STATEMENT OF

ELIZABETH GOITEIN
SENIOR DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

HEARING ON

MODERNIZING THE GOVERNMENT'S CLASSIFICATION SYSTEM

MARCH 23, 2023

Introduction

Chairman Peters, Ranking Member Paul, and members of the committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice at New York University School of Law.[1]

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. I co-direct the Center's Liberty and National Security Program, which works to advance effective national security policies that respect constitutional values and the rule of law. An important focus of the Liberty and National Security Program is excessive government secrecy in the area of national security. The Brennan Center has published several in-depth research reports on this topic, including *Executive Privilege: A Legislative Remedy* (2009); *Reducing Overclassification Through Accountability* (2011); and *The New Era of Secret Law* (2016).

The primary driver of excessive national security secrecy is "overclassification" (used here to describe the classification of information that does not require protection in the interest of national security; the classification of information at a higher level than warranted by its sensitivity; and the continued classification of information that no longer requires protection). It is widely acknowledged that the government classifies far too much information. Many insiders have concluded that most classified information could safely be made public. Moreover, current processes for declassification have no hope of keeping pace — which means that even properly classified information remains classified long after its sensitivity has abated. The problem has reached crisis proportions is growing exponentially with the proliferation of digital information.

Overclassification produces a range of concrete harms. It harms democratic self-governance, because the American people cannot weigh in on policies and practices that are withheld from them. It harms the rule of law, because it can be used to shield misconduct or even the law itself. It harms interbranch oversight and, in turn, the Constitution's separation of powers, because it deprives Congress and the courts of information they need to do their jobs. And it harms national security, because it impedes the sharing of threat information within or outside the government; leads officials to lose respect for the system and to cut corners in protecting classified information; and expands the universe of people with access to classified information.

The causes of overclassification can be traced to a combination of excessive discretion and skewed incentives. Those authorized to classify information in the first instance have nearly unlimited discretion to do so, while downstream users who are responsible for identifying and marking classified information are often acting without clear guidance. When these officials are faced with the choice of whether to classify or apply classification markings, all of the incentives push in the direction of secrecy. Perhaps most notably, officials who fail to protect information that is later deemed sensitive are subject to harsh penalties, while no one has ever faced serious

[1] This testimony is submitted on behalf of a Center affiliated with New York University School of Law but does not purport to represent the school's institutional views on this topic. Parts of this testimony are taken or adapted from ELIZABETH GOITEIN & DAVID M. SHAPIRO, REDUCING OVERCLASSIFICATION THROUGH ACCOUNTABILITY (Brennan Ctr. for Justice 2011).

consequences for wrongly classifying information. Indeed, agencies lack any mechanism to identify employees or contractors who engage in overclassification.

Congress can and should step in. Although classification policy is primarily set by executive order, the Constitution gives Congress and the executive branch shared authority over national security matters, and Congress has enacted several laws addressing the handling of national security information. There has been no significant presidential action in this area since 2009. With every year that passes, democratic debate, the rule of law, and interbranch oversight are further eroded, and our national security is exposed to additional unnecessary risk.

Lawmakers, blue ribbon commissions, and advocates have put forward many promising solutions to the problem of overclassification. This testimony recommends ten sets of actions Congress should take to reduce unnecessary classification, ensure that classification takes place at the appropriate level, and facilitate the declassification of information that no longer requires protection.

I. The History of Overclassification and Where We Are Today

Overclassification is as old as classification itself. A 1940 executive order on classification by President Franklin Delano Roosevelt marked the beginning of the modern classification regime,[2] and each of the multiple government studies to address the issue since then has reported widespread overclassification.

