

The Protection of Classified Information: The Legal Framework

Jennifer K. Elsea
Legislative Attorney

January 10, 2013

Congressional Research Service
7-5700
www.crs.gov
RS21900

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

The publication of secret information by *WikiLeaks* and multiple media outlets, followed by news coverage of leaks involving high-profile national security operations, has heightened interest in the legal framework that governs security classification and declassification, access to classified information, agency procedures for preventing and responding to unauthorized disclosures, and penalties for improper disclosure. Classification authority generally rests with the executive branch, although Congress has enacted legislation regarding the protection of certain sensitive information. While the Supreme Court has stated that the President has inherent constitutional authority to control access to sensitive information relating to the national defense or to foreign affairs, no court has found that Congress is without authority to legislate in this area.

This report provides an overview of the relationship between executive and legislative authority over national security information, and summarizes the current laws that form the legal framework protecting classified information, including current executive orders and some agency regulations pertaining to the handling of unauthorized disclosures of classified information by government officers and employees. The report also summarizes criminal laws that pertain specifically to the unauthorized disclosure of classified information, as well as civil and administrative penalties. Finally, the report describes some recent developments in executive branch security policies and relevant legislative activity.

Contents

Background 1
Executive Order 13526 3
Handling of Unauthorized Disclosures 5
- Information Security Oversight Office 6
- Intelligence Community 7
- Department of Defense 8

Penalties for Unauthorized Disclosure 10
- Criminal Penalties 10
- Civil Penalties and Other Measures 10

Declassification vs. Leaks and "Instant Declassification" 11
Recent Developments 14
- Executive Branch Initiatives 14
- Congressional Activity 15

Contacts

Author Contact Information 17

Background

Prior to the New Deal, classification decisions were left to military regulation.[1] In 1940, President Franklin Roosevelt issued an executive order authorizing government officials to protect information pertaining to military and naval installations.[2] Presidents since that time have continued to set the federal government's classification standards by executive order, but with one critical difference: while President Roosevelt cited specific statutory authority for his action, later presidents have cited general statutory *and constitutional* authority.[3]

The Supreme Court has never directly addressed the extent to which Congress may constrain the executive branch's power in this area. Citing the President's constitutional role as Commander-in-Chief,[4] the Supreme Court has repeatedly stated in dicta that "[the President's] authority to classify and control access to information bearing on national security ... flows primarily from this Constitutional investment of power in the President and exists quite apart from any explicit congressional grant."[5] This language has been interpreted by some to indicate that the President has virtually plenary authority to control classified information. On the other hand, the Supreme Court has suggested that "Congress could certainly [provide] that the Executive Branch adopt new [classification procedures] or [establish] its own procedures—subject only to whatever limitations the Executive Privilege may be held to impose on such congressional ordering."[6] In fact, Congress established a separate regime in the Atomic Energy Act for the protection of nuclear-related "Restricted Data."[7]

Congress has directed the President to establish procedures governing the access to classified material so that no person can gain such access without having undergone a background check.[8]

---

[1] *See* Harold Relyea, *The Presidency and the People's Right to Know*, in THE PRESIDENCY AND INFORMATION POLICY 1, 16-18 (1981).

[2] Exec. Order No. 8381 (1940).

[3] *Compare* Exec. Order No. 10501 (1953) *with, e.g.*, Exec. Order No. 13292 (2003). The most recent Executive Order on classified information, Exec. Order No. 13526 (Dec. 29, 2009), also cites constitutional authority.

[4] U.S. CONST., art. II, §2.

[5] Department of the Navy v. Egan, 484 U.S. 518, 527 (1988) (quoting Cafeteria Workers v. McElroy, 367 U.S. 886, 890 (1961). In addition, courts have also been wary to second-guess the executive branch in areas of national security. *See, e.g.,* Haig v. Agee, 453 U.S. 280, 291 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention."). The Court has suggested, however, that it might intervene where Congress has provided contravening legislation. *Egan* at 530 ("Thus, *unless Congress specifically has provided otherwise*, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs.")(emphasis added).

[6] EPA v. Mink, 410 U.S. 73, 83 (1973).

[7] 42 U.S.C. §2011 *et seq*. In addition, the Invention Secrecy Act (codified at 35 U.S.C. §181 *et seq*.) authorizes the Commissioner of Patents to keep secret those patents on inventions in which the government has an ownership interest and the widespread knowledge of which would, in the opinion of the interested agency, harm national security. For a more detailed discussion of these and other regulatory regimes for the protection of sensitive government information, *see* CRS Report RL33502, *Protection of National Security Information*, by Jennifer K. Elsea; CRS Report RL33303, *"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information*.

[8] Counterintelligence and Security Enhancement Act of 1994, Title VIII of P.L. 103-359 (codified at 50 U.S.C. §435 *et seq*.). Congress has also required specific regulations regarding personnel security procedures for employees of the National Security Agency, P.L. 88-290, 78 Stat. 168, codified at 50 U.S.C. §§831 - 835. Congress has also prohibited the Department of Defense from granting or renewing security clearances for officers, employees, or contract personnel who had been convicted of a crime (and served at least one year prison time) and for certain other reasons, with a (continued...)

