The Protection of Classified Information: The Legal Framework

Jennifer K. Elsea
Legislative Attorney

May 18, 2017

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

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

This report provides an overview of the relationship between executive and legislative authority over national security information. It 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

Contacts

Background

Prior to the New Deal, decisions regarding classification of national security information 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,[3] later Presidents have cited general statutory and constitutional authority.[4]

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,[5] 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."[6] This language has been interpreted by some to indicate that the President has virtually plenary authority to control classified information.[7] On the other hand, the Supreme

[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] *See id.* (citing the act of January 12, 1938, 52 Stat. 3, §1).

[4] *See, e.g.*, Exec. Order No. 10501 (1953); Exec. Order No. 13292 (2003). President Obama's executive order on classified information, Exec. Order No. 13526 (Dec. 29, 2009), also cites constitutional authority. The Trump Administration has not issued a new executive order pertaining to classified information.

[5] U.S. CONST., art. II, §2.

[6] 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).

[7] President George W. Bush objected to some provisions of the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458 (2004), that he viewed as impeding on presidential prerogatives:

> Several provisions of the Act, including Title III and section 7601, purport to regulate access to classified national security information. The Supreme Court of the United States has stated that the President's authority to classify and control access to information bearing on national security flows from the Constitution and does not depend upon a legislative grant of authority. The executive branch shall construe such provisions in a manner consistent with the Constitution's commitment to the President of the executive power, the power to conduct the Nation's foreign affairs, and the authority as Commander in Chief.

Statement on Signing the Intelligence Reform and Terrorism Prevention Act of 2004, 2004 PUB. PAPERS 3118, 3119 (Dec. 17, 2004). President Bush used similar language to object to other provisions regarding congressional notification. *See, e.g.*, 2002 PUB. PAPERS 46, 47-48 (Jan. 10, 2002); *id.*at 1870 (Oct. 23, 2002); 2003 PUB. PAPERS 1217 (Sep. 30, 2003); *id.* at 1603 (Nov. 22, 2003); 2004 PUB. PAPERS 1494 (Aug. 5, 2004); 2005 PUB. PAPERS 1794 (Nov. 30, 2005; *id.* at 1901 (Dec. 5, 2005); 2006 PUB. PAPERS 1152, 1153 (June 15, 2006); *id.* at 1733 (Sep. 29, 2006). President Trump used nearly identical language to object to a provision in the Consolidated Appropriations Act of 2017, P.L. 115-31 (2017), that requires 30 days' advance congressional notification prior to establishing a new special access program (§8009). In his signing statement, President Trump wrote:

> The President's authority to classify and control access to information bearing on the national security flows from the Constitution and does not depend upon a legislative grant of authority. Although I expect to be able to provide the advance notice contemplated by section 8009 in most

(continued...)

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."[8] In fact, Congress established a separate regime in the Atomic Energy Act for the protection of nuclear-related "Restricted Data."[9]

Congress has directed the President to establish procedures governing the access to classified material so that generally no person can gain such access without having undergone a background check.[10] 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.[11] These standards include the establishment of uniform procedures for, *inter alia*, background checks, denial of access to classified information, and notice of such denial.[12] There is an exception to the due process requirements, however, where compliance could damage national security, although the statute directs agency heads to submit a report to the congressional intelligence committees in such a case.[13]

With the authority to determine classification standards vested in the President, these standards tend to change when a new administration takes control of the White House.[14] 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

(...continued)

> situations as a matter of comity, situations may arise in which I must act promptly while protecting certain extraordinarily sensitive national security information. In these situations, I will treat these sections in a manner consistent with my constitutional authorities, including as Commander in Chief.

Statement by President Donald J. Trump on Signing H.R. 244 into Law (May 5, 2017), https://www.whitehouse.gov/the-press-office/2017/05/05/statement-president-donald-j-trump-signing-hr-244-law; *see also* Steven Aftergood, *Trump Objects to Legislated Limits on Secrecy*, FED'N AM. SCIENTISTS: SECRECY NEWS (May 8, 2017), https://fas.org/blogs/secrecy/2017/05/trump-saps/ (noting similarity between Supreme Court *Egan* quote and President's claim).