Coolidge Committee: In 1956, the Defense Department Committee on Classified Information, convened by Secretary of Defense Charles Wilson to study classification at the Department of Defense and chaired by Assistant Secretary Charles Coolidge,[3] warned that "overclassification has reached serious proportions."[4]

Wright Commission: Responding to a congressional mandate, the Commission on Government Security, chaired by Loyd Wright, former President of the American Bar Association, prepared a comprehensive review of government security in 1957.[5] The Commission's Report noted that "[i]n the course of its studies, the Commission has been furnished with information classified as 'confidential' which could have been so classified only by the widest stretch of the imagination."[6]

Moss Subcommittee: In 1958, the House Special Government Information Subcommittee, under Chairman John E. Moss, issued a report on secrecy within the Department

---

[2] KEVIN R. KOSAR, CONG. RESEARCH SERV., 97-771, SECURITY CLASSIFICATION POLICY AND PROCEDURE: E.O. 12958, AS AMENDED 3 (2009).
[3] *See* COMM'N ON PROTECTING AND REDUCING GOV'T SECRECY, REPORT OF THE COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY, S. DOC. NO. 105-2, at app. G-1 (1997) [hereinafter MOYNIHAN COMMISSION REPORT] (discussing Coolidge Committee).
[4] DEF. DEP'T COMM. ON CLASSIFIED INFO., REPORT TO THE SECRETARY OF DEFENSE 6 (1956) [hereinafter COOLIDGE COMMITTEE REPORT].
[5] *See* MOYNIHAN COMMISSION REPORT, *supra* note 3, at app. G-1 (discussing Wright Commission).
[6] COMM'N ON GOV'T SEC., 84TH CONG., REPORT OF THE COMMISSION ON GOVERNMENT SECURITY 174-75 (1957).

of Defense. The report found "innumerable specific instances" of unnecessary secrecy "which ranged from the amusing to the arrogant."[7]

Seitz Task Force: Chaired by Frederick Seitz, former head of the National Academy of Sciences, the Defense Science Board Task Force on Secrecy focused on the effects of classification on scientific progress and reported its findings to the Chairman of the Defense Science Board in 1970. The Task Force reported that "the volume of scientific and technical information that is classified could profitably be decreased by perhaps as much as 90 percent …."[8]

Stilwell Commission: Following the arrest of Navy members charged with espionage, Defense Secretary Caspar Weinberger established the Commission to Review DoD [Department of Defense] Security Policy and Practices, chaired by General Richard Stilwell. The Stilwell Commission focused on "systemic vulnerabilities or weaknesses in DoD security policies."[9] In 1985, the Stilwell Commission reported that, at the Department of Defense, "too much information appears to be classified."[10]

Joint Security Commission: Following the end of the Cold War, Defense Secretary William Perry and CIA Director R. James Woolsey established the Joint Security Commission to "develop a new approach to security."[11] In 1994, the Commission found that "the classification system … has grown out of control. More information is being classified and for extended periods of time."[12]

Moynihan Commission: In 1997, the Commission on Protecting and Reducing Government Secrecy, a bipartisan congressional body chaired by Senator Daniel Patrick Moynihan, issued a comprehensive report on the classification regime. The report found that "[t]he classification system … is used too often to deny the public an understanding of the policymaking process."[13]

Despite the sobering findings of these various bodies, the recommendations they generated were almost never adopted. Thus, according to a leading expert on classification, although "generations of critics have risen to attack, bemoan, lampoon, and correct the excesses of government secrecy," they have rarely "had a measurable and constructive impact."[14]

---

[7] SPECIAL SUBCOMM. ON GOV'T INFO., REPORT OF THE SPECIAL SUBCOMMITTEE ON GOVERNMENT INFORMATION, H.R. REP. NO. 85-1884, at 4 (1958) [hereinafter MOSS SUBCOMMITTEE REPORT].
[8] DEF. SCI. BD. TASK FORCE ON SECRECY, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON SECRECY 2 (1970).
[9] COMM'N TO REVIEW DOD SEC. POLICIES AND PRACTICES, KEEPING THE NATION'S SECRETS: A REPORT TO THE SECRETARY OF DEFENSE app. E, at 1 (1985).
[10] *Id.* at 31.
[11] Letter from Jeffery H. Smith to William J. Perry, Sec'y of Def., and R. James Woolsey, Dir. of Cent. Intelligence (Feb. 28, 1994), *reprinted in* JOINT SEC. COMM'N, REDEFINING SECURITY: A REPORT TO THE SECRETARY OF DEFENSE AND THE DIRECTOR OF CENTRAL INTELLIGENCE ii (1994) [hereinafter JOINT SECURITY COMMISSION REPORT].
[12] *Id.* at 6.
[13] MOYNIHAN COMMISSION REPORT, *supra* note 3, at xxi.
[14] Stephen Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL'Y REV. 399, 404 (2009).