Congress also directed the President, in formulating the classification procedures, to adhere to certain minimum standards of due process with regard to access to classified information.[9] These include the establishment of uniform procedures for, *inter alia*, background checks, denial of access to classified information, and notice of such denial.[10] The statute also explicitly states that the agency heads are not required to comply with the due process requirement in denying or revoking an employee's security clearance where doing so could damage national security, although the statute directs agency heads to submit a report to the congressional intelligence committees in such a case.[11]

With the authority to determine classification standards vested in the President, these standards tend to change whenever a new administration takes control of the White House.[12] The differences between the standards of one administration and the next have often been dramatic. As one congressionally authorized commission put it in 1997:

> The rules governing how best to protect the nation's secrets, while still insuring that the American public has access to information on the operations of its government, past and present, have shifted along with the political changes in Washington. Over the last fifty years, with the exception of the Kennedy Administration, a new executive order on classification was issued each time one of the political parties regained control of the Executive Branch. These have often been at variance with one another ... at times even reversing outright the policies of the previous order.[13]

Various congressional committees have investigated ways to bring some continuity to the classification system and to limit the President's broad powers to shield information from public examination.[14] In 1966, Congress passed the Freedom of Information Act (FOIA), creating a presumption that government information will be open to the public unless it falls into one of FOIA's exceptions. One exception covers information that, under executive order, must be kept secret for national security or foreign policy reasons.[15] In 2000, Congress enacted the Public Interest Declassification Act of 2000,[16] which established the Public Interest Declassification Board to advise the President on matters regarding the declassification of certain information, but the act expressly disclaims any intent to restrict agency heads from classifying or continuing the classification of information under their purview, nor does it create any rights or remedies that

(...continued)

waiver possible only in "meritorious cases," P.L. 106-398 §1, Div. A, Title X, §1071(a), 114 Stat. 1654, 10 U.S.C. §986.

[9] 50 U.S.C. §435(a).

[10] *Id.*

[11] *Id.* §435(b). The House Conference Report that accompanied this legislation in 1994 suggests that Congress understood that the line defining the boundaries of executive and legislative authority in this area is blurry at best. The conferees made explicit reference to the *Egan* case, expressing their desire that the legislation not be understood to affect the President's authority with regard to security clearances. *See* H.R. REP. 103-753, at 54.

[12] *See Report of the Commission on Protecting and Reducing Government Secrecy*, S. DOC. NO. 105-2, at 11 (1997).

[13] *Id.*

[14] *See, e.g., Availability of Information from Federal Departments and Agencies: Hearings Before the House Committee on Government Operations*, 85th Cong. (1955).

[15] 5 U.S.C. §552(b)(1). The Supreme Court has honored Congress's deference to executive branch determinations in this area. EPA v. Mink, 410 U.S. 73 (1973). Congress, concerned that the executive branch may have declared some documents to be "national security information" that were not vital to national security, added a requirement that such information be "properly classified pursuant to an executive order." 5 U.S.C. §552(b)(1)(B).

[16] P.L. 106-567, title VII, Dec. 27, 2000, 114 Stat. 2856, 50 U.S.C. §435 note.

may be enforced in court.[17] Most recently, Congress passed the Reducing Over-Classification Act, P.L. 111-258, which, among other things, requires executive branch agencies' inspectors general to conduct assessments of their agencies' implementation of classification policies.[18]

Executive Order 13526

The present standards for classifying and declassifying information were last amended on December 29, 2009.[19] Under these standards, the President, Vice President, agency heads, and any other officials designated by the President may classify information upon a determination that the unauthorized disclosure of such information could reasonably be expected to damage national security.[20] Such information must be owned by, produced by, or under the control of the federal government, and must concern one of the following:

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities, intelligence sources/methods, cryptology;
- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to national security;
- federal programs for safeguarding nuclear materials or facilities;
- vulnerabilities or capabilities of national security systems; or
- weapons of mass destruction.[21]

Information may be classified at one of three levels based on the amount of danger that its unauthorized disclosure could reasonably be expected to cause to national security.[22] Information is classified as "Top Secret" if its unauthorized disclosure could reasonably be expected to cause "exceptionally grave damage" to national security. The standard for "Secret" information is "serious damage" to national security, while for "confidential" information the standard is "damage" to national security. Significantly, for each level, the original classifying officer must identify or describe the specific danger potentially presented by the information's disclosure.[23] In case of significant doubt as to the need to classify information or the level of classification

[17] *Id.* §§705 and 707.

[18] P.L. 111-258, §6, codified at 50 U.S.C. §435 note.

[19] Classified National Security Information, Exec. Order No. 13526, 3 C.F.R. 298 (2009). For a more detailed description and analysis, see CRS Report R41528, *Classified Information Policy and Executive Order 13526*, by Kevin R. Kosar.

[20] Exec. Order No. 13526 §1.1. The unauthorized disclosure of foreign government information is presumed to damage national security. *Id.* §1.1(b).

[21] *Id.* §1.4. In addition, when classified information which is incorporated, paraphrased, restated, or generated in a new form, that new form must be classified at the same level as the original. *Id.* §§2.1 - 2.2.

[22] *Id.* §1.2.