[8] Environmental Protection Agency v. Mink, 410 U.S. 73, 83 (1973).

[9] 42 U.S.C. §§2162-69 (2017). In addition, the Invention Secrecy Act, 35 U.S.C. §181-88 (2017), 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 R41404, *Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information*, by Stephen P. Mulligan and Jennifer K. Elsea; "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information.

[10] Counterintelligence and Security Enhancement Act of 1994, Title VIII of P.L. 103-359 (codified at 50 U.S.C. §§3161-64 (2017)). Congress has also required specific regulations regarding personnel security procedures for employees of the National Security Agency, P.L. 88-290, 78 Stat. 168 (1964)(codified at 50 U.S.C. §§831 – 835 (2017)).

[11] 50 U.S.C. §3161(a) (2017).

[12] *Id.*

[13] *Id.* §3161(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.Rept. 103-753, at 54.

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

> 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.[15]

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.[16] In 1966, Congress passed the Freedom of Information Act (FOIA),[17] 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.[18] In 2000, Congress enacted the Public Interest Declassification Act of 2000,[19] which established the Public Interest Declassification Board to advise the President on matters regarding the declassification of certain information. However, 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 may be enforced in court.[20] Most recently, Congress passed the Reducing Over-Classification Act, P.L. 111-258 (2010), which, among other things, requires executive branch agencies' inspectors general to conduct assessments of their agencies' implementation of classification policies.[21]

Congress occasionally takes an interest in declassification of specific materials that might be deemed essential for some public purpose. The procedural rules of both the Senate and House provide a means for disclosing classified information in the intelligence committees' possession where the intelligence committee of the respective house (either the House Permanent Select Committee on Intelligence (HPSCI) or the Senate Select Committee on Intelligence (SSCI)) determines by vote that such disclosure would serve the public interest.[22] In the event the intelligence committee votes to disclose classified information that was submitted by the executive branch, and the executive branch requests it be kept secret, the committee is required to notify the President. The information may be disclosed after five days unless the President formally objects and certifies that the threat to the U.S. national interest outweighs any public interest in disclosing it, in which case the question may be referred to the full chamber.[23]

It does not appear that either house has invoked its procedure for disclosing classified information. In fact, in at least one instance, Congress deferred to the executive branch even with respect to materials prepared by Congress,[24] albeit perhaps using documents obtained from the

---

[15] *Id.*

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

[17] P.L. 89-554, 80 Stat. 383 (1966) (codified as amended at 5 U.S.C. §552 (2017)).

[18] 5 U.S.C. §552(b)(1) (2017). 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) (2017).

[19] P.L. 106-567, title VII, 114 Stat. 2856 (2000) (codified as amended at 50 U.S.C. §3161 note (2017).

[20] *Id.* §§705 and 707.

[21] P.L. 111-258, §6, 124 Stat. 2651 (2010) (codified at 50 U.S.C. §3161 note (2017)).

[22] Rules of the House of Representatives, 114th Congress, Rule X, 11(g)(1); S.Res. 400, 94th Congress, Sec. 8(a).

[23] Rules of the House of Representatives, 114th Congress, Rule X, 11(g)(2); S.Res. 400, 94th Congress, Sec. 8(b). The House and Senate Rules regarding the vote to disclose classified information are substantially similar, although the Senate Manual additionally requires notification to the Majority and Minority Leaders.

[24] *See, e.g.*, S.Rept. 114-8 at 12 (describing negotiations between the Chairman of the SSCI and the Obama (continued...)

executive branch. A recent example involved the 28 pages of classified text from the report of the Joint Inquiry of the HPSCI and the SSCI into the Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.[25] The report of the Joint Inquiry was completed in 2002 and referred to the executive branch for a classification review, which determined that three of the four parts of the report could be disclosed to the public, but that the disclosure of a portion of the report would pose national security risks.[26] Despite calls for the release of the 28 pages by some Members and former Members,[27] and legislative proposals to mandate disclosure,[28] the intelligence committees awaited a declassification review by the intelligence community before releasing the material in redacted form.