Indeed, some fifty years after the Coolidge Committee's report, the 9/11 Commission highlighted the same problem: "Current security requirements nurture overclassification and excessive compartmentation of information among agencies."[15] This overclassification and compartmentation may have come at a high price. According to the 9/11 Commission, these problems inhibited information sharing, making it more difficult for the government to piece together disparate items of information and anticipate the September 11 attacks.[16]

Government officials of all political stripes have criticized the classification of documents that pose no risk to national security, giving startling estimates of the problem's scope. Rodney B. McDaniel, National Security Council Executive Secretary under President Ronald Reagan, estimated that only ten percent of classification was for "legitimate protection of secrets."[17] A top-ranking Department of Defense official in the George W. Bush administration estimated that overclassification stood at 50 percent.[18] While not putting a number on the problem, former CIA Director Porter Goss admitted, "[W]e overclassify very badly. There's a lot of gratuitous classification going on . . . ."[19] And the current Director of National Intelligence, Avril Haines, has acknowledged the severity of the overclassification problem, noting that "deficiencies in the current classification system undermine our national security, as well as critical democratic objectives, by impeding our ability to share information in a timely manner."[20]

Stark examples of overclassification have occurred throughout the history of the modern classification regime. Some border on the absurd, while others represent violations of the public trust:

- A World War II-era report by the Navy titled "Shark Attacks on Human Beings" remained classified until 1958, when the Moss Subcommittee inquired whether the report warranted classification. The report "detailed 69 cases of shark attacks upon human beings; 55 of the attacks occurred between 1907 and 1940 and at least 5 of the remaining 14 attacks were covered in newspaper stories published prior to the report. The classified document also included an article entitled 'The

---

[15] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U. S., THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 417 (2004) [hereinafter 9/11 COMMISSION REPORT].
[16] *See id.* at 353, 355, 417.
[17] *See* MOYNIHAN COMMISSION REPORT, *supra* note 3, at 36 (quoting McDaniel); *see also Emerging Threats: Overclassification and Pseudo-Classification: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform*, 109th Cong. 115 (Mar. 2, 2005) [hereinafter *2005 Overclassification Hearing*] (written statement of Thomas Blanton, Director, National Security Archive) (discussing McDaniel's statement).
[18] *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats and Int'l Relations of the H. Comm. on Gov't Reform*, 108th Cong. 82 (Aug. 24, 2004) (testimony of Carol A. Haave, Deputy Under Secretary of Defense, Counterintelligence and Security).
[19] *Intelligence Oversight and the Joint Inquiry: Hearing Before the Nat'l Comm'n on Terrorist Attacks Upon the United States* (testimony of Rep. Peter Goss), *available at* http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-22.pdf.
[20] Letter from Avril Haines, Dir. Nat'l Intelligence, to Senators Wyden and Moran (Jan. 5, 2022), *available at* https://sgp.fas.org/othergov/intel/dni-010522.pdf.

Shark Situation in the Waters About New York,' taken from the Brooklyn Museum Quarterly of 1916."[21]

- In 1947, an Atomic Energy Commission official issued a memo on nuclear radiation experiments that the government conducted on human beings. The memo instructed, "[N]o document [shall] be released which refers to experiments with humans and might have [an] adverse effect on public opinion or result in legal suits. Documents covering such work . . . should be classified 'secret.'"[22]

- In the 1960s, the FBI wiretapped Dr. Martin Luther King, Jr.'s telephone. Information about this activity was classified "Top Secret," meaning that its disclosure "reasonably could be expected to cause exceptionally grave damage to the national security,"[23] even though its sole purpose, in the FBI's own words, was to gain information about King's personal life that could be used to "completely discredit [him] as a leader of the Negro people."[24]

- In *New York Times Co. v. United States*,[25] the Nixon administration argued in the Supreme Court for a prior restraint against publication of the "Pentagon Papers" — government documents regarding relations between the United States and Vietnam. Before oral argument, Solicitor General Erwin Griswold reviewed the items that the Department of Defense, State Department, and National Security Agency wanted to keep secret and "quickly came to the conclusion that most of them presented no serious threat to national security."[26] Ultimately, due to Griswold's objections, the government maintained its claim of secrecy with respect to only a fraction of these items in court.