[23] *Id.* Classifying authorities are specifically prohibited from classifying information for reasons other than protecting national security, such as to conceal violations of law or avoid embarrassment. *Id.* §1.7(a).

appropriate, the information is to remain unclassified or be classified at the lowest level of protection considered appropriate.[24]

The officer who originally classifies the information establishes a date for declassification based upon the expected duration of the information's sensitivity. If the office cannot set an earlier declassification date, then the information must be marked for declassification in 10 years' time or 25 years, depending on the sensitivity of the information.[25] The deadline for declassification can be extended if the threat to national security still exists.[26]

Classified information is required to be declassified "as soon as it no longer meets the standards for classification."[27] The original classifying agency has the authority to declassify information when the public interest in disclosure outweighs the need to protect that information.[28] On December 31, 2006, and every year thereafter, all information that has been classified for 25 years or longer and has been determined to have "permanent historical value" under Title 44 of the U.S. Code will be automatically declassified, although agency heads can exempt from this requirement classified information that continues to be sensitive in a variety of specific areas.[29]

Agencies are required to review classification determinations upon a request for such a review that specifically identifies the materials so that the agency can locate them, unless the materials identified are part of an operational file exempt under the Freedom of Information Act (FOIA)[30] or are the subject of pending litigation.[31] This requirement does not apply to information that has undergone declassification review in the previous two years; information that is exempted from review under the National Security Act;[32] or information classified by the incumbent President and staff, the Vice President and staff (in the performance of executive duties), commissions appointed by the President, or other entities within the executive office of the President that advise the President.[33] Each agency that has classified information is required to establish a system for periodic declassification reviews.[34] The National Archivist is required to establish a similar systemic review of classified information that has been transferred to the National Archives.[35]

---

[24] *Id.* §§1.1-1.2. This presumption is a change from the predecessor order.

[25] Exec. Order No. 13526 at §1.5. Exceptions to the time guidelines are reserved for information that can be expected to reveal the identity of a human intelligence source or key design concepts of weapons of mass destruction. *Id*.

[26] *Id.* §1.5(c).

[27] *Id.* §3.1(a).

[28] *Id.* §3.1(d).

[29] *Id.* §3.3.

[30] 5 U.S.C. §552. For more information, see CRS Report R41406, *The Freedom of Information Act and Nondisclosure Provisions in Other Federal Laws* , by Gina Stevens.

[31] Exec. Order No. 13526 §3.5.

[32] 50 U.S.C. §§403-5c, 403-5e, 431.

[33] Exec. Order No. 13526 §3.5.

[34] *Id.* §3.4. "Need-to-know" is based on a determination within the executive branch in accordance with relevant directives that a prospective recipient "requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." *Id.* §6.1(dd).

[35] *Id.* §3.4. Exec. Order No. 13526 creates a new National Declassification Center (NDC) within the National Archives to facilitate and standardize the declassification process. *Id.* §3.7. For more information about the NDC, see CRS Report R41528, *Classified Information Policy and Executive Order 13526*, by Kevin R. Kosar

Access to classified information is generally limited to those who demonstrate their eligibility to the relevant agency head, sign a nondisclosure agreement, and have a need to know the information.[36] The need-to-know requirement can be waived, however, for former Presidents and Vice Presidents, historical researchers, and former policy-making officials who were appointed by the President or Vice President.[37] The information being accessed may not be removed from the controlling agency's premises without permission. Each agency is required to establish systems for controlling the distribution of classified information.[38]

The Information Security Oversight Office (ISOO)—an office within the National Archives—is charged with overseeing compliance with the classification standards and promulgating directives to that end.[39] ISOO is headed by a Director, who is appointed by the Archivist of the United States, and who has the authority to order declassification of information that, in the Director's view, is classified in violation of the aforementioned classification standards.[40] In addition, there is an Interagency Security Classifications Appeals Panel ("the Panel"), headed by the ISOO Director and made up of representatives of the heads of various agencies, including the Departments of Defense, Justice, and State, as well as the Central Intelligence Agency, and the National Archives.[41] The Panel is empowered to decide appeals of classifications challenges[42] and to review automatic and mandatory declassifications. If the ISOO Director finds a violation of E.O. 13526 or its implementing directives, then the Director must notify the appropriate classifying agency so that corrective steps can be taken.

Handling of Unauthorized Disclosures

Under E.O. 13526, each respective agency is responsible for maintaining control over classified information it originates and is responsible for establishing uniform procedures to protect classified information and automated information systems in which classified information is stored or transmitted. Standards for safeguarding classified information, including the handling, storage, distribution, transmittal, and destruction of and accounting for classified information, are developed by the ISOO. Agencies that receive information classified elsewhere are not permitted to transfer the information further without approval from the classifying agency. Persons authorized to disseminate classified information outside the executive branch are required to ensure it receives protection equivalent to those required internally. In the event of a knowing, willful, or negligent unauthorized disclosure (or any such action that could reasonably be expected to result in an unauthorized disclosure), the agency head or senior agency official is required to notify ISOO and to "take appropriate and prompt corrective action." Officers and employees of the United States (including contractors, licensees, etc.) who commit a violation are subject to sanctions that can range from reprimand to termination.[43]

[36] *Id.* §4.1.

[37] *Id.* §4.4.

[38] *Id.* §4.2.

[39] *Id.* §5.2.

[40] *Id.* §3.1(c).

[41] *Id.* §5.3.

[42] *Id.* §5.3(b)(1) - (3) For example, an authorized holder of classified information is allowed to challenge the classified status of such information if the holder believes that status is improper. *Id.* §1.8.

[43] *Id.* §5.5. Specifically, administrative sanctions available with respect to "officers and employees of the United States (continued...)

Executive Order 12333, United States Intelligence Activities,[44] spells out the responsibilities of members of the Intelligence Community[45] for the protection of intelligence information, including intelligence sources and methods. Under section 1.7 of E.O. 12333, heads of departments and agencies with organizations in the Intelligence Community (or the heads of such organizations, if appropriate) must report possible violations of federal criminal laws to the Attorney General "in a manner consistent with the protection of intelligence sources and methods."

