Order Code RS21900
Updated December 21, 2006

CRS Report for Congress

The Protection of Classified Information: The Legal Framework

Jennifer K. Elsea
Legislative Attorney
American Law Division

Summary

Recent incidents involving "leaks" of classified information have heightened interest in the legal framework that governs security classification, access to classified information, and penalties for improper disclosure. Classification authority has generally rested 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 and regulations that form the legal framework protecting classified information.

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

[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. 8,381 (1940).

[3] *Compare* Exec. Order No. 10,501 (1953) *with, e.g.* Exec. Order 13,292 (2003).

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] 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

---

[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*, by Genevieve J. Knezo.

[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 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.*

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 may be enforced in court.[17]

---

[11] *Id.* at § 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.

[17] *Id.* §§ 705 and 707.

Executive Order 12,958 (as amended). The present standards for classifying and declassifying information were last amended in March, 2003.[18] Under these current 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.[19] 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;
- 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.[20]

Information is 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.[21] 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.[22] 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.[23] The deadline for declassification can be extended if the threat to national security still exists.[24]

---

[18] Exec. Order No. 12,958, as amended by Exec. Order No. 13,292 (2003), 68 F.R. 15,315 (March 28, 2003).

[19] Exec. Order No. 12,958 (as amended by Exec. Order No. 13,292 (2003)), § 1.1. The unauthorized disclosure of foreign government information is presumed to damage national security. *Id.* at § 1.1(b).

[20] *Id.* at § 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.* at §§ 2.1 - 2.2.

[21] *Id.* at § 1.2.

[22] *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.* at § 1.7(a).

[23] *Id.* at § 1.5.

[24] *Id.* at § 1.5(c).

Classified information is required to be declassified "as soon as it no longer meets the standards for classification,"[25] although there is a presumption that classified information continues to meet these standards. The original classifying agency has the authority to declassify information when the public interest in disclosure outweighs the need to protect that information.[26] 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.[27]

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.[28] 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;[29] 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.[30] Each agency that has classified information is required to establish a system for periodic declassification reviews.[31] The National Archivist is required to establish a similar systemic review of classified information that has been transferred to the National Archives.[32]

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.[33] 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.[34] 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.[35]

The Information Security Oversight Office (ISOO) — an office within the National Archives — is charged with overseeing compliance with the classification standards and

---

[25] *Id.* at § 3.1(a).

[26] *Id.* at § 3.1(b).

[27] *Id.* at § 3.3.

[28] *Id.* at § 3.5.

[29] 50 U.S.C. §§ 403-5c, 403-5e, 431.

[30] Exec. Order No. 12,958 (as amended by Exec. Order No. 13,292 (2003)), § 3.5.

[31] *Id.* at § 3.4.

[32] *Id.*

[33] *Id.* at § 4.1.

[34] *Id.* at § 4.4.

[35] *Id.* at § 4.2.

promulgating directives to that end.[36] 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.[37] 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.[38] The Panel is empowered to decide appeals of classifications challenges[39] and to review automatic and mandatory declassifications. If the ISOO Director finds a violation of Executive Order 12,958 (as amended) or its implementing directives, then the Director must notify the appropriate classifying agency so that corrective steps can be taken. 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.[40]

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.[41] 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.[42] 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.[43]

---

[36] *Id.* at § 5.2.

[37] *Id.* at § 3.1(c).

[38] *Id.* at § 5.3.

[39] *Id.* at § 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.* at § 1.8.

[40] *Id.* at § 5.5.

[41] 18 U.S.C. § 1924. Agencies often require employees to sign non-disclosure agreements prior to obtaining access to classified information, the validity of which was upheld by the Supreme Court in *Snepp v. United States*, 444 U.S. 507 (1980).

[42] 50 U.S.C. § 783.

[43] 18 U.S.C. § 798. This provision is part of the Espionage Act (codified at 18 U.S.C. §§ 792 - 799), which generally protects against the unauthorized transmission of a much broader category of "national defense" information, prescribing fines and a prison term of up to 10 years.