50 USC § 421 (the Intelligence Identities Protection Act, sometimes referred to as the human intelligence [HUMINT] statute) shows that journalists are already legally accountable for publishing leaked classified intelligence. But since no one has ever been prosecuted under these statutes, they remain unenforced and yet to be tested in the courts.

Like Government officials, journalists also exercise a public trust. But they exercise it without any apparent legal accountability for violating the public trust when they reveal the Nation’s secrets. This is wrong. Legal accountability for journalists is especially needed in the absence of an enforceable code of ethics for journalist conduct. The overwhelming majority of journalists do not publish classified information, and some recognize the ethical implications of compromising sensitive intelligence sources and methods.\textsuperscript{16} But a few egregious offenders traffic heavily in classified intelligence. In one example, Steven Aftergood, director of the Federation of the American Scientists’ anti-secrecy project, wrote: “Over the past couple of years, Mr. [Bill] Gertz [of the Washington Times] has written more stories based on classified Government documents than you can shake a stick at, infuriating Clinton administration officials and making a mockery of official classification policy.” Aftergood also repeated a statement from Gertz that ran in the conservative Weekly Standard: “We believe in stories that make you say ‘holy shit’ when you read them,” the columnist boasted.\textsuperscript{17} The complete lack of accountability of such journalists for costly compromises of information that jeopardize the Nation’s security must change under the force of law.
First Amendment Issues

Constitutional experts will address First Amendment implications of any proposed laws that may be interpreted to constrain freedom of the press. Importantly, the Supreme Court has not recognized an absolute right of publication. But neither has it made clear its conception of acceptable restrictions. Still, I believe that holding publishers of classified intelligence legally accountable under carefully drawn legislation would not be proscribed by the First Amendment.

Constitutional arguments that address First Amendment issues will have to consider the following:

- The Government’s exclusive authority to classify—and declassify—Government information is firmly established in law.
- The protection of sources and methods is also well established in both statutory law and judicial decisions, including a Supreme Court decision in Central Intelligence Agency v. Sims that recognizes the Government’s “compelling interest” in protecting the confidentiality of intelligence sources.
- Congress’ willingness to regulate publications disclosing intelligence where the potential for serious harm exists is already established in the Intelligence Identities Protection Act (50 USC § 421), and in the SIGINT statute (18 USC § 798) as well.\(^\text{18}\)
- One leaker (a Government employee, not a journalist) has been convicted of providing classified information to the press, and this decision was upheld on appeal.\(^\text{19}\)
- Publishing classified intelligence has not been established as a constitutionally protected right.
- A compelling argument can be made for extending the harm principle to protecting classified intelligence from press exposure when the Nation’s security is jeopardized as a consequence. For example, the media’s assistance (unwitting, to be sure) to the terrorists who planned and conducted the attacks in New York and Washington on September 11, 2001, provides a vivid example of harm to intelligence—and thus to the Nation—that deserved better protection than we now afford it.\(^\text{20}\)

Of course, the inherent tension between First Amendment rights and the Government’s interest in protecting national security is dynamic and may never be solved with finality. But the current balance so favors First Amendment rights that compelling constitutional interests involving national security can be superseded. Here we should entertain redressing a potential constitutional imbalance by reconsidering a time-tested democratic principle first developed by the preeminent philosopher of liberty, John Stuart Mill: “the only purpose for which power can rightfully be exercised over any member of a civilized community, against his will, is to prevent harm to others.”\(^\text{21}\)

Under the harm principle—for example, yelling “FIRE!” in a crowded theater when there is none—a variety of exceptions to free speech are well established in American law, such as obscenity, defamation, breach of peace, and “fighting words.”
To this list we should add: "the compromise of U.S. intelligence required in the service of the Nation’s security."

**Improving Existing Laws**

Referring to the conclusion of the 1996 report of the National Counterintelligence Policy Board, if we lack the political will to write a new law—and I am convinced that lack of will is our chief obstacle here—then I urge that we amend our present, defective laws to help us curtail the loss of present and future U.S. intelligence capabilities.

The statutory responsibility to “protect intelligence sources and methods from unauthorized disclosures” is explicitly assigned to the Director of Central Intelligence in the National Security Act of 1947 (Section 103), and similarly in the Central Intelligence Agency Act of 1949. The protection of sources and methods is also further authorized in Freedom of Information Act (FOIA) exemptions (in 5 USC § 552 (b) (1) and (b) (3)), and in several significant court cases including the Supreme Court decisions in *Snepp v. United States* and *Central Intelligence Agency v. Sims*. In *Snepp*, the Court established that “The government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service.”