- The Air Force Office of Special Investigations classified a paper on "Espionage in the Air Force Since World War II," submitted by a master's degree candidate at the Defense Intelligence College. One page, marked as "Secret," contained nothing but the following quote from *The Light of Day*, a spy novel by Erick Ambler: "I think that if I were asked to single out one specific group of men, one category, as being the most suspicious, unreasonable, petty, inhuman, sadistic, double-crossing set of bastards in any language, I would say without hesitation: 'The people who run counterespionage departments.'"[27]

---

[21] MOSS SUBCOMMITTEE REPORT, *supra* note 7, at 125.
[22] Memorandum from O.G. Haywood, Jr., Colonel, Corps of Engineers, to Dr. [Harold] Fidler, Atomic Energy Commission, *Medical Experiments on Humans* (Apr. 17, 1947), *available at* http://www.hss.energy.gov/HealthSafety/ohre/roadmap/overview/074930/index.html.
[23] Exec. Order No. 13,526 § 1.2(a)(1), 75 Fed. Reg. 705, 707 (Dec. 29, 2009) [hereinafter E.O. 13526].
[24] SENATE SELECT COMM. TO STUDY GOV'TAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT OF THE SENATE SELECT COMM. TO STUDY GOVERNMENT OPERATIONS: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 125 (1976) [hereinafter CHURCH COMMITTEE FINAL REPORT BOOK III].
[25] New York Times Co. v. United States, 403 U.S. 713 (1971).
[26] Erwin N. Griswold, *Secrets Not Worth Keeping: The Courts and Classified Information*, WASH. POST, Feb. 15, 1989, at A25.
[27] *Espionage in the Air Force Since World War II* (unpublished M.S. thesis, Defense Intelligence College), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB90/dubious-06.pdf.

- During the Clinton administration, the CIA released the government's annual intelligence budget for fiscal years 1997 and 1998, but then asserted that historical budget figures from decades earlier — going back as far as 1947 — had to remain secret. [28]

- After 9/11, the administration of President George W. Bush detained hundreds of alleged "enemy combatants" at Guantánamo Bay without trial. Administration officials justified this measure by asserting that these detainees were the "worst of the worst" and that their detention was critical to national security.[29] However, the administration classified the actual risk assessments that were conducted for the detainees. A leak of these assessments revealed that, in many cases, the government could find no recorded reason for the detainee's transfer to Guantánamo.[30] By definition, that fact reveals no intelligence sources or methods, but it does raise deeply troubling questions about the government's conduct in detaining these individuals.

- A 2006 cable from a U.S. diplomat described a wedding he attended in Russia's Republic of Dagestan. The paragraph describing a typical Dagestani wedding was classified as "Confidential," meaning that its release "reasonably could be expected to cause damage to the national security."[31] The paragraph included the following classified observations:

> Dagestani weddings . . . take place in discrete parts over three days. On the first day the groom's family and the bride's family simultaneously hold separate receptions. . . . The next day, the groom's parents hold another reception, this time for the bride's family and friends, who can "inspect" the family they have given their daughter to. On the third day, the bride's family holds a reception for the groom's parents and family.[32]

- In July 2019, a national security aide expressed concerns to a White House legal adviser about a phone call between President Donald Trump and Ukrainian President Volodymyr Zelensky, in which Trump appeared to condition U.S. aid to

---

[28] *See* Letter from Gregory L. Moulton, Exec. Sec'y, Agency Release Panel, Cent. Intelligence Agency, to Steven Aftergood, Senior Research Analyst, Fed'n of American Scientists (Dec. 14, 2000), *available at* http://www.fas.org/sgp/foia/1947/cia121400.pdf.

[29] *See* Katharine Q. Seelye, *Threats and Responses: The Detainees*, N.Y. TIMES, Oct. 23, 2002, at A14; Joby Warrick, *A Blind Eye to Guantánamo?*, WASH. PO., July 12, 2008, at A2; Donald Rumsfeld, Sec'y of Def., DoD News Briefing with Secretary Rumsfeld and General Pace (June 14, 2005), *available at* http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=3854.