One notable instance in which Congress sought and procured the declassification of government information involved records pertaining to prisoners of war and personnel listed as missing in action after the Vietnam War ("POW/MIA").[29] Congress initially required certain agencies to provide information regarding "live-sightings" of such personnel to next of kin, with the exception of "information that would reveal or compromise sources and methods of intelligence collection."[30] Congress subsequently directed the Department of Defense (DOD) to create an accessible library of documents related to POW/MIA, excluding records that would be exempt under certain provisions of FOIA.[31] The Senate Select Committee on POW/MIA Affairs considered invoking the procedural rule described above to declassify relevant documents, but deemed that untested avenue unsuitable because it would have required the Committee to identify the documents beforehand and to have had them in its possession. Furthermore, enforcement of the measure would have required the full vote of the Senate.[32] Instead, Members wrote to President George H. W. Bush requesting an executive order to accomplish the declassification of relevant records.[33] It was followed by a resolution expressing the sense of the Senate that the President should expeditiously issue an executive order for the declassification, without compromising national security, of relevant documents.[34] President Bush complied.[35]

(...continued)

Administration regarding redactions necessary to release an unclassified version of the Committee's executive summary to its report on the Central Intelligence Agency's detention and interrogation of detainees).

[25] H.Rept. 107-792. For a discussion of the contents and release of the 28 pages, see CRS In Focus IF10438, *Finding #20 and the Case of the "28 Pages"*.

[26] *See* Director of National Intelligence, Statement by the ODNI on the Declassification of Part Four of the SSCI and HPSCI's 2002 Report on the Committees' Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 (July 15, 2016), https://www.dni.gov/index.php/newsroom/reports-and-publications/214-reports-publications-2016/1397-statement-by-the-office-of-the-director-of-national-intelligence-on-the-declassification-of-part-four-of-the-senate-select-committee-on-intelligence-and-house-permanent-select-committee-on-intelligence%E2%80%99s-2002-report-on-the-committees%E2%80%99-joint-inquiry-into-i.

[27] *See* IF10438, *supra* footnote 25.

[28] *E.g.*, S. 1471 (114th Cong.); H.Res. 779 (114th Cong.); H.Res. 14 (114th Cong.).

[29] *See* Report of the Select Committee on POW/MIA Affairs, S.Rept. 103-1, at 233-44, available at http://lcweb2.loc.gov/frd/pow/senate_house/pdf/report_S.pdf.

[30] P.L. 100-453 §404, 102 Stat. 1908 (1988) (codified at 50 U.S.C. §3161 note (2017)).

[31] P.L. 102-90, div. A, §1082, 105 Stat. 1480 (1991) (codified at 50 U.S.C. §3161 note (2017)). The POW/MIA database was created at the Library of Congress and may be accessed at http://lcweb2.loc.gov/frd/pow/powhome.html.

[32] S.Rept. 103-1 at 237.

[33] *Id.* at 237-38.

[34] S.Res. 324 (102d Cong.).

[35] Exec. Order No. 12812, 57 Fed. Reg. 32879 (July 22, 1992).

More recently, Congress has directed the President or agency heads to undertake a declassification review of records pertaining to specific matters and to release them as appropriate. For example, Congress in 2000 directed the President to "order all Federal agencies and departments that possess relevant information [about the murders of churchwomen in El Salvador] to make every effort to declassify and release" them to victims' families.[36] In 2002, Congress directed the Secretary of Defense to submit to Congress and to the Secretary of Veterans Affairs "a comprehensive plan for the review, declassification, and submittal" of all information related to Project 112—a series of biological and chemical warfare vulnerability tests conducted by the Department of Defense[37]—that would be relevant for that project's participants' health care.[38] In 2004, Congress directed the Secretary of Defense to "review and, as determined appropriate, revise the classification policies of the Department of Defense with a view to facilitating the declassification of data that is potentially useful for the monitoring and assessment of the health of members of the Armed Forces who have been exposed to environmental hazards during deployments overseas."[39] In 2007, Congress directed the Director of the Central Intelligence Agency (CIA) to make public a version of the executive summary of the CIA Office of the Inspector General report on "CIA Accountability Regarding Findings and Conclusions of the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001," declassified "to the maximum extent possible, consistent with national security."[40] And in 2014, Congress directed the Director of National Intelligence (DNI) to conduct a declassification review of documents collected during the raid that killed Osama bin Laden, requiring a justification for materials that remain classified after the review.[41]

Executive Order 13526

The current standards for classifying and declassifying information were last amended on December 29, 2009, in Executive Order 13526.[42] 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.[43] 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;

[36] P.L. 106-429, §587, 114 Stat. 1900A–58 (2000).