Thus, perhaps the simplest approach to improving existing statutes is to amend the National Security Act of 1947 by melding Title 18 provisions criminalizing unauthorized disclosures of classified information with the well-established legal principle that intelligence sources and methods deserve special protection. Such an amendment would insert new language establishing criminal penalties for Government officials who leak classified information that damages sources and methods, as well as for uncleared writers and publishers who publicize this classified information in the media. Such language could be inserted immediately after Section 604, and the present Section 607 could be amended to specifically define “intelligence sources and methods.”

We could also amend the 1917 espionage statute (Title 18 USC § 793) to establish a distinct legal identity for intelligence information, activities, operations, sources, and methods—apart from national defense. Since considerable intelligence activities can be argued as unconnected with national defense, stricter definition would remove the need to satisfy an additional prosecutorial burden. We should also ease the burden of intent or “willfulness” standards, requiring only that the Government show that classified intelligence information was publicly disclosed. I would restrict any “intent” burden only to establishing a leaker’s intent to knowingly disclose classified intelligence instead of the higher culpability bar of establishing intended damage to the Nation.

I believe that we should also amend the Intelligence Identities Protection Act (50 USC § 421) to remove the burden of establishing patterns of disclosures, since some singular disclosures are so serious, perhaps resulting in loss of life, that legal penalties for exposing sensitive agents who risk their lives to help the United States and its allies must be clearly established. The intent standard should also be relaxed because
agent identities can be revealed to discerning readers (such as foreign intelligence services or terrorist organizations) through merely descriptive information even when actual names are withheld. And, unless we craft a new law to accomplish this, I would broaden the scope of this narrow statute that now covers only human operations to also apply to technical collection activity, including from spaceborne sensors.

Further, we should amend 18 USC § 794 to include nonstate actors such as terrorist organizations, along with "foreign governments or agents thereof" as is currently written, and soften the intent burden analogous to the amended § 793 above.

Finally, we need to amend the Classified Information Procedures Act to afford much greater protection during investigative and judicial proceedings for highly sensitive compartmented information, which, when leaked, may not even be investigated or officially reported for prosecution. This legal timidity results from an understandable Government incentive to avoid calling further attention to a particularly sensitive activity or capability. The U.S. Government has shown a debilitating reluctance to pursue legal remedies for the most serious leaks partly because subsequent courtroom publicity of sensitive information subverts its first objective of protecting such information from further disclosures.

**Strengthening Enforcement**

*Until those who, without authority, reveal classified information are deterred by the real prospect of productive investigations and strict application of appropriate penalties, they will have no reason to stop their harmful actions.*

—Attorney General John Ashcroft

Better enforcement will also require real political will—surely more than we have seen since United States v. Morison. Where to begin? First, acknowledge the Lunev Axiom: Recognize that Government leakers and the journalists who publish the classified materials they provide do the equivalent work of spies. Even if their motives differ, the effects can be the same. Through press leaks, unauthorized disclosures can be every bit as damaging as espionage because of the focused exploitation of the U.S. press by adversaries. If leakers and journalists were caught providing the same classified information clandestinely to a foreign power, they could, and some probably would, be prosecuted for espionage. But if published in the press—where leaked sensitive information becomes available to all foreign governments and terrorists, not just one—leakers and journalists alike derive effective immunity from prosecution under a Government that lacks the will to enforce its laws.

Let me state this categorically: Adversarial foreign countries and terrorists rely heavily on the U.S. press to acquire sensitive information about intelligence in order to deploy countermeasures against it. Since such disclosures can have the same effect as espionage, we should treat Government leakers and their collaborating journalists as subject to the same laws that apply to spies whose work is more clandestine, but sometimes no more damaging. While the espionage statutes are, for the most part, seriously flawed in their applicability to leaks, for the present they are all that
we have. Also, to date, neither leaker nor publisher has been taken to account under
laws specifically designed to protect against damaging disclosures of sensitive signals
or human intelligence. We should thus begin by trying to enforce the three pertinent
laws now on the books: 18 USC § 793 against leakers; 18 USC § 798 against leakers and
publishers of classified SIGINT information; and 50 USC § 421 against leakers and
publishers who expose HUMINT sources.

