BRENNAN CENTER FOR JUSTICE
TWENTY YEARS
at New York University School of Law

ELECTION 2016
CONTROVERSIES

Classified Information: What You Need to Know

As Secretary of State, Hillary Clinton used a private server to send and receive work-related e-mails. The discovery that these e-mails included some classified information has spurred a contentious debate over whether Clinton jeopardized national security. This discussion has suffered from a lack of public understanding about the classification system and how it works. Below are facts that add important perspective to the issue.

The Facts About Clinton's E-mails

The FBI reviewed more than 30,000 e-mails that Clinton's team turned over. Several e-mails showed that State Department staffers were making an effort not to include any classified information in their correspondence. The FBI nonetheless discovered that 110 e-mails included information that was classified at the time the e-mails were sent, but was not marked as such in the e-mails. These included eight e-mail chains containing information classified as "Top Secret," the highest level of classification. An additional three e-mails contained the symbol "(C)," which denotes the lowest level of classification ("confidential"), at the beginning of certain paragraphs.

How Classification Works

Who decides whether to classify information?

Each president since Franklin Delano Roosevelt has issued an executive order that governs the classification system. The current order, issued by President Obama on December 29, 2009, is Executive Order 13526 ("EO 13526").

As set forth in the order, the president and certain other high-level executive officials may designate officials as "original classification authorities" ("OCAs"). There were 2,199 such officials in Fiscal Year 2015. These officials are authorized to make original classification decisions.

The standard for classification

OCAs "may" classify information (but are not required to do so) if they determine that "the unauthorized disclosure of the information reasonably could be expected to result in damage to national security," *and* if the information falls within a list of eight broad categories – including, for instance, "military plans, weapons systems, or operations," "intelligence sources or methods," and "foreign relations or foreign activities of the United States." Information may be classified as "confidential," "secret," or "top secret," depending on the severity of the potential harm to national security. *See EO 13526 sections 1.1 and 1.4.*

Although most classification decisions are discretionary, Congress has required the classification of certain types of nuclear information. In addition, EO 13526 states that "The unauthorized disclosure of

foreign government information is presumed to cause damage to the national security." "Foreign government information" is defined as information provided to the U.S. by foreign governments with the expectation that the information will be held in confidence. *See EO 13526 sections 1.1(d) and 6.1(s).*

The process for classification

As described above, the standard for classifying information is a subjective one, and even if the standard is met, classification is usually discretionary. Accordingly, OCAs are required to clearly mark information as classified so that others who use the information know of its status. The marking requirements are fairly elaborate and are set forth in the executive order and implementing regulations.

For e-mails, the highest classification level represented in the e-mail (documents may contain different information that is classified at different levels) must appear at the top and bottom of the text. In addition, each portion of the text – for example, each paragraph – must be marked with a symbol designating the classification level for that portion. There also must be a "classification authority block" toward the bottom of the e-mail, identifying the person who classified the information, the source of authority to classify, and the date for declassification. *See 32 C.F.R. § 2001.23(b).*

Agencies maintain "classification guides," which list specific categories of information that have been classified by OCAs. Agencies are required to keep their guides updated to reflect recent classification decisions. *See 32 C.F.R. § 2001.15(d).*

Receipt and use of classified information

About 4.5 million people are authorized to have access to classified information. There are two ways in which the classification status of information (including the level of classification) is conveyed to those individuals. First, if they are receiving the information in the form of an e-mail or document, it should be marked. Second, regardless of whether markings appear, the information should be encompassed in one of the categories listed in an agency guide.

The vast majority of people who are authorized to have access to classified information are not OCAs; they cannot classify information in the first instance. However, these individuals may need to communicate already-classified information to others. When they do so, they must properly mark the information as classified – an act known as "derivative classification." *See 32 C.F.R. §2001.32.*

Classified information may only be accessed and handled in secure environments, with the level of security depending on the level of classification. In general, classified information may only be handled in special facilities and may only be processed on special networks contained within such facilities. *See 32 C.F.R. Subpart E.*

Penalties for mishandling or leaking classified information

The mishandling of classified information is usually dealt with through administrative sanctions. These may include reprimand, suspension without pay, removal, termination of classification authority, or loss or denial of access to classified information. *See EO 13526 section 5.5.*

Criminal penalties are available for particularly severe abuses. 18 U.S.C. § 1924 imposes penalties for knowingly removing classified material without authority and with the intent to keep it in an unauthorized location. This charge is available only for knowing and intentional mishandling, such as

occurred in the cases of former National Security Advisor Sandy Berger and former CIA Director John Deutch.