Information Security Oversight Office

ISOO Directive No. 1 (32 CFR Part 2001) provides further direction for agencies with responsibilities for safeguarding classified information. Sec. 2001.41 states:

> Authorized persons who have access to classified information are responsible for: (a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person; (b) Meeting safeguarding requirements prescribed by the agency head; and (c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

Sec. 2001.45 of ISOO Directive No. 1 requires agency heads to establish a system of appropriate control measures to limit access to classified information to authorized persons. Sec. 2001.46 requires that classified information is transmitted and received in an authorized manner that facilitates detection of tampering and precludes inadvertent access. Persons who transmit classified information are responsible for ensuring that the intended recipients are authorized to receive classified information and have the capacity to store classified information appropriately. Documents classified "Top Secret" that are physically transmitted outside secure facilities must be properly marked and wrapped in two layers to conceal the contents, and must remain under the constant and continuous protection of an authorized courier. In addition to the methods prescribed for the outside transmittal of Top Secret documents, documents classified at Secret or Confidential levels may be mailed in accordance with the prescribed procedures. Agency heads

(...continued)

Government, and its contractors, licensees, certificate holders, and grantees" accused of violating government security regulations, "knowingly, willfully, or negligently," 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." *See infra* section "Civil Penalties and Other Measures."

[44] 46 Fed. Reg. 59,941 (1981), as amended by Exec .Order No. 13284, 68 Fed. Reg. 4,077 (2003), Exec. Order No. 13355, 69 Fed. Reg. 53,593 (2004) and Exec. Order No. 13470, 73 Fed. Reg. 45,328 (2008). A version of the Order as amended is available at http://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

[45] The Intelligence Community is defined by 50 U.S.C. § 401a(4) and E.O. 12333 to include the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency (CIA), the Bureau of Intelligence and Research of the Department of State (INR), the National Security Service of the Federal Bureau of Investigation (FBI), the Office of Intelligence and Analysis of the Department of Homeland Security (DHS), the Office of Intelligence or the Coast Guard (CG), other DHS elements concerned with the analysis of intelligence information, the Office of Intelligence and Analysis of the Treasury Department, the Energy Department, the Drug Enforcement Agency (DEA), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), the National Geospatial Intelligence Agency (NGA), Army Intelligence, Air Force Intelligence, Navy Intelligence, and Marine Corps Intelligence, as well as "[s]uch other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community."

are required to establish procedures for receiving classified information in a manner that precludes unauthorized access, provides for detection of tampering and confirmation of contents, and ensures the timely acknowledgment of the receipt (in the case of Top Secret and Secret information).

Sec. 2001.48 prescribes measures to be taken in the event of loss, possible compromise or unauthorized disclosure. It states: "Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose."

Agency heads are required to establish appropriate procedures to conduct an inquiry or investigation into the loss, possible compromise or unauthorized disclosure of classified information, in order to implement "appropriate corrective actions" and to "ascertain the degree of damage to national security." The department or agency in which the compromise occurred must also advise any other government agency or foreign government agency whose interests are involved of the circumstances and findings that affect their information or interests. Agency heads are to establish procedures to ensure coordination with legal counsel in any case where a formal disciplinary action beyond a reprimand is contemplated against a person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads are to ensure coordination with the Department of Justice and the legal counsel of the agency where the individual believed to be responsible is assigned or employed. Violators are generally subject to imprisonment or fine, and in some cases, loss of retirement or other benefits.

Intelligence Community

The most recent intelligence community directives related to the safeguarding of classified information appear to be Intelligence Community Directive (ICD) 700, Protection of National Intelligence, effective June 7, 2012,[46] and ICD 701, Security Policy Directive for Unauthorized Disclosures of Classified Information, effective March 14, 2007.[47] ICD 700 mandates an integration of counterintelligence and security functions for the purpose of protecting national intelligence and sensitive information and, among other things, to strengthen "deterrence, detection, and mitigation of insider threats, defined as personnel who use their authorized access to do harm to the security of the US through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of resources or capabilities."[48] Under ICD 701, Senior Officials of the Intelligence Community (SOICs)[49] are to promptly notify the Director of National Intelligence (DNI) and, if appropriate, law enforcement authorities of any actual or suspected unauthorized disclosure of classified information, including any media leak, that is likely to cause damage to national security interests, unless the disclosure is the subject of a counterespionage or counterintelligence investigation. Disclosures to be reported include:

> Unauthorized disclosure to an international organization, foreign power, agent of a foreign power, or terrorist organization;

[46] Available at http://www.dni.gov/files/documents/ICD/ICD_700.pdf.

[47] Available at http://www.fas.org/irp/dni/icd/icd-701.pdf.

[48] ICD 700 §D.3.c.

[49] Senior Officials of the Intelligence Community (SOICs) means "heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations." Exec. Order No. 12333 at §1.7.

> National intelligence activities or information that may be at risk of appearing in the public media, either foreign or domestic, without official authorization;
>
> Loss or compromise of classified information that poses a risk to human life;
>
> Loss or compromise of classified information that is indicative of a systemic compromise;
>
> Loss or compromise of classified information storage media or equipment;
>
> Discovery of clandestine surveillance and listening devices;
>
> Loss or compromise of classified information revealing U.S. or a foreign intelligence partner's intelligence operations or locations, or impairing foreign relations;
>
> Such other disclosures of classified information that could adversely affect activities related to US national security; and
>
> Loss or compromise of classified information revealing intelligence sources or methods, US intelligence requirements, capabilities and relationships with the US Government.

Upon determining that a compromise meeting the above reporting criteria has or may have occurred, the SOIC is required promptly to report it to the DNI, through the Special Security Center (SSC), and to any other element with responsibility for the material at issue. The SOIC is then required to provide updated reports as appropriate (or as directed). This process occurs in tandem with any required reporting to law enforcement authorities.