We should also enforce 18 USC § 794 against leakers and publishers of classified
intelligence whose disclosures injure the United States and advantage foreign nations
just as surely as any spies' disclosures that are provided clandestinely. Further, we
should empanel grand juries to determine criminal offenses for serious unauthorized
disclosures, and compel journalists under *Branzburg v. Hayes* (408 US 665, 1972) to
identify their law-breaking Government sources of classified intelligence. In addition,
we should subpoena in the course of legal proceedings to recover stolen Government
property—classified intelligence documents that we believe are in the possession of
Government leakers or journalists, and thus outside the normal physical protections
that the U.S. Government provides to sensitive classified intelligence information.
Government officials, journalists, and publishers who are found to be in possession of
documentary classified intelligence should also be prosecuted under 18 USC § 641 for
possession of stolen Government property.

We need to recognize that sensitive intelligence information is classified by this
Government for good reasons—precisely because its protection really is essential to
the security of the Nation. But the legal protections we afford it are woefully insuffi-
cient, and not nearly as good as those we provide to other Government or Govern-
ment-protected information—such as banking, agricultural, and census data, and
even crop estimates and insider trading for securities—whose acquisition by foreign
adversaries and terrorists would not make any difference at all.

**Consequences of Not Acting**

"If the law supposed that," said Mr. Bumble, "the law is an ass."

—Charles Dickens, *Oliver Twist*

The consequences of legal inaction are high—perhaps higher than we should
ask the American citizen to bear. Years of inaction, indifference, and permissive ne-
glect are taking an enormous and unacceptable toll on U.S. intelligence capabilities.
And the toll is higher still since September 11, 2001. Intelligence leaks do serious and
often irreversible damage to our sensitive collection capabilities. By publicly unveiling
unique and often fragile collection capabilities through leaks, the media actively help
our adversaries to weaken U.S. intelligence. These disclosures offer valuable insights
to our enemies—at no cost to them—into possible errors in their assessments of how
well or poorly U.S. intelligence works against them, as well as useful feedback on how
well they succeed or fail in countering U.S. intelligence. This kind of feedback not
only facilitates more effective intelligence denial activities, it also increases the risk of
foreign manipulation of our intelligence for deception operations.
Unless comprehensive measures with teeth are taken to identify and hold leakers and their publishing collaborators accountable for the significant, often irreversible, damage they inflict on vital U.S. intelligence capabilities, the damage will continue unabated. Conceivably, without some legally effective corrective action, the situation could even worsen, leading to intelligence on significant national security issues that is less accurate, less complete, and less timely than it would be without foreign countermeasures made possible by unauthorized disclosures. Warning of surprise attacks against the United States by terrorists or other hostile adversaries could be further degraded. Moreover, multi-billion-dollar collection programs could become less effective—and therefore, less cost-effective—than they would otherwise be if foreign adversaries were not learning how to neutralize or manipulate such programs through unauthorized disclosures.

The alternative is better intelligence capabilities for the United States. This can result through no added costs by merely better protecting the sources and methods we now have and those that are in the pipeline. Stemming press leaks will afford significantly better protection. Better laws—and enforcement of these laws—will make this possible. If we continue to be encumbered by a failure of will, our present climate of permissive neglect will become one of pernicious neglect.

Notes

1 This chapter is a slightly revised version of an article entitled "Laws and Leaks of Classified Intelligence: The Consequences of Permissive Neglect," in Studies in Intelligence 47, no. 1 (March 2003), 39-49. While this chapter has been reviewed by the Central Intelligence Agency for classified content, the views expressed here are those of the author and not necessarily those of the CIA, the National Intelligence Council, or other U.S. Government organizations.

2 USA Today, October 11, 2000, 15A.

3 The scope of my concern with classified information here extends only to intelligence, which encompasses intelligence information, activities, operations, sources, and methods. I exclude from my purview other kinds of classified information, such as military (for example, war plans and weapons systems) and diplomatic secrets, not because they are unimportant, but because I believe that intelligence increasingly requires a distinct legal identity.


6 Wayne Jackson, Allen Welsh Dulles, Director of Central Intelligence (July 1973, declassified history, volume 4, 29-31, Record Group 263, National Archives).

7 Christopher Andrew, For the President’s Eyes Only (New York: Harper Perennial, 1966), 359.


9 In the case of India’s nuclear program, damaging press leaks further disclosed sources and methods beyond the data revealed in the official demarches delivered in 1995 and 1998.


17 The concept that persons outside of government as well as inside it should face criminal penalties for knowingly disclosing classified information is discussed in Ballou and McLarney, section 1.B.2., and has been discussed at least since 1957; see the Wright Commission’s *Report of the Commission on Government Security* (Washington, DC: Government Printing Office, 1957), xxii.