In addition, one provision of the 1917 Espionage Act imposes penalties for allowing, through "gross negligence," the removal of information relating to the national defense from its proper place of custody. (50 U.S.C. § 793(f)) As FBI Director James Comey testified before Congress, the Department of Justice has long had concerns about the constitutionality of this provision and therefore has brought only one such prosecution in the past century.

There are also several criminal provisions that penalize the intentional leaking of classified information, which is considered a much more serious offense. President Obama has brought several prosecutions against low-level government officials after they disclosed information that revealed government fraud, waste, or abuse. In contrast, prosecutions against high-level officials who leak information for strategic or personal purposes are rare. General David Petraeus was prosecuted and pled guilty; he was sentenced to two years' probation and a $100,000 fine. Other officials in this category, however – including Richard Armitage, Alberto Gonzales, Leon Panetta, and John Brennan – were not prosecuted or otherwise penalized.

Problems with the Classification System

"Overclassification" – the unnecessary classification of information – is widespread within the federal government. The evidence on this point is overwhelming:

- Since the inception of the classification system, no fewer than eight blue-ribbon commissions or special congressional investigations, including the 9/11 Commission, have found overclassification to be a significant problem.

- Current and former government officials have estimated that anywhere from 50 to 90 percent of classified documents could safely be released.

- When a member of the public asks an agency to declassify a specified document through a process known as "Mandatory Declassification Review," the agency decides in 90 percent of cases that some or all of the information can be released.

In part due to overclassification, the amount of classified information that exists today is staggering:

- Although classification levels have dipped significantly in the past three fiscal years, there were still more than 50,000 new secrets created in FY 2015, and there were more than 50 *million* derivative classification decisions.

- There are more than 2,000 agency classification guides, many of which are hundreds of pages long.

- The Pentagon's list of code names for highly classified "Special Access Programs" runs 300 pages, leading Director of National Intelligence James Clapper to remark, "There's only one entity in the entire universe that has visibility on all SAPs – that's God."

In addition, there is a high rate of noncompliance with the procedural rules designed to ensure that the system works as it should. The Information Security Oversight Office ("ISOO"), the government office charged with overseeing classification policy, conducts yearly audits of agencies' classification programs. In FY 2015, ISOO conducted reviews at nine agencies and found the following:

- Only two of the nine agencies had enacted regulations that fully implemented the standards of EO 13526.
- In a majority of the reviewed agencies, the classification guides were not complete, not accurate, and/or not current.
- ISOO reviewed 1,184 classified documents at the nine agencies and found that 49.2 percent of documents were not properly marked. At two of the agencies had an error rate of more 70 percent, and two had an error rate of 60 percent.
- Training programs were inadequate in most of the agencies reviewed.

Conclusions

The facts above suggest a number of conclusions that may be relevant to the debate over Clinton's e-mails:

- Because the standard for classification decisions is a subjective one and because most classification decisions are discretionary, a person receiving classified information will not necessarily know that the information is classified unless it is properly marked or included in an accurate and updated agency classification guide.
- Officials who regularly deal with particular classified programs will likely recognize classified information associated with those programs, regardless of whether it is marked. However, given the number of classified programs and the sheer volume of classified information, no official could be familiar with all of it.
- The fact that information is classified does not mean that its disclosure could harm national security. Evidence on the prevalence of "overclassification" suggests that *most* classified information could safely be released.
- Overclassification exists at all levels. The "top secret" information in Clinton's e-mails, for example, reportedly included references to the CIA's drone strike program. The existence of this program remains highly classified despite the fact that it is well-known around the world and is often referred to by U.S. officials.
- With only one exception in the past century, the Department of Justice has prosecuted the mishandling of classified information only when it was able to conclude that the person knew he or she was mishandling classified information and intended to do so.