[30] *WikiLeaks: Many at Guantanamo 'Not Dangerous,'* BBC NEWS (Apr. 25, 2011), https://www.bbc.co.uk/news/world-us-canada-13184845.

[31] E.O. 13526 § 1.2(a)(3) (2009).

[32] Confidential Cable from the U.S. Embassy Moscow on a Wedding in Dagestan (Aug. 31, 2006) (on file with the N.Y. TIMES), *available at* http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/cables-06MOSCOW9533. The excerpted text is representative of the full paragraph.

> Ukraine on Zelensky agreeing to open a criminal investigation into Trump's political rival, Joe Biden, and his son Hunter. The White House lawyer responded by ordering the transcript of the call to be moved into a highly classified server in order to tightly limit the number of people with access to it.[33]

In part due to overclassification, the amount of classified information that exists today is staggering. There were more than 50,000 original classification decisions and nearly 50 million derivative classification decisions in FY 2017 (the last year for which such data are publicly available).[34] There were also more than 2,000 agency classification guides, many of which were hundreds of pages long.[35] In 2011, the Pentagon's list of code names for highly classified "Special Access Programs" ran 300 pages, leading former 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."[36]

The current declassification system is incapable of keeping up with the petabytes of classified information being generated each year. Since 1995, executive orders on classification have required that information be "automatically" declassified at 25 years; in practice, however, declassification is anything but automatic. Multiple agencies engage in lengthy "equity reviews," a laborious process that guarantees a massive backlog of classified documents. This backlog will only continue to balloon as the government produces — and classifies — ever-greater volumes of digital data.

II. Why Overclassification Happens

To solve the problem of overclassification, it is necessary to understand why it happens, which in turn requires an understanding of the rules and processes that characterize the current classification system.

A. The Classification and Declassification Systems: An Overview

Most of the rules and processes for classification are set by executive order, as supplemented by regulations issued by the Information Security Oversight Office (ISOO) — the office within the National Archives and Records Association that is responsible for overseeing classification. The executive order that currently governs the classification system as it operates within the executive branch is executive Order 13526, issued by President Obama in 2009.[37]

---

[33] Carol D. Leonnig et al., *White House Lawyer Moved Transcript of Trump Call to Classified Server After Ukraine Adviser Raised Alarms*, WASH PO. (Oct. 30, 2019), https://www.washingtonpost.com/politics/white-house-lawyer-moved-transcript-of-trump-call-to-classified-server-after-ukraine-adviser-raised-alarms/2019/10/30/ba0fbdb6-fb4e-11e9-8190-6be4deb56e01_story.html.

[34] INFO. SEC. OVERSIGHT OFF., 2017 REPORT TO THE PRESIDENT 1 (May 2018), https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf [hereinafter ISOO 2017 REPORT].

[35] *Id*. at 2.

[36] Dana Priest & William M. Arkin, *Top Secret America: A Hidden World, Growing Beyond Control*, WASH. PO. (Jul. 19, 2010), https://www.washingtonpost.com/investigations/top-secret-america/2010/07/19/hidden-world-growing-beyond-control-2/.

[37] In addition, Executive Order 12,829 governs classified information handled by U.S. government contractors, licensees, and grantees. *See* 58 Fed. Reg. 3,479 (Jan. 6. 1993).

Through this executive order, the president has delegated his authority to classify information — an authority that derives from Article II of the U.S. Constitution — to certain executive branch officials, who have in turn delegated the authority more widely.[38] As of 2021, 1,491 officials had the authority to classify information in the first instance.[39]

These "original classification authorities" (OCAs) are given broad discretion to classify information. There are two substantive criteria that must be met: the OCA must determine that disclosure of the information could reasonably be expected to harm national security,[40] and the information must fall within a list of specified categories.[41] The OCA classifies the information as Confidential, Secret, or Top Secret, depending on how much damage could reasonably be expected to occur as a result of disclosure.[42] Within those three levels, information may be more tightly restricted through various additional designations, such as "sensitive compartmented information" (SCI).