20 Ballou and McLarney.


22 The significant example identified by Ari Fleischer (see note 10) is far from an isolated case. Numerous others in the classified literature show damage to counterterrorist capabilities in all collection disciplines, particularly SIGINT and HUMINT.


24 *Snepp v. United States*, 444 US 507, 509 n.3 (1980), and *Central Intelligence Agency v. Sims*, 471 US 159, 177 (1985). In *Sims*, the Court anticipated the Lunsford Axiom and implicitly identified a D&D rationale in protecting sources and methods: “Foreign intelligence services have both the capacity to gather and analyze any information that is in the public domain and the substantial expertise in deducing the identities of intelligence sources from seemingly unimportant details . . . .” Cited in Ballou and McLarney. Discussion here is also based on Jay Ryan, “Criminalizing the Publication of Classified Information: The Clash between National Security and the First Amendment,” unpublished paper, April 24, 2003, 6–8.

25 Ryan, 9–10.

26 Letter to the Speaker of the House, 5.
U.S. Supreme Court

Totten v. United States, 92 U.S. 105 (1875)

Totten v. United States

92 U.S. 105

APPEAL FROM THE COURT OF CLAIMS

Syllabus

An action cannot be maintained against the government in the Court of Claims upon a contract for secret services during the war made between the President and the claimant.

MR. JUSTICE FIELD delivered the opinion of the Court.

This case comes before us on appeal from the Court of Claims. The action was brought to recover compensation for services alleged to have been rendered by the claimant's intestate, William A. Lloyd, under a contract with President Lincoln, made in July, 1861, by which he was to proceed south and ascertain the number of troops stationed at different points in the insurrectionary states, procure plans of forts and fortifications, and gain such other information as might be beneficial

Page 92 U. S. 106

to the government of the United States, and report the facts to the President; for which services he was to be paid $200 a month.

The Court of Claims finds that Lloyd proceeded under the contract within the rebel lines and remained there during the entire period of the war, collecting and from time to time transmitting information to the President, and that upon the close of the war he was only reimbursed his expenses. But the court, being equally divided in opinion as to the authority of the President to bind the United States by the contract in question, decided, for the purposes of an appeal, against the claim and dismissed the petition.

We have no difficulty at to the authority of the President in the matter. He was undoubtedly authorized during the war, as commander-in-chief of the armies of the United States, to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy, and contracts to compensate such agents are so far binding upon the government as to render it lawful for the President to direct payment of the amount stipulated out of the contingent fund under his control. Our objection is not to the contract, but to the action upon it in the Court of Claims. The service stipulated by the contract was a secret service; the information sought was to be obtained clandestinely, and was to be communicated privately; the employment and the service were to be equally concealed. Both employer and agent must
have understood that the lips of the other were to be forever sealed respecting the relation of either to the matter. This condition of the engagement was implied from the nature of the employment, and is implied in all secret employments of the government in time of war or upon matters affecting our foreign relations where a disclosure of the service might compromise or embarrass our government in its public duties or endanger the person or injure the character of the agent. If upon contracts of such a nature an action against the government could be maintained in the Court of Claims whenever an agent should deem himself entitled to greater or different compensation than that awarded to him, the whole service in any case, and the manner of its discharge, with the details of dealings

Page 92 U. S. 107

with individuals and officers, might be exposed, to the serious detriment of the public. A secret service, with liability to publicity in this way, would be impossible, and, as such services are sometimes indispensable to the government, its agents in those services must look for their compensation to the contingent fund of the department employing them and to such allowance from it as those who dispense that fund may award. The secrecy which such contracts impose precludes any action for their enforcement. The publicity produced by an action would itself be a breach of a contract of that kind, and thus defeat a recovery.

It may be stated as a general principle that public policy forbids the maintenance of any suit in a court of justice the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential and respecting which it will not allow the confidence to be violated. On this principle, suits cannot be maintained which would require a disclosure of the confidences of the confessional, or those between husband and wife, or of communications by a client to his counsel for professional advice, or of a patient to his physician for a similar purpose. Much greater reason exists for the application of the principle to cases of contract for secret services with the government, as the existence of a contract of that kind is itself a fact not to be disclosed.