The required formal notification to the DNI is to include a complete statement of the facts, the scope of the unauthorized disclosure, sources and methods that may be at risk, the potential effect of the disclosure on national security, and corrective or mitigating actions. SOICs are further required to identify all factors that contributed to the compromise of classified information and take corrective action or make recommendations to the DNI.

Department of Defense

Department of Defense Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public" (July 22, 2005)[50] governs procedures for handling unauthorized disclosures of classified information to the public. In the event of a known or suspected disclosure of classified information, the heads of DoD components must report the incident to the Deputy Secretary of Defense of Intelligence and conduct a preliminary investigation to confirm that classified information was disclosed, identify the particulars of the incident and who was involved, ascertain whether the information was properly classified or was authorized to be released, and identify any leads that might identify the person or persons responsible. The preliminary investigation should also ascertain whether further inquiry might increase the damage caused by the compromise.

Enclosure 2 to Directive 5210.50 lists factors for determining whether to initiate an additional investigation by military, criminal, or counterintelligence investigative organizations, or the Department of Justice:

[50] Available at http://www.dtic.mil/whs/directives/corres/pdf/521050p.pdf.

The accuracy of the information disclosed.

The damage to national security caused by the disclosure and whether there were compromises regarding sensitive aspects of current classified projects, intelligence sources, or intelligence methods.

The extent to which the disclosed information was circulated and the number of persons known to have access to it.

The degree to which an investigation shall increase the damage caused by the disclosure.

The existence of any investigative leads.

The reasonable expectation of repeated disclosures.

The extent to which the classified information was circulated outside the Department of Defense.

If classified DoD information appears in a newspaper or other media, the head of the appropriate DoD component is responsible for the preparation of a "DOJ Media Leak Questionnaire" to submit to the Deputy Secretary of Defense for Intelligence, who prepares a letter for the Chief, Internal Security Section of the Criminal Division at the Department of Justice. The following eleven questions[51] are to be promptly and fully addressed:

- Date and identity of the article containing classified information.
- Specific statements that are classified, and whether the information is properly classified.
- Whether disclosed information is accurate.
- Whether the information came from a specific document, and if so, the originating office and person responsible for its security.
- Extent of official circulation of the information.
- Whether information has been the subject of prior official release.
- Whether pre-publication clearance was sought.
- Whether sufficient information or background data has been published officially or in the press to make educated speculation on the matter possible.
- Whether information is to be made available for use in a criminal prosecution.
- Whether information has been considered for declassification.
- The effect the disclosure of the classified data might have on the national defense.

[51] The questions are listed in enclosure 4 of DoDD 5210.50, and apparently are part of a Memorandum of Understanding concluded between the Department of Justice and elements of the Intelligence Community. *See* U.S. Congress, Senate Select Committee on Intelligence, *Concerning Unauthorized Disclosure of Classified Information*, 106th Cong., 2nd sess., June 14, 2000 (Statement of Attorney General Janet Reno).

Penalties for Unauthorized Disclosure

In addition to administrative penalties agencies may employ to enforce information security, there are several statutory provisions that address the protection of classified information as such. No blanket prohibition exists to make it unlawful simply to disclose without authority any information that is classified by the government for national security reasons.[52]

Criminal Penalties

Generally, federal law prescribes a prison sentence of no more than a year and/or a $1,000 fine for officers and employees of the federal government who knowingly remove classified material without the authority to do so and with the intention of keeping that material at an unauthorized location.[53] Stiffer penalties—fines of up to $10,000 and imprisonment for up to 10 years—attach when a federal employee transmits classified information to anyone that the employee has reason to believe is an agent of a foreign government.[54] A fine and a 10-year prison term also await anyone, government employee or not, who publishes, makes available to an unauthorized person, or otherwise uses to the United States' detriment classified information regarding the codes, cryptography, and communications intelligence utilized by the United States or a foreign government.[55] Finally, the disclosure of classified information that discloses any information identifying a covert agent, when done intentionally by a person with authorized access to such identifying information, is punishable by imprisonment for up to 15 years.[56] A similar disclosure by one who learns the identity of a covert agent as a result of having authorized access to classified information is punishable by not more than ten years' imprisonment. Under the same provision, a person who undertakes a "pattern of activities intended to identify and expose covert agents" with reason to believe such activities would impair U.S. foreign intelligence activities, and who then discloses the identities uncovered as a result is subject to three years' imprisonment, whether or not violator has access to classified information.[57]

Civil Penalties and Other Measures

In addition to the criminal penalties outlined above, the executive branch employs numerous means of deterring unauthorized disclosures by government personnel using administrative measures based on terms of employment contracts. The agency may impose disciplinary action or revoke a person's security clearance. The revocation of a security clearance is usually not reviewable by the Merit System Protection Board[58] and may mean the loss of government

[52] For a broader overview of statutory provisions applicable to specific types of sensitive information, see CRS Report R41404, *Criminal Prohibitions on the Publication of Classified Defense Information*, by Jennifer K. Elsea.

[53] 18 U.S.C. §1924.

[54] 50 U.S.C. §783.

[55] 18 U.S.C. §798.

[56] 50 U.S.C. §421.

[57] "Classified information" for the purpose of this provision is defined as "information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security." 50 U.S.C. §426.