[37] *See* U.S. Department of Veterans Affairs, Public Health, About Project 112 and Project SHAD, available at https://www.publichealth.va.gov/exposures/shad/basics.asp.

[38] P.L. 107-314, div. A, §709, 116 Stat. 2586 (2002) (codified at 10 U.S.C. §1074 note (2017)). For information about Project 112 and related veterans' health benefits, visit the Department of Veterans Affairs website at http://www.benefits.va.gov/COMPENSATION/claims-postservice-exposures-project_112_shad.asp.

[39] P.L. 108-375, div. A, §735, 118 Stat. 1999 (2004) (codified at 10 U.S.C. §1074 note (2017)).

[40] P.L. 110-53 §605, 121 Stat. 337 (2007).

[41] P.L. 113-126, §313, 128 Stat. 1399 (2014).

[42] 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*.

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

- 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.[44]

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.[45] 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.[46] In case of significant doubt as to the need to classify information or the level of classification appropriate, the information is to remain unclassified or be classified at the lowest level of protection considered appropriate.[47]

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.[48] The deadline for declassification can be extended if the threat to national security still exists.[49]

Classified information is required to be declassified "as soon as it no longer meets the standards for classification."[50] The original classifying agency has the authority to declassify information when the public interest in disclosure outweighs the need to protect that information.[51] 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.[52]

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)[53]

---

[44] *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.

[45] *Id.* §1.2.

[46] *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).

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

[48] 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.*

[49] *Id.* §1.5(c).

[50] *Id.* §3.1(a).

[51] *Id.* §3.1(d).

[52] *Id.* §3.3.

[53] 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.

or are the subject of pending litigation.[54] 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;[55] 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.[56] Each agency that has classified information is required to establish a system for periodic declassification reviews.[57] The National Archivist is required to establish a similar systemic review of classified information that has been transferred to the National Archives.[58]

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.[59] 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.[60] 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.[61]

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.[62] 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.[63] In addition, there is an Interagency Security Classifications Appeals Panel (ISCAP), 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.[64] ISCAP is empowered to decide appeals of classifications challenges[65] 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.

[54] Exec. Order No. 13526 §3.5.

[55] 50 U.S.C. §§3141-43 (2017).

[56] Exec. Order No. 13526 §3.5.

[57] *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).

[58] *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*.

[59] Exec. Order No. 13526 §4.1.

[60] *Id.* §4.4.

[61] *Id.* §4.2.

[62] *Id.* §5.2.

[63] *Id.* §3.1(c).

[64] *Id.* §5.3.

[65] *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.

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.[66]

Executive Order 12333, United States Intelligence Activities,[67] spells out the responsibilities of members of the Intelligence Community[68] 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 C.F.R. Part 2001) provides further direction for agencies with responsibilities for safeguarding classified information. Section 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

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

[67] 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.

[68] The Intelligence Community is defined by 50 U.S.C. ' 3003(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."

> 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.[69]

Section 2001.45 of ISOO Directive No. 1[70] requires agency heads to establish a system of appropriate control measures to limit access to classified information to authorized persons. Section 2001.46 requires that classified information is transmitted and received in an authorized manner that facilitates detection of tampering and precludes inadvertent access.[71] 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.[72] 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.[73] 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.[74] Agency heads 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).[75]

Section 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."[76]

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."[77] 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.[78] 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.[79] 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

[69] 32 C.F.R. §2001.41 (2016).

[70] 32 C.F.R. §2001.45 (2016).

[71] 32 C.F.R. §2001.46(a) (2016).

[72] *Id.*

[73] 32 C.F.R. §2001.46(b)(1) (2016).

[74] 32 C.F.R. §2001.46(c) (2016).

[75] 32 C.F.R. §2001.46(f) (2016).

