Order Code RS21900
Updated August 5, 2004

The Protection of Classified Information: The Legal Framework

Nathan Brooks
Legislative Attorney
American Law Division

Summary

Classification authority has generally rested with the Executive Branch, although Congress has enacted legislation regarding the protection of certain sensitive information. It is not clear, however, how much – if any – authority the Legislative Branch has to constrain the Executive Branch's power 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.

Introduction. A recent incident involving access to classified information[1] has created heightened interest in the laws that govern security classification and access to classified information, as well as the penalties for violating these laws. This report provides an overview of the relationship between Executive and Legislative authority over sensitive government information, and summarizes the current laws and regulations that form the legal framework protecting such information.

Background. Prior to the New Deal, classification decisions were left to military regulation.[2] In 1940, however, President Franklin Roosevelt issued an Executive Order authorizing government officials to protect national security.[3] Since that time, presidents have followed this precedent and set the federal government's classification standards by Executive Order, but with one critical difference: while President Roosevelt cited specific

[1] The controversy centers around the alleged removal of copies of classified information from the National Archives by Samuel R. Berger, former National Security Advisor to President Bill Clinton. *See* Susan Schmidt and Dan Eggan, *FBI Probes Berger for Document Removal*, Washington Post, July 20, 2004, at A2.

[2] *See* Harold Relyea, *The Presidency and the People's Right to Know*, in The Presidency and Information Policy 1, 16-18 (1981).

[3] Executive Order No. 8,381 (1940).

statutory authority for his action, later presidents have cited general statutory *and Constitutional* authority.[4]

While presidents have generally grounded their authority to classify materials in statute and in the Constitution, it is not clear how much – if any – authority the Legislative Branch has to constrain the Executive Branch's power in this area. The Supreme Court has never directly addressed this issue. Citing the President's constitutional role as Commander-in-Chief,[5] however, 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]

Nevertheless, 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.[7] 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.[8] These include the establishment of uniform procedures for, *inter alia*, background checks, denial of access to classified information, and notice of such denial.[9] The statute also explicitly states that the agency heads are not required to comply with the due process requirement where doing so could damage

---

[4] *See, e.g.*, Executive Order No. 10,501 (1953); and Executive Order 13,292 (2003).

[5] U.S. Constitution, 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"). There is also Supreme Court dicta to suggest a stronger – but still limited – role for Congress in classification of information. *EPA v. Mink*, 410 U.S. 73, 83 (1973) ("Congress could certainly have provided that the Executive Branch adopt new [classification procedures] or it could have established its own procedures – subject only to whatever limitations the Executive Privilege may be held to impose on such congressional ordering").

[7] *See* the 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 authorized a separate classification regime for the protection of nuclear-related information under the Atomic Energy Act (codified at 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 RL31845, *"Sensitive but Unclassified" and Other Federal Security Controls on Scientific and Technical Information" History and Current Controversy*, by Genevieve J. Knezo; *see also* CRS Report RS21727, *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*, by Mitchell A. Sollenberger.

[8] 50 U.S.C. § 435(a).

[9] *Id.*

national security, although the statute directs agency heads to submit a report to the congressional intelligence committees in such a case.[10]

With the authority to determine classification standards vested in the President, these standards tend to change when a new party is swept into the White House.[11] The differences between the standards of one administration and the previous administration 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.[12]

Various congressional committees have investigated ways to bring some continuity to the classification system[13] 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 group of excepted information is that which under Executive Order must be kept secret for national security or foreign policy reasons.[15]

---

[10] *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 cited above, *supra* note 6 and accompanying text, expressing their desire that the legislation not be understood to intrude on the President's authority with regard to security clearances. *See* H.R. Conf. Rep. 103-753,

[11] *See Report of the Commission on Protecting and Reducing Government Secrecy*, S. Doc. 105-2, at 11 (1997).

[12] *Id.*

[13] *See, e.g., id.*

[14] *See, e.g., Availability of Information from Federal Departments and Agencies: Hearings Before the House Committee on Government Operations*, 85th Cong., 1st Sess. (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). This only means, however, that the Executive Branch must comply with its own regulations. Without a statutory standard for determining what is proper, however, courts have been left with the aforementioned Executive Order-based standards. *See* CRS Report RL31245, *Protection of National Security Information: The Classified Information Protection Act of 2001*, by Jennifer Elsea; *see also* Note, *Keeping Secrets: Congress, the Courts, and National Security Information*, 103 Harv. L. Rev. 906 (1990).

Executive Order 12,958 (as amended). The present standards for classifying and declassifying information were last amended in March, 2003.[16] Under these current standards, the President, Vice President, agency heads, and any other officials so 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.[17] Such information must be owned by, produced by, or under the control of the federal government, and must concern one of the following:

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities, intelligence sources/methods, cryptology;
- foreign relations/activities of the United States;
- 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.[18]

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.[19] 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 set at "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.[20] The officer who originally classifies the information must attempt to establish 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 ten years' time or twenty-five years, depending on the sensitivity.[21] The duration of

---

[16] Executive Order No. 12,958, as amended by Executive Order No. 13,292 (2003); available at 68 F.R. 15,315 (March 28, 2003).

[17] Executive Order No. 12,958 (as amended by Executive 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).

[18] *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.

[19] *Id.* at § 1.2.

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

[21] *Id.* at § 1.5.

classification can be extended if the threat to national security possessed by the information still exists.[22]

Classified information is required to be declassified "as soon as it no longer meets the standards for classification,"[23] 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.[24] 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.[25]

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.[26] 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,[27] 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.[28] Each agency that has classified information is required to establish a system for periodic declassification reviews.[29] The National Archivist is required to establish a similar systemic review of classified information that has been transferred to the National Archives.[30]

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.[31] 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.[32] The information being accessed may not be removed from the controlling agency's premises without permission.

---

[22] *Id.* at § 1.5(c).

[23] *Id.* at § 3.1(a).

[24] *Id.* at § 3.1(b).

[25] *Id.* at § 3.3.

[26] *Id.* at § 3.5.

[27] 50 U.S.C. §§ 403-5c, 403-5e, 431.

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

[29] *Id.* at § 3.4.

[30] *Id.*

[31] *Id.* at § 4.1.

[32] *Id.* at § 4.4.

Each agency is required to establish systems for controlling the distribution of classified information.[33]

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.[34] 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.[35] 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.[36] The Panel is empowered to decide appeals of classifications challenges[37] 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.[38]

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.[39] Stiffer penalties – fines of up to $10,000 and imprisonment for up to ten years – attach when a federal employee transmits classified information to anyone that employee has reason to believe is an agent of a foreign government.[40] Fines and a ten-year prison terms 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.[41]

---

[33] *Id.* at § 4.2.

[34] *Id.* at § 5.2.

[35] *Id.* at § 3.1(c).

[36] *Id.* at § 5.3.

[37] *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.

[38] *Id.* at § 5.5.

[39] 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).

[40] 50 U.S.C. § 783.

[41] 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 ten years.