[58] *See* Department of Navy v. Egan, 484 U.S. 518, 526-29 (1988). Federal courts may review constitutional challenges based on the revocation of security clearance. Webster v. Doe, 486 U.S. 592 (1988).

employment. Government employees may be subject to monetary penalties for disclosing classified information.[59] Violators of the Espionage Act and the Atomic Energy Act provisions may be subject to loss of their retirement pay.[60]

Agencies also rely on contractual agreements with employees, who typically must sign non-disclosure agreements prior to obtaining access to classified information,[61] sometimes agreeing to submit all materials that the employee desires to publish to a review by the agency. The Supreme Court enforced such a contract against a former employee of the Central Intelligence Agency (CIA), upholding the government's imposition of a constructive trust on the profits of a book the employee sought to publish without first submitting it to CIA for review.[62]

In 1986, the Espionage Act was amended to provide for the forfeiture of any property derived from or used in the commission of an offense.[63] Violators of the Atomic Energy Act may be subjected to a civil penalty of up to $100,000 for each violation of Energy Department regulations regarding dissemination of unclassified information about nuclear facilities.[64]

Under some circumstances, the government can also use injunctions to prevent disclosures of information. The courts have generally upheld injunctions against former employees' publishing information they learned through access to classified information.[65] The Supreme Court also upheld the State Department's revocation of passports for overseas travel by persons planning to expose U.S. covert intelligence agents, despite the fact that the purpose was to disrupt U.S. intelligence activities rather than to assist a foreign government.[66]

Declassification vs. Leaks and "Instant Declassification"

As noted above, E.O. 13526 sets the official procedures for the declassification of information. Once information is declassified, it may be released to persons without a security clearance.[67] Leaks, by contrast, might be defined as the release of classified information to persons without a security clearance, typically journalists. Recent high-profile leaks of information regarding

[59] *See* 42 U.S.C. §2282(b) (providing for fine of up to $100,000 for violation of Department of Energy security regulations).

[60] 5 U.C.S. §8312 (2001)(listing violations of 18 U.S.C. §§793 & 798, 42 U.S.C. §2272-76, and 50 U.S.C. §421, among those for which forfeiture of retirement pay or annuities may be imposed).

[61] *See* United States v. Marchetti, 466 F.2d 1309 (4th Cir.), *cert. denied,* 409 U.S. 1063 (1972) (enforcing contractual non-disclosure agreement by former employee regarding "secret information touching upon the national defense and the conduct of foreign affairs" obtained through employment with CIA).

[62] *See* Snepp v. United States, 444 U.S. 507 (1980); s*ee also* Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech,* 83 CORNELL L. REV. 261, 274 (1998)(noting the remedy in *Snepp* was enforced despite the agency's stipulation that the book did not contain any classified information).

[63] *See* 18 U.S.C. §§793(h), 794(d), 798(d).

[64] 42 U.S.C. §2168(b).

[65] *See* United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972) (granting an injunction to prevent a former CIA agent from publishing a book disclosing government secrets).

[66] *See* Haig v. Agee, 453 U.S. 280 (1981).

[67] Declassification is an information management step that is distinct and precedes release. Thus, it is not unusual for information to be declassified and then a lengthy period ensues before it is publicly released.

sensitive covert operations in news stories that seemed to some to portray the Obama Administration in a favorable light[68] raised questions regarding the practice of "instant declassification," or whether disclosure of classified information to journalists may ever be said to be an "authorized disclosure" by a senior official.

The processes for declassification set forth in E.O. 13526 seem to presuppose that agencies and classifying officials will not have any need or desire to disclose classified information in their possession other than to comply with the regulations. Yet it has long been noted that there seems to be an informal process for "instant declassification" of information whose release to the public serves an immediate need. As Representative William Moorhead, at the time chairman of the Foreign Operations and Government Information Subcommittee of the House Government Operations Committee, stated in 1974:

> Critics of the present system of handling classified information within the Executive Branch point to an obvious double standard. On one hand, the full power of the Government's legal system is exercised against certain newspapers for publishing portions of the Pentagon Papers and against someone like Daniel Ellsberg for his alleged role in their being made public. This is contrasted with other actions by top Executive officials who utilize the technique of "instant declassification" of information they want leaked. Sometimes it is an "off-the-record" press briefing or "backgrounders" that becomes "on-the-record" at the conclusion of the briefing or at some future politically strategic time. Such Executive Branch leaks may be planted with friendly news columnists. Or, the President himself may exercise his prerogative as Commander in Chief to declassify specific information in an address to the Nation or in a message to the Congress seeking additional funds for a weapons systems.[69]

Nothing in the Executive Order addresses an informal procedure for releasing classified information. E.O. 13526 section 1.1. provides that "[c]lassified information shall not be declassified automatically as a result of any *unauthorized* disclosure of identical or similar information," but does not address what happens in the event of a disclosure that was in fact authorized. By definition, classified information is designated as such based on whether its *unauthorized* disclosure can reasonably be expected to cause a certain level of damage to national security.[70] This may be read to suggest that disclosures may be authorized under such circumstances when no damage to national security is reasonably expected. Nothing in the order provides explicit authority to release classified information that exists apart from the authority to declassify, but it is possible that such discretionary authority is recognized to release information outside the community of authorized holders without formally declassifying it.

Part 4 of the Executive Order describes safeguarding of classified information from unauthorized disclosure[71] and preventing access to such information by "unauthorized persons." Most of the

---

[68] *See National Security Leaks and the Law, Hearing before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary* 1-2, 112th Cong. (2012) (statement of Rep. Sensenbrenner).

[69] William S. Moorhead, *Operation and Reform of the Classification System in the United States* 90, in SECRECY AND FOREIGN POLICY (Thomas M. Franck and Edward Weisband, eds. 1974). For an account of notable government leaks at the time, see *id*. at at 89; *Information Security: Classification of Government Documents*, 85 HARV. L. REV. 1189, 1206-07 (1972). For a more recent chronology of government leaks, see Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233, 251-53 (2008) (quoting various high-level officials who admitted to leaking information in order to generate public support for a program or to promote some other political or bureaucratic agenda).