[76] 32 C.F.R. §2001.48(a) (2016).

[77] 32 C.F.R. §2001.48(c) (2016).

[78] 32 C.F.R. §2001.48(b) (2016).

[79] 32 C.F.R. §2001.48(e) (2016).

the individual believed to be responsible is assigned or employed.[80] ISOO must be notified in case of a violation that (1) is reported to congressional oversight committees; (2) may attract significant public attention; (3) involves large amounts of classified information; or (4) reveals a potential systemic weakness in security practices.[81]

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;[82] ICD 701, Security Policy Directive for Unauthorized Disclosures of Classified Information, effective March 14, 2007;[83] and ICD 703, Protection of Classified National Intelligence, Including Sensitive Compartmented Information, effective June 21, 2013.[84] Damage assessments in the event of an unauthorized disclosure or compromise of classified national intelligence are governed by ICD 732, effective June 27, 2014.[85]

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."[86] Under ICD 701, Senior Officials of the Intelligence Community (SOICs)[87] 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;
>
> 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;

[80] *Id.*

[81] 32 C.F.R. §2001.48(d) (2016).

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

[83] Available at https://www.dni.gov/files/documents/FOIA/DF-2016-00127.pdf.

[84] Available at https://www.dni.gov/files/documents/ICD/ICD%20703.pdf.

[85] Available at https://www.dni.gov/files/documents/ICD/ICD%20732.pdf.

[86] ICD 700 §D.4.c (2012).

[87] 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.

> 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.[88]

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.[89] The SOIC is then required to provide updated reports as appropriate (or as directed).[90] This process occurs in tandem with any required reporting to law enforcement authorities.[91]

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.[92] 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.[93]

Department of Defense

Department of Defense Directive 5210.50, "Management of Serious Security Incidents Involving Classified Information" (October 27, 2014),[94] prescribes policy and responsibilities for handling unauthorized disclosures of classified information to the public and other serious security incidents. More detailed procedures governing specific types of information possibly compromised are found in DOD Manual 5200.01, Volume 3, Enclosure 6, "Security Incidents Involving Classified Information," February 24, 2012.[95] In the event of a known or suspected disclosure of classified information, the heads of DOD components must take prompt action to decide the nature and circumstances of the disclosure, determine the extent of damage to national security, and take appropriate corrective action.[96] If the inquiry or investigation turns up information suggestive of a criminal or counterintelligence nature, component heads are to cease investigation pending coordination with the relevant Deputy Chief Information Officer (DCIO) or Defense Counter-Intelligence (CI) component.[97]

Security inquiries are to be initiated and completed within 10 duty days unless an extension is required.[98] The inquiry is aimed at discovering:

> (a) When, where, and how did the incident occur? What persons, situations, or conditions caused or contributed to the incident?
>
> (b) Was classified information compromised?

[88] ICD 701 §E (2007).

[89] *Id.* §F.

[90] *Id.*

[91] *Id.* §F.2.

[92] *Id.* §F.3.

[93] *Id.* §G.3.

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

[95] Available at http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf.

[96] *Id.* §6(a).

[97] *Id.* §6(b).

[98] *Id.* §6(d)(2).

> (c) If a compromise occurred, what specific classified information and/or material was involved? What is the classification level of the information disclosed?
>
> (d) If classified material is alleged to have been lost, what steps were taken to locate the material?
>
> (e) Was the information properly classified?
>
> (f) Was the information officially released?
>
> (g) In cases of compromise involving the public media:
>
> 1. In what specific media article, program, book, Internet posting or other item did the classified information appear?
>
> 2. To what extent was the compromised information disseminated or circulated?
>
> 3. Would further inquiry increase the damage caused by the compromise?
>
> (h) Are there any leads to be investigated that might lead to identifying the person(s) responsible for the compromise?
>
> (i) If there was no compromise, and if the incident was unintentional or inadvertent, was there a specific failure to comply with established security practices and procedures that could lead to compromise if left uncorrected and/or is there a weakness or vulnerability in established security practices and procedures that could result in a compromise if left uncorrected? What corrective action is required?[99]

Section 7(f) lists factors for determining whether to initiate an additional investigation by a DCIO or the Department of Justice (DOJ) in the event classified information appears in the public media:

> 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, both within and outside the Department of Defense, 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.[100]

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 Under 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[101] are to be promptly and fully addressed:

---

[99] *Id.* §6(d)(4).