*Judgment affirmed.*
UNITED STATES V. REYNOLDS, 345 U. S. 1 (1953)

U.S. Supreme Court

United States v. Reynolds, 345 U.S. 1 (1953)

No. 21. Argued October 21, 1952

Decided March 9, 1953

345 U.S. 1

CERTIORARI TO THE UNITED STATES COURT OF APPEALS

FOR THE THIRD CIRCUIT

Syllabus

A military aircraft on a flight to test secret electronic equipment crashed, and certain civilian observers aboard were killed. Their widows sued the United States under the Tort Claims Act and moved under Rule 34 of the Federal Rules of Civil Procedure for production of the Air Force's accident investigation report and statements made by surviving crew members during the investigation. The Secretary of the Air Force filed a formal claim of privilege, stating that the matters were privileged against disclosure under Air Force regulations issued under R.S. § 161, and that the aircraft and its personnel were "engaged in a highly secret mission." The Judge Advocate General filed an affidavit stating that the material could not be furnished "without seriously hampering national security," but he offered to produce the surviving crew members for examination by plaintiffs and to permit them to testify as to all matters except those of a "classified nature."

Held: in this case, there was a valid claim of privilege under Rule 34; and a judgment based under Rule 37 on refusal to produce the documents subjected the United States to liability to which Congress did not consent by the Tort Claims Act. Pp. 345 U. S. 2-12.

(a) As used in Rule 34, which compels production only of matters "not privileged," the term "not privileged" refers to "privileges" as that term is understood in the law of evidence. P. 345 U. S. 6.
(b) When the Secretary lodged his formal claim of privilege, he invoked a privilege against revealing military secrets which is well established in the law of evidence. Pp. 345 U. S. 6-7.

Page 345 U. S. 2

(c) When a claim of privilege against revealing military secrets is invoked, the courts must decide whether the occasion for invoking the privilege is appropriate, and yet do so without jeopardizing the security which the privilege was meant to protect. Pp. 345 U. S. 7-8.

(d) When the formal claim of privilege was filed by the Secretary, under circumstances indicating a reasonable possibility that military secrets were involved, there was a sufficient showing of privilege to cut off further demand for the documents on the showing of necessity for its compulsion that had been made. P. 345 U. S. 10.

(e) In this case, the showing of necessity was greatly minimized by plaintiffs' rejection of the Judge Advocate General's offer to make the surviving crew member available for examination. P. 345 U. S. 11.

(f) The doctrine in the criminal field that the Government can invoke its evidentiary privileges only at the price of letting the defendant go free has no application in a civil forum, where the Government is not the moving party, but is a defendant only on terms to which it has consented. P. 345 U. S. 12.

192 F.2d 987 reversed.

In a suit under the Tort Claims Act, the District Court entered judgment against the Government. 10 F.R.D. 468. The Court of Appeals affirmed. 192 F. 2d 987. This Court granted certiorari. 343 U.S. 918. Reversed and remanded, p. 345 U. S. 12.

MR. CHIEF JUSTICE VINSON delivered the opinion of the Court.

These suits under the Tort Claims Act [Footnote 1] arise from the death of three civilians in the crash of a B-29 aircraft at

Page 345 U. S. 3

Waycross, Georgia, on October 6, 1948. Because an important question of the Government's privilege to resist discovery [Footnote 2] is involved, we granted certiorari. 343 U.S. 918.

The aircraft had taken flight for the purpose of testing secret electronic equipment, with four civilian observers aboard. While aloft, fire broke out in one of the bomber's engines. Six of the nine crew members, and three of the four civilian observers were killed in the crash.
The widows of the three deceased civilian observers brought consolidated suits against the United States. In the pretrial stages, the plaintiffs moved, under Rule 34 of the Federal Rules of Civil Procedure, [Footnote 3] for production of the Air Force's official accident investigation report and the statements of the three surviving crew members, taken in connection with the official investigation. The Government moved to quash the motion, claiming that these matters were privileged against disclosure pursuant to Air Force regulations promulgated under R.S. § 161. [Footnote 4] The District Judge sustained plaintiffs' motion, holding that good cause for production had been shown. [Footnote 5] The claim of privilege under R.S. § 161 was rejected on the premise that the Tort Claims Act, in making the Government liable "in the same manner" as a private individual, [Footnote 6] had waived any privilege based upon executive control over governmental documents.

Shortly after this decision, the District Court received a letter from the Secretary of the Air Force stating that "it has been determined that it would not be in the public interest to furnish this report . . . ." The court allowed a rehearing on its earlier order, and, at the rehearing, the Secretary of the Air Force filed a formal "Claim of Privilege." This document repeated the prior claim based generally on R.S. § 161, and then stated that the Government further objected to production of the documents "for the reason that the aircraft in question, together with the personnel on board, were engaged in a highly secret mission of the Air Force." An affidavit of the Judge Advocate General, United States Air Force, was also filed.

with the court, which asserted that the demanded material could not be furnished "without seriously hampering national security, flying safety and the development of highly technical and secret military equipment." The same affidavit offered to produce the three surviving crew members, without cost, for examination by the plaintiffs. The witnesses would be allowed to refresh their memories from any statement made by them to the Air Force, and authorized to testify as to all matters except those of a "classified nature."