[70] E.O. 13,526 §1.2.

[71] "Unauthorized disclosure" means "a communication or physical transfer of classified information to an unauthorized recipient." *Id*. §6.1(rr). "Unauthorized" recipient is not defined.

provisions appear to envision classified documents or communications and storage devices used for classified information rather than the spoken word. Section 4.1(g) requires agency heads and the Director of National Intelligence to "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." If "transmitted" is read to include oral dissemination and "unauthorized persons" is read to mean persons who do not meet the criteria set forth in section 4.1(a),[72] then it would seem that agency heads who approve leaks could be in breach of their responsibilities under the Order.

Moreover, there is a provision for "emergency disclosure" of classified information "when necessary to respond to an imminent threat to life or in defense of the homeland" to "an individual or individuals who are otherwise not eligible for access." Section 4.2(b) provides that such disclosures must be in accordance with implementing regulations or procedures the classifying agency implements; must be undertaken in such a way as to minimize the information disclosed and the number of individuals who receive it; and must be reported promptly to the originator. Information disclosed under this provision is not deemed to be declassified. The existence of this provision could be read to cut against an interpretation that permits selected release of classified information to reporters for broader dissemination, but it could also be read not to preclude a different procedure by which an agency head who is the original classifying authority for the information at issue might simply authorize remarks to the press that reference classified information in such a way as to minimize harm to national security

As a practical matter, however, there is little to stop agency heads and other high-ranking officials from releasing classified information to persons without a security clearance when it is seen as suiting government needs. The Attorney General has prosecutorial discretion to choose which leaks to prosecute. If in fact a case can be made that a senior official has made or authorized the disclosure of classified information, successful prosecution under current laws may be impossible because the scienter requirement (i.e., guilty state of mind) is not likely to be met. The Espionage Act of 1917, for example, requires proof that the discloser has the intent or reason to believe the information will be used against the United States or to the benefit of a foreign nation.[73] In cases under the Espionage Act, courts tend to show deference to the government with respect to the sensitivity of whatever classified information was released. Oftentimes in such cases, knowledge that the information is classified is enough to persuade a court that damage to national security can be expected. However, in the event the disclosure was made or authorized by a person who has the authority to make such determinations, it would seem likely that court deference would result in acquittal absent some overwhelming proof of ill intent. A belief on the part of a lower level official that a particular disclosure was authorized could serve as an effective defense to any prosecution, and could entitle the defendant to depose high level government officials in preparation for his or her defense.

Executive Branch policy appears to treat an official disclosure as a declassifying event, while non-attributed disclosures have no effect on the classification status of the information. For example, the Department of Defense instructs agency officials, in the event that classified

[72] A person who does meet the criteria in section 4.1.(a) is defined as an "authorized holder" under the definitions section of the Order, section 6.1(c).

[73] 18 U.S.C. §793. For more information about criminal laws proscribing leaks, see CRS Report R41404, *Criminal Prohibitions on the Publication of Classified Defense Information*, by Jennifer K. Elsea. The level of knowledge required to prove an offense depends on the type of information alleged to have been disclosed, and it is not necessarily a crime to disclose information merely because it is classified. *See id*.

information appears in the media, to neither confirm nor deny the accuracy of the information.[74] The Under Secretary of Defense for Intelligence is then advised to "consult with the Assistant Secretary of Defense for Public Affairs and other officials having a primary interest in the information to determine if the information was officially released under proper authority."[75] The regulation does not clarify what happens in the event the disclosure turns out to have been properly authorized. It appears no further action need be taken, whether to inform employees that the information no longer need be protected or to make annotations in classified records to reflect the newly declassified status of the information. In any event, any documents that contain that information potentially contain other classified information as well, in which case each such document would retain the highest level of classification applicable to information in the document. Thus, it seems unlikely that the authorized disclosure of classified information to the media will often result in the public release of any records.

Recent Developments

The following sections address efforts undertaken by the Executive Branch and Congress to address disclosures of classified information by federal employees.

Executive Branch Initiatives

In October 2011 the President issued Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."[76] Among other measures, it establishes an interagency Insider Threat Task Force with a mandate to:

> 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.[77]

The President issued the resulting new policy and minimum standards for agencies in implementing their own insider threat programs in November 2012.[78]

The Director of National Intelligence issued a revised directive in June 2012 to govern the protection of national intelligence by the intelligence community.[79] It emphasizes the integration

[74] Department of Defense, *Department of Defense Manual*, 5200.01-V3, February 24, 2012 encl. 6 at 93.

[75] *Id*. at 94.

[76] Exec. Order No. 13587, 3 C.F.R. 276 (2011), *available at* http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-.

[77] *Id*. §6.