[100] *Id.* §7(f).

[101] The questions apparently originated as 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).

- Date and identity of the media source (article, blog, television, or other oral presentation) containing classified information.
- Specific statement(s) 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 or release 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 and the person competent to testify on its classification.
- Whether information has been considered for declassification.
- The effect the disclosure of the classified data might have on the national defense.[102]

Department of State

Information security at the State Department[103] is governed by 12 FAM 500 and 600.[104] The Bureau of Administration is responsible for implementing E.O. 13526 as it applies to the classification and declassification of material, the marking of classified material, and relevant training and guidance.[105] The Bureau of Diplomatic Security (DS) is responsible for protecting classified information and special access programs.[106] Senior agency officials have the primary responsibility for overseeing their respective agency's information security program, while supervisors are charged with safeguarding classified information within their organizational units.[107] Individual employees having access to classified material are responsible for maintaining its security.[108]

Security incidents are to be reported through the appropriate security officer to DS by filling out a standard form.[109] The employee suspected of having caused the incident is given an opportunity

[102] DOD Manual 5200.01, Volume 3, Enclosure 6, Appendix 2, "DOJ Media Leaks Questionnaire," February 24, 2012.

[103] U.S. Department of State Foreign Affairs Manual Volume 12 –Diplomatic Security, Part 500, Information Security and Part 600, Information Security Technology, available at http://fam.state.gov. 12.FAM 500 applies to all national security and sensitive information that is "owned by, originated by, produced by or for, or under the control of Foreign Affairs Agencies" at all State Department-controlled locations. 12 FAM 511.1. Foreign Affairs Agencies include the Department of State, United States Agency for International Development, Overseas Private Investment Corporation, Trade and Development Program, and all other executive branch personnel located under the jurisdiction of a chief of mission. *Id.*

[104] 12 FAM 500 and 600.

[105] *Id.* at 512.1-1.

[106] *Id.*

[107] *Id.* at 512.1.

[108] *Id.* at 512.1-3.

[109] *Id.* at 553.1.

to provide a statement of defense or mitigating circumstances, after which the incident is referred to his or her supervisor and to DS.[110] DS is responsible for evaluating security incidents and performing final adjudication of them and initiation of any further action deemed necessary.[111] Investigations of loss, unauthorized disclosure, or serious compromise of classified information are covered in 12 FAM 228.4 and are the responsibility of the Professional Responsibility Division (DS/ICI/PR) of the Office of Investigations and Counterintelligence.[112] In the event of a "media leak" of classified information, the originating agency is to undertake an initial investigation to determine if any other agency had access to the information, and if necessary request that such receiving agency conduct an appropriate investigation into the unauthorized disclosure.[113] The manual notes that DOJ may decide to prosecute those who disclose classified information without authority, but does not provide a list of reporting criteria.[114]

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, but only certain types of information or in specific situations. There is no blanket prohibition on the unauthorized disclosure of classified information.[115] The Espionage Act itself does not mention classified information, but prohibits transmittal of national defense information with the relevant intent or state of mind.[116]

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.[117] 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.[118] 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.[119] Finally, the disclosure of classified information that reveals any information identifying a covert agent, when done intentionally by a person with authorized access to such

[110] *Id.*

[111] 12 FAM 556.

[112] *Id.* at 228.4-1.

[113] *Id.* at 228.4-4.

[114] *See id.* It is possible that a memorandum of understanding regarding cooperation with DOJ on such matters exists, *see* 12 FAM 221.2.

[115] For a broader overview of statutory provisions applicable to specific types of sensitive information, see CRS Report R41404, *Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information*, by Stephen P. Mulligan and Jennifer K. Elsea.

[116] 18 U.S.C. §793 (2017). For a detailed description of the Espionage Act, see CRS Report R41404.

[117] 18 U.S.C. §1924 (2017).

[118] 50 U.S.C. §783 (2017).