The District Court ordered the Government to produce the documents in order that the court might determine whether they contained privileged matter. The Government declined, so the court entered an order, under Rule 37(b)(2)(i), [Footnote 7] that the facts on the issue of negligence would be taken as established in plaintiffs' favor. After a hearing to determine damages, final judgment was entered for the plaintiffs. The Court of Appeals affirmed, [Footnote 8] both as to the showing of good cause for production of the documents and as to the ultimate disposition of the case as a consequence of the Government's refusal to produce the documents.
We have had broad propositions pressed upon us for decision. On behalf of the Government, it has been urged that the executive department heads have power to withhold any documents in their custody from judicial view if they deem it to be in the public interest. [Footnote 9] Respondents have asserted that the executive's power to withhold documents was waived by the Tort Claims Act. Both positions have constitutional overtones which we find it unnecessary to pass upon, there being a narrower ground for decision, *Touhy v. Ragen*, 340 U. S. 462 (1951); *Rescue Army v. Municipal Court of Los Angeles*, 331 U. S. 549, 331 U. S. 574-585 (1947).

The Tort Claims Act expressly makes the Federal Rules of Civil Procedure applicable to suits against the United States. [Footnote 10] The judgment in this case imposed liability upon the Government by operation of Rule 37, for refusal to produce documents under Rule 34. Since Rule 34 compels production only of matters "not privileged," the essential question is whether there was a valid claim of privilege under the Rule. We hold that there was, and that therefore the judgment below subjected the United States to liability on terms to which Congress did not consent by the Tort Claims Act.

We think it should be clear that the term "not privileged" as used in Rule 34, refers to "privileges" as that term is understood in the law of evidence. When the Secretary of the Air Force lodged his formal "Claim of Privilege," he attempted therein to invoke the privilege against revealing military secrets, a privilege which is well established in the law of evidence. [Footnote 11] The existence of the privilege is conceded by the court below, [Footnote 12] and, indeed, by the most outspoken critics of governmental claims to privilege. [Footnote 13]

Judicial experience with the privilege which protects military and state secrets has been limited in this country. [Footnote 14] English experience has been more extensive, but still relatively slight compared with other evidentiary privileges. [Footnote 15] Nevertheless, the principles which control the application of the privilege emerge quite clearly from the available precedents. The privilege belongs to the Government, and must be asserted by it; it can neither be claimed [Footnote 16] nor waived [Footnote 17] by a private party. It is not to be lightly invoked. [Footnote 18] There must be formal claim of privilege, lodged by the head of the department which has control over the matter, [Footnote 19] after actual personal consideration by that officer. [Footnote 20] The court itself must determine whether the circumstances are appropriate for the claim of privilege, [Footnote 21] and yet do so without forcing a disclosure of the very thing the privilege is designed to protect. [Footnote 22] The latter requirement is the only one which presents real difficulty. As to it, we find it helpful to draw upon judicial experience in dealing with an analogous privilege, the privilege against self-incrimination.
The privilege against self-incrimination presented the courts with a similar sort of problem. Too much judicial inquiry into the claim of privilege would force disclosure of the thing the privilege was meant to protect, while a complete abandonment of judicial control would lead to intolerable abuses. Indeed, in the earlier stages

Page 345 U. S. 9

of judicial experience with the problem, both extremes were advocated, some saying that the bare assertion by the witness must be taken as conclusive, and others saying that the witness should be required to reveal the matter behind his claim of privilege to the judge for verification. [Footnote 23] Neither extreme prevailed, and a sound formula of compromise was developed. This formula received authoritative expression in this country as early as the Burr trial. [Footnote 24] There are differences in phraseology, but, in substance, it is agreed that the court must be satisfied from all the evidence and circumstances, and

"from the implications of the question, in the setting in which it is asked, that a responsive answer to the question or an explanation of why it cannot be answered might be dangerous because injurious disclosure could result."

Hoffman v. United States, 341 U. S. 479, 341 U. S. 486-487 (1951). [Footnote 25] If the court is so satisfied, the claim of the privilege will be accepted without requiring further disclosure.