[78] Press Release, White House Office of the Press Secretary, Presidential Memorandum—National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand. The policy and standards do not appear to have been made public.

of security and counterintelligence functions for, among other purposes, strengthening deterrence, detection and mitigation of "insider threats," which it defined as "personnel who use their authorized access to do harm to the security of the US through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of resources or capabilities." It also establishes an inspection process to ensure that departments and agencies that handle national intelligence maintain effective operational security practices. Also in June 2012, the Office of the Director of National Intelligence announced two new measures aimed to protect classified information from unauthorized disclosure, The Director mandated the inclusion of a new question related to unauthorized disclosures to counterintelligence polygraph examinations and requested the Intelligence Community Inspector General to lead independent investigations of selected unauthorized disclosure cases where the Justice Department has declined to prosecute.[80]

The Department of Defense issued a revised version of the DoD Information Security Program manual, which among other things mandates a department-wide incident reporting system to track unauthorized disclosures. It also tasks the Undersecretary of Defense for Intelligence, in consultation with the Assistant Secretary for Public Affairs, with monitoring all "major, national level media reporting" for unauthorized disclosures of DoD classified information[81] as a part of a new "top down reporting system to detect unauthorized disclosures." The Department also put into effect an automated security incident reporting system and an improved system for monitoring DoD networks, and initiated a DoD Insider Threat Program as well as an Unauthorized Disclosure Working Group.[82]

Congressional Activity

The 112th Congress held at least two hearings on the topic of unauthorized disclosures of classified information.[83] Congress also passed a measure as part of the National Defense Authorization Act for FY2012 to require the Defense Department to establish a "program for information sharing protection and insider threat mitigation for the information systems of the Department of Defense to detect unauthorized access to, use of, or transmission of classified or controlled unclassified information."[84] Its purpose appears to be avoidance of a reiteration of the *Wikileaks* disclosures, and the program is required to make use of both technology based solutions as well as a "governance structure and process" to integrate these technologies into existing security measures.

(...continued)

[79] Intelligence Community Directive (ICD) 700, Protection of National Intelligence, effective June 7, 2012, *available at* http://www.dni.gov/files/documents/ICD/ICD_700.pdf.

[80] Press Release, Office of the Director of National Intelligence, Director Clapper Announces Steps to Deter and Detect Unauthorized Disclosures (June 25, 2012), *available at* http://www.dni.gov/index.php/newsroom/press-releases/96-press-releases-2012/586-director-clapper-announces-steps-to-deter-and-detect-unauthorized-disclosures.

[81] Press Release, Department of Defense Office of the Assistant Secretary (Public Affairs), Statement from George Little on Defense Initiatives to Limit Unauthorized Disclosures of Classified Information (July 19, 2012), *available at* http://www.defense.gov/Releases/Release.aspx?ReleaseID=15451. The four-volume manual for the DoD Information Security Program is available at http://www.dtic.mil/whs/directives/corres/pub1.html.

[82] *Id*.

[83] *National Security Leaks and the Law, Hearing before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. (2012); *Disclosures of National Security Information and Impact on Military Operations*, *Hearing before the H. Comm. on Armed Services*, 112th Cong (2012).

[84] P.L. 112-81, §922, codified at 10 U.S.C. §2224 note.

The Intelligence Authorization Act for FY2013, S. 3454, 112th Congress, as reported by the Senate Intelligence Committee, contained a number of measures to address the disclosure of classified information by federal employees, whether authorized or not, especially if the disclosure were to the media. Opposition to these measures resulted in a manager's amendment to the bill with all but one of these provisions removed.[85] Section 504 of the bill, as passed by both houses of Congress, requires a government official who approves a disclosure of classified information to the media, or to another person for publication, to first report the decision and other matters related to the disclosure to the congressional intelligence committees. The provision applies to "national intelligence or intelligence related to national security" that is classified or has been declassified for the purpose of making the disclosure, where the disclosure is made by a government officer, employee, or contractor. According to the original committee report, the reporting is intended to keep the intelligence committees apprised of expected media disclosures of relevant classified information and to assist in distinguishing between "authorized disclosures" and "unauthorized leaks."[86] As amended, the requirement sunsets one year after enactment.

Provisions that were dropped from the bill include a requirement for heads of agencies and departments of the intelligence community to maintain a list of all "authorized disclosures" to media personnel; a requirement to establish procedures for administrative investigations of unauthorized disclosures and to report the procedures and any investigations to the intelligence committees; a requirement for an assessment of measures to improve detection capabilities, including the practical feasibility of including questions regarding disclosure of classified information and contact with the media in polygraph examinations; and measures related to agency "insider threat" programs and employee non-disclosure agreements. Another provision would have required the Attorney General to submit a report to the congressional intelligence committees describing the effectiveness of and potential improvements to the process for investigating and prosecuting unauthorized disclosures of classified information; potential modifications to the policy on subpoenaing reporters; and suggested modifications to the Classified Information Procedures Act.[87]

Some of the more controversial measures that were eliminated from the bill involved restrictions on media access to government officials. One was a prohibition on federal officers, employees, and contractors who have security clearances, including some who have left government service within the prior year, from entering into agreements with the media to provide analysis or commentary on matters related to classified intelligence activities or intelligence related to national security. Another would have limited the individuals authorized to provide background or off-the-record information to the media regarding intelligence activities to the Director and Deputy Directors or their equivalents of each agency and designated public affairs officers. Another would have required the Director of National Intelligence to prescribe regulations regarding the interaction of cleared personnel with the media. Such persons would have been required to report all contacts with the media to the appropriate security office. Also eliminated was a prohibition on federal officers, employees, and contractors from possessing a security clearance after having made any unauthorized disclosure regarding the existence of, or classified details relating to, a covert action as defined in 50 U.S.C. Section 413(b).

---

[85] *See* Greg Miller, *Senate Committee Drops Anti-Leaks Measures*, WASH. POST, Dec. 22, 2012, at A3.

[86] S.Rept. 112-192.

[87] For information about the Classified Information Procedures Act, see CRS Report R41742, *Protecting Classified Information and the Rights of Criminal Defendants: The Classified Information Procedures Act*, by Edward C. Liu and Todd Garvey.

Author Contact Information

Jennifer K. Elsea
Legislative Attorney
jelsea@crs.loc.gov, 7-5466