[119] 18 U.S.C. §798 (2017).

identifying information, is punishable by imprisonment for up to 15 years.[120] 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 10 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.[121]

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 Systems Protection Board[122] and may mean the loss of government employment. Government employees may also be subject to monetary penalties for disclosing classified information.[123] Violators of the Espionage Act and the Atomic Energy Act provisions may additionally be subject to loss of their retirement pay.[124]

Agencies also rely on contractual agreements with employees, who typically must sign non-disclosure agreements prior to obtaining access to classified information,[125] 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.[126]

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 that violates the Espionage Act.[127] 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.[128]

---

[120] 50 U.S.C. §3121 (2017).

[121] "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. §3126 (2017).

[122] *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).

[123] *See* 42 U.S.C. §2282(b) (2017) (providing for fine of up to $100,000 for violation of Department of Energy security regulations).

[124] 5 U.S.C. §8312 (2017) (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).

[125] *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).

[126] *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).

[127] *See* 18 U.S.C. §§793(h), 794(d), 798(d) (2017).

[128] 42 U.S.C. §2168(b) (2017).

Under some circumstances, the government can also use injunctions to prevent disclosures of information. In at least one instance, a court upheld an injunction against a former employee's publishing of information learned through access to classified information.[129] 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.[130]

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.[131] Leaks, by contrast, might be defined as the release of classified information to persons without a security clearance, typically journalists. In 2012, some allegedly high-profile leaks of information regarding sensitive covert operations in news stories that seemed to some to portray the Obama Administration in a favorable light[132] 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

[129] *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).

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

[131] 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.

[132] *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) (citing *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NY TIMES, June 1, 2012, at A1; *Secret 'Kill List' Proves a Test of Obama's Principles and Will*, NY TIMES, May 29, 2012, at A1; *Stuxnet Was the Work of U.S. and Israeli Experts, Officials Say*, WASH, POST., June 2, 2012).

> Chief to declassify specific information in an address to the Nation or in a message to the Congress seeking additional funds for a weapons system.[133]

E.O. 13526 does not address an informal procedure for releasing classified information. Section 1.1 of the E.O. 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 classified based on whether its *unauthorized* disclosure can reasonably be expected to cause a certain level of damage to national security.[134] This definition 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 E.O. 13526 describes safeguarding of classified information from unauthorized disclosure[135] and preventing access to such information by "unauthorized persons." Most of the 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 interpreted to include oral dissemination and "unauthorized persons" is interpreted to mean persons who do not meet the criteria set forth in Section 4.1(a),[136] 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. However, it could also be read to allow a different procedure by which an agency head, who is the original classifying

---

[133] 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 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).

[134] E.O. 13526 §1.2.

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

[136] *Id.* §4,1(a). The criteria are (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. A person who meets these criteria is defined as an "authorized holder" under the definitions section of the Order, Section 6.1(c).

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 seemingly 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 could be brought that a senior official has made or authorized the disclosure of classified information, successful prosecution under current laws may be difficult 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.[137] Although the nature and sensitivity of the information that was released are elements for the jury to decide,[138] knowledge that the information is classified may be enough to persuade a court that damage to national security can be expected.[139] However, in the event the disclosure was made or authorized by a person who has the authority to make such determinations—as to whether the information will be used against the United States or to the benefit of a foreign nation—it would seem likely that such deference would potentially result in not meeting the scienter requirement absent some proof of ill intent. For example, 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 information appears in the media, to neither confirm nor deny the accuracy of the information.[140] 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."[141] 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 needs to 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 would often result in the public release of any records.

---

[137] 18 U.S.C. §793 (2017). For more information about criminal laws proscribing leaks, see CRS Report R41404, *Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information*, by Stephen P. Mulligan and 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.*

[138] *See* United States v. Morison, 844 F.2d 1057, 1073 (4th Cir.), *cert. denied*, 488 U.S. (1988) (upholding conviction under 18 U.S.C. §793 for delivery of classified photographs to publisher). Whether the information is "related to the national defense" under this meaning is a question of fact for the jury to decide. *Id.* at 1073.

[139] *See* United States v. Kiriakou, 898 F. Supp. 2d 921, 925 (E.D. Va. 2012) (noting that defendant was a "government employee trained in the classification system who could appreciate the significance of the information he allegedly disclosed"). The court noted that the potentially damaging nature of intangible information due to its disclosure can largely be inferred from the fact that information is classified. *Id.* at 921.