Regardless of how it is articulated, some like formula of compromise must be applied here. Judicial control over the evidence in a case cannot be abdicated to the

Page 345 U. S. 10

caprice of executive officers. Yet we will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case. It may be possible to satisfy the court, from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the occasion for the privilege is appropriate, and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.

In the instant case, we cannot escape judicial notice that this is a time of vigorous preparation for national defense. Experience in the past has made it common knowledge that air power is one of the most potent weapons in our scheme of defense, and that newly developing electronic devices have greatly enhanced the effective use of air power. It is equally apparent that these electronic devices must be kept secret if their full military advantage is to be exploited in the national interests. On the record before the trial court, it appeared that this accident occurred to a military plane which had gone aloft to test secret electronic equipment. Certainly there was a reasonable danger that the
accident investigation report would contain references to the secret electronic equipment which was the primary concern of the mission.

Of course, even with this information before him, the trial judge was in no position to decide that the report was privileged until there had been a formal claim of privilege. Thus, it was entirely proper to rule initially that petitioner had shown probable cause for discovery of the documents. Thereafter, when the formal claim of privilege was filed by the Secretary of the Air Force, under

Page 345 U. S. 11

circumstances indicating a reasonable possibility that military secrets were involved, there was certainly a sufficient showing of privilege to cut off further demand for the document on the showing of necessity for its compulsion that had then been made.

In each case, the showing of necessity which is made will determine how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate. Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted, but even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake. [Footnote 26] A fortiori, where necessity is dubious, a formal claim of privilege, made under the circumstances of this case, will have to prevail. Here, necessity was greatly minimized by an available alternative, which might have given respondents the evidence to make out their case without forcing a showdown on the claim of privilege. By their failure to pursue that alternative, respondents have posed the privilege question for decision with the formal claim of privilege set against a dubious showing of necessity.

There is nothing to suggest that the electronic equipment, in this case, had any causal connection with the accident. Therefore, it should be possible for respondents to adduce the essential facts as to causation without resort to material touching upon military secrets. Respondents were given as reasonable opportunity to do just that when petitioner formally offered to make the surviving crew members available for examination. We think that offer should have been accepted.

Page 345 U. S. 12

Respondents have cited us to those cases in the criminal field, where it has been held that the Government can invoke its evidentiary privileges only at the price of letting the defendant go free. [Footnote 27] The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense. Such rationale has no application in a civil forum, where the Government is not the moving party, but is a defendant only on terms to which it has consented.
The decision of the Court of Appeals is reversed, and the case will be remanded to the District Court for further proceedings consistent with the views expressed in this opinion.

_Reversed and remanded._

MR. JUSTICE BLACK, MR. JUSTICE FRANKFURTER, and MR. JUSTICE JACKSON dissent substantially for the reasons set forth in the opinion of Judge Maris below. 192 F.2d 987.

[Footnote 1]


[Footnote 2]

Federal Rules of Civil Procedure, Rule 34.

[Footnote 3]

"Rule 34. Discovery and Production of Documents and Things for Inspection, Copying, or Photographing. Upon motion of any party showing good cause therefor and upon notice to all other parties, and subject to the provisions of Rule 30(b), the court in which an action is pending may (1) order any party to produce and permit the inspection and copying or photographing, by or on behalf of the moving party, of any designated documents, papers, books, accounts, letters, photographs, objects, or tangible things, not privileged, which constitute or contain evidence relating to any of the matters within the scope of the examination permitted by Rule 26(b) and which are in his possession, custody, or control; or (2) order any party to permit entry upon designated land or other property in his possession or control for the purpose of inspecting, measuring, surveying, or photographing the property or any designated object or operation thereon within the scope of the examination permitted by Rule 26(b). The order shall specify the time, place, and manner of making the inspection and taking the copies and photographs and may prescribe such terms and conditions as are just."

[Footnote 4]

5 U.S.C. § 22:

"The head of each department is authorized to prescribe regulations, not inconsistent with law, for the government of his department, the conduct of its officers and clerks, the distribution and performance of its business, and the custody, use, and preservation of the records, papers, and property appertaining to it."

Air Force Regulation No. 62-7(5)(b) provides:
"Reports of boards of officers, special accident reports, or extracts therefrom will not be furnished or made available to persons outside the authorized chain of command without the specific approval of the Secretary of the Air Force."

[Footnote 5]

10 F.R.D. 468.

[Footnote 6]

28 U.S.C. § 2674:

"The United States shall be liable, respecting the provisions of this title relating to tort claims, in the same manner and to the same extent as a private individual under like circumstances, but shall not be liable for interest prior to judgment or for punitive damages."

