Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

February 3, 2023

# Rules and Statutes Relevant to Safeguarding Classified Materials

The discovery of classified documents at the homes, offices, or other facilities used by Presidents and former Presidents and Vice Presidents has spurred Department of Justice investigations. These discoveries may also raise questions regarding the effectiveness of the policies or procedures for protecting and accounting for materials classified for reasons of national security. This In Focus describes current rules for safeguarding such classified materials and the remedial actions prescribed upon the discovery of a potential breach.

## Executive Order 13,526

The current standards for classifying, safeguarding, and declassifying information were last amended on December 29, 2009, by Executive Order 13,526, 75 Fed. Reg. 707. Under these standards, the President, Vice President, agency heads designated by the President, and any other officials delegated authority by the President, Vice President, or agency head may classify certain types of information upon a determination that its unauthorized disclosure could reasonably be expected to damage national security. The level of classification and the requirements for safeguarding such information vary according to the severity of damage the original classification authority determines would result from its unauthorized disclosure. The executive order defines "damage to the national security" as "harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information."

Under the executive order, information may be classified as "Top Secret" if its unauthorized disclosure could reasonably be expected to cause "exceptionally grave damage to the national security." The standard for a classification level of "Secret" is that its unauthorized disclosure could reasonably be expected to cause "serious damage to the national security," and classification as "Confidential" is applied if the unauthorized disclosure could reasonably be expected to cause "damage to the national security." The original classifying officer must identify or describe the specific danger potentially presented by the information's disclosure. Agency heads are required 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."

Executive Order 13,526 further mandates that "classified information may not be removed from official premises without proper authorization." In addition, officials or employees who are leaving agency service cannot remove classified information from an agency's control or direct that the information be declassified for the purpose of removing it from agency control. Officers and employees of the United States, as well as other individuals specified in the order, shall be subject to appropriate sanctions if they, among other things, knowingly, willfully, or negligently "disclose to unauthorized persons information properly classified" or "contravene any other provision of th[e] order."

Agency heads, for their part, are required to take "appropriate and prompt corrective action when a violation or infraction . . . occurs" and must notify the Information Security Oversight Office (ISOO) in the event of a disclosure to an unauthorized person. The executive order defines a "violation" to include "any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information," and defines an "infraction" as any "knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a 'violation.'" The ISOO Director is required to notify the agency head or appropriate official upon determination that a violation has occurred in order that corrective action may be taken, including administrative sanctions against the offending official or employee.

## ISOO Regulations

The ISOO—an office within the National Archives and Records Administration—is charged with overseeing compliance with the standards for classification and protection of classified information under 32 C.F.R. pt. 2001. These regulations provide that "authorized persons" are responsible for protecting classified information from persons without authorized access to that information. This procedure includes securing the classified information in approved equipment or facilities whenever it is not under the direct control of an authorized person. Furthermore, authorized persons are responsible for "[m]eeting safeguarding requirements prescribed by the agency head."

### Storing Classified Materials

In general, classified materials must be stored in security containers or open storage areas approved by the General Service Administration. Supplemental controls, such as inspections and intrusion detection systems, are required for storing Top Secret and Secret information. Additional safeguarding requirements apply to materials that pertain to special access programs (SAP) and Sensitive Compartmented Information (SCI).

### Transmitting Classified Materials

Classified information physically transmitted outside of government facilities must be protected by two layers, both of which are designed to provide reasonable evidence of tampering and to conceal the material. Couriers and other authorized persons are required to "ensure that the information remains under their constant and continuous protection" and to make "direct point-to-point delivery."

### Reporting Instances of Lost, Compromised, or Disclosed Information

Under governing regulations, any person who "has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person" is required to report the circumstances immediately to the official designated for this purpose. The agency head then conducts an investigation or inquiry into any loss, possible compromise, or unauthorized disclosure of classified information to determine appropriate corrective action and to assess the damage to national security. The agency head or senior agency official shall also notify ISOO when such a violation occurs in the event the breach: (1) is reported to congressional oversight committees in the Legislative branch; (2) may attract significant public attention; (3) involves large amounts of classified information; or (4) reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices. In "[c]ases involving information originated by a foreign government or another U.S. government agency," the department or agency in which the compromise occurred must also advise the foreign government or U.S. government agency that originated the compromised information of the circumstances and findings that affect the originator's information or interests. If the loss, possible compromise, or unauthorized disclosure of classified information involves a possible criminal violation and prosecution is contemplated, agency heads must ensure coordination with the Department of Justice and the legal counsel of the agency where the individual believed to be responsible is assigned or employed.

## Criminal Penalties

There are several statutory provisions that address the protection of classified information, but only certain types of information or in specific situations. The Espionage Act, 18 U.S.C. §§ 793-798, prohibits transmittal of national defense information with the relevant intent or state of mind. For example, § 798 criminalizes the *knowing and willful* disclosure of such information. The Espionage Act also prohibits those who are not entitled to access national security information from willfully retaining it and failing to deliver it to the officer or employee of the United States entitled to receive it. Maximum penalties for violating these provisions range in severity from fines and imprisonment for one year to the death penalty.

There are other statutes that prohibit the unlawful removal or retention of government documents that apply to classified material. For example, 18 U.S.C. § 1924 prohibits "an officer, employee, contractor, or consultant of the United States" in possession of documents or materials containing classified information from "knowingly remov[ing] such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location." Under this provision, an individual can be fined or imprisoned for up to five years. 18 U.S.C. § 641 prohibits the theft or conversion of government property, regardless of its classification. 18 U.S.C. § 2071 generally prohibits, among other things, "willfully and unlawfully conceal[ing], remov[ing], mutilat[ing], obliterat[ing], or destroy[ing] . . . any record,. . . paper, or document" that is "filed or deposited with any clerk or officer of any court of the United States, or in any public office, or with any judicial or public officer of the United States."

For more information relating to the classification, protection, and declassification of national security information, as well as enforcement of these requirements, see CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Jennifer K. Elsea.

**Jennifer K. Elsea**, Legislative Attorney
**Andreas Kuersten**, Legislative Attorney

**IF12318**

## Disclaimer