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

[141] *Id*. at 94.

The Intelligence Authorization Act for FY2013, P.L. 112-277 (2013) section 504 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."[142] Originally scheduled to sunset after a year, the provision was made permanent in the Intelligence Authorization Act for 2014.[143] Any reports to Congress of authorized disclosures submitted pursuant to this provision apparently are classified.[144]

Insider Threat Risk Management

In October 2011 President Obama issued Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."[145] Among other measures, it established 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.[146]

President Obama issued the resulting new policy and minimum standards for agencies in implementing their own insider threat programs in November 2012.[147]

Concerned about *WikiLeaks* and other disclosures of classified information by those with access, the 112th Congress held at least two hearings on the topic of unauthorized disclosures of classified information.[148] 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

[142] S.Rept. 112-192 (2012).

[143] P.L. 113-126 §328, 128 Stat. 1405 (2014) (codified at 50 U.S.C. §3349 (2017)).

[144] *See* Steven Aftergood, *Report on Disclosures to the Media is Classified*, FED'N AM. SCIENTISTS: SECRECY NEWS, Oct. 9, 2014, https://fas.org/blogs/secrecy/2014/10/authorized-disclosures/ (describing rejection of FOIA request for reports of authorized disclosures).

[145] Exec. Order No. 13587, 3 C.F.R. 276 (2011), *available at* https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.

[146] *Id*. §6.

[147] 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.

[148] *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).

to detect unauthorized access to, use of, or transmission of classified or controlled unclassified information."[149] 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.[150]

As initially reported by the Senate Intelligence Committee, S. 3454 (112th Cong.) 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 the reporting provision regarding authorized disclosures removed.[151] Some of the 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.[152] 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.[153] Another would have required the Director of National Intelligence to prescribe regulations regarding the interaction of cleared personnel with the media.[154] Such persons would have been required to report all contacts with the media to the appropriate security office.[155] 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) (now classified at 50 U.S.C. Section 3091).[156]

The insider threat issue was revisited in the Intelligence Authorization Act for FY2016, passed as Division M of the Consolidated Appropriations Act of 2016, P.L. 114-113 (2015). Section 306 added a requirement to Title 5, *U.S. Code*, for the DNI to direct agencies to each establish an "enhanced personnel security program" to integrate a broader data set into reassessments of the continuing eligibility of personnel to hold security clearances or sensitive positions. Specifically,

> The enhanced personnel security program of an agency shall integrate relevant and appropriate information from various sources, including government, publicly available and commercial data sources, consumer reporting agencies, social media and such other sources as determined by the Director of National Intelligence.[157]

The provision requires the agency programs to conduct random automated record checks of the selected sources of data at least twice within a five-year period for each covered person, unless

[149] P.L. 112-81, §922 (2011) (codified at 10 U.S.C. §2224 note (2017)).

[150] The Government Accountability Office (GAO) issued an assessment of DOD's implementation of its Insider Threat Program in 2015. U.S. GOV'T ACCOUNTABILITY OFF., GAO 15-544, INSIDER THREATS: DOD SHOULD STRENGTHEN MANAGEMENT AND GUIDANCE TO PROTECT CLASSIFIED INFORMATION AND SYSTEMS (2015).

[151] The bill was enacted as P.L. 112-277 in January, 2013. *See supra* "Declassification vs. Leaks and "Instant Declassification"" for an explanation of the reporting provision, §504.

[152] S. 3454 (as reported, 112th Cong.) §505.

[153] *Id.* §506.

[154] *Id.* §507.

[155] *Id.*

[156] *Id.* §512.

[157] 5 U.S.C. §11001(b)(1) (2017).

that individual is subject to more frequent reviews.[158] The deadline to implement the programs is five years after enactment (which will occur December 15, 2020) or the date on which the backlog of overdue periodic reinvestigations is eliminated, as determined by DNI.[159]

Author Contact Information

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

[158] 5 U.S.C. §11001(c) (2017).

[159] 5 U.S.C. §11001(a) (2017).