[Footnote 7]

"Rule 37. Refusal to Make Discovery: Consequences."

"* * * *"

"(b) Failure to Comply With Order."

"* * * *"

"(2) Other Consequences. If any party or an officer or managing agent of a party refuses to obey . . . an order made under Rule 34 to produce any document . . . , the court may make such orders in regard to the refusal as are just, and, among others, the following:"

"(i) An order that the matters regarding which the questions were asked, or the character or description of the thing or land, or the contents of the paper, or the physical or mental condition of the party, or any other designated facts shall be taken to be established for the purposes of the action in accordance with the claim of the party obtaining the order. . . ."

[Footnote 8]

192 F.2d 987.

[Footnote 9]

[Footnote 10]"

[Footnote 11]

Totten v. United States, 92 U.S. 105, 92 U.S. 107 (1875); Firth Sterling Steel Co. v. Bethlehem Steel Co., 199 F. 353 (1912); Pollen v. Ford Instrument Co., 26 F.Sup. 583 (1939); Cresmer v. United States, 9 F.R.D. 203 (1949); see Bank Line v. United States, 68 F.Sup. 587 (1946), 163 F.2d 133 (1947). 8 Wigmore on Evidence (3d ed.) § 2212(a), p. 161, and § 2378(g)(5), at pp. 785 et seq.; 1 Greenleaf on Evidence (16th ed.) §§ 250-251; Sanford, Evidentiary Privileges Against the Production of Data Within the Control of Executive Departments, 3 Vanderbilt L.Rev. 73, 74-75 (1950).

[Footnote 12]

192 F.2d 987, 996.

[Footnote 13]

See Wigmore, op. cit. supra, note 11

[Footnote 14]

See cases cited supra, note 11

[Footnote 15]


[Footnote 16]


[Footnote 17]

In re Grove, 180 F. 62 (1910).

[Footnote 18]

Marshall, C.J., in the Aaron Burr trial, I Robertson's Reports 186:

"That there may be matter, the production of which the court would not require is certain. . . . What ought to be done under such circumstances presents a delicate question, the discussion of which, it is hoped, will never be rendered necessary in this country."
[Footnote 19]

Firth case, supra, note 16

[Footnote 20]

"The essential matter is that the decision to object should be taken by the minister who is the political head of the department, and that he should have seen and considered the contents of the documents, and himself have formed the view that, on grounds of public interest, they ought not to be produced. . . ."


[Footnote 21]

Id. at 642:

"Although an objection validly taken to production, on the ground that this would be injurious to the public interest, is conclusive, it is important to remember that the decision ruling out such documents is the decision of the judge. . . . It is the judge who is in control of the trial, not the executive. . . ."

(Emphasis supplied.)

[Footnote 22]

Id. at pp. 638-642; cf. the language of this Court in Hoffman v. United States, 341 U. S. 479, 341 U. S. 486 (1951), speaking of the analogous hazard of probing too far in derogation of the claim of privilege against self-incrimination:

"However, if the witness, upon interposing his claim, were required to prove the hazard in the sense in which a claim is usually required to be established in court, he would be compelled to surrender the very protection which the privilege is designed to guarantee."

(Emphasis supplied.)

[Footnote 23]

Compare the expressions of Rolfe, B. and Willes, C.J., in Regina v. Garbett, 2 C. & K. 474, 492 (1847); see 8 Wigmore on Evidence (3d ed.) § 2271.

[Footnote 24]

I Robertson's Reports 244:
"When a question is propounded, it belongs to the Court to consider and decide whether any direct answer to it can implicate the witness; if this be decided in the negative, then he may answer it without violating the privilege which is secured to him by law. If a direct answer to it may criminate himself, then he must be the sole judge what his answer would be. The Court cannot participate with him in this judgment, because they cannot decide on the effect of his answer without knowing what it would be, and a disclosure of that fact to the judges would strip him of the privilege which the law allows and which he claims."

[Footnote 25]

Brown v. United States, 276 U. S. 134 (1928); Mason v. United States, 244 U. S. 362 (1917).

[Footnote 26]

See Totten v. United States, 92 U. S. 105 (1875), where the very subject matter of the action, a contract to perform espionage, was a matter of state secret. The action was dismissed on the pleadings without ever reaching the question of evidence, since it was so obvious that the action should never prevail over the privilege.

[Footnote 27]

United States v. Andolschek, 142 F.2d 503 (1944); United States v. Beekman, 155 F.2d 580 (1946).