The OCA also must specify the date on which the information must be declassified. The executive order sets a default of 10 years, unless the official can determine an earlier date or unless "the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision."[43] Despite the fact that 10 years is the intended default period for classification, there have been several years in which classification for 25 years was more common than classification for 10 years or less.[44]

In order to access classified information, individuals must have a clearance at the appropriate level of classification, and the relevant agency official must assess that they have a "need to know" the information. There are more than 4 million people, inside and outside government, who have security clearances that make them eligible to access classified information.[45] When such people produce documents, emails, or text messages that include classified information, they must mark that information as classified. This process of marking information is known as "derivative" classification. Unlike original classification, derivative classification should not involve any exercise of discretion; the person is merely carrying forward a determination already made by an OCA. To ensure that derivative classifiers are aware of the classification status of the information with which they work, agencies produce security classification guides — manuals that are meant to capture original classification decisions relevant to the agencies' various programs and activities.

In theory, once information reaches its declassification date or otherwise no longer meets the criteria for classification, it should be declassified. In practice, however, information is not

---

[38] *See* E.O. 13526 § 1.3 (2009).
[39] INFO. SEC. OVERSIGHT OFF., 2021 ANNUAL REPORT TO THE PRESIDENT 14 (Jul. 2022), https://www.archives.gov/files/isoo/reports/isoo-2021-annual-report-to-the-president-final.pdf [hereinafter ISOO 2021 REPORT].
[40] E.O. 13526 § 1.1 (2009).
[41] *Id.* at § 1.4.
[42] *Id.* at § 1.2.
[43] *Id.* at § 1.5(b).
[44] *See* ISOO 2017 REPORT, *supra* note 34, at 44.
[45] NAT'L COUNTERINTELLIGENCE AND SEC. CTR., FISCAL YEAR 2019 ANNUAL REPORT ON SECURITY CLEARANCE DETERMINATIONS 7 (Apr. 2020), https://sgp.fas.org/othergov/intel/clear-2019.pdf.

declassified until agencies perform a declassification review. Unless the information is subject to a Freedom of Information Act request or a request for mandatory declassification review (a process by which agencies consider requests by remembers of the public to declassify particular documents), such review is highly unlikely to occur until 25 years after the date of classification.

When classified information reaches the 25-year mark, the executive order states that it "shall be automatically declassified whether or not the records have been reviewed"[46] (a requirement that has been entirely ignored, as discussed below). Nine categories of information are exempt from automatic declassification.[47] Information falling within these categories is subject to another round of review, called "systematic declassification," at the 50-year mark, at which point information falling within two of the nine categories may remain classified for another 25 years.[48]

B. The Causes of Overclassification

The causes of overclassification are manifold, but they boil down to a combination of two primary factors: overbroad discretion on the part of those performing the classification and declassification functions, and a skewed incentive system that leads officials to exercise their discretion in favor of secrecy.

OCAs have almost complete discretion classify information as long as they conclude that its disclosure could harm national security. The information must fall within a list of categories set forth in the executive order, but many of these categories are written extremely broadly — e.g., "foreign relations or foreign activities of the United States,"[49] and "scientific, technological, or economic matters relating to the national security."[50] Moreover, although OCAs must be "able to identify or describe the damage" that could result from disclosure,[51] there is no requirement that they actually do so. In the ordinary course of business, no one reviews their decisions.

Derivative classifiers, for their part, should exercise no discretion at all; in theory, they are merely carrying forward an OCA's decision. In practice, however, there is often significant uncertainty as to the classification status of any given piece of information. There are literally thousands of security classification guides, and they can run into the hundreds of pages. Moreover, some of the guides describe categories of classified information in terms that are so broad, they effectively deputize the user to act as an original classifier. For instance, a State Department guide (one of the few that have been declassified) presented the following criteria for classifying information on United States involvement in international disputes:

> In those cases where the U.S. has been, or may again be, involved as an intermediary, it is an additional concern that information not be released which

[46] E.O. 13526 § 3.3(a) (2009).
[47] *Id.* § 3.3(b).
[48] *Id.* § 3.3(h).
[49] *Id.* § 1.4(d).
[50] *Id.* § 1.4(e).
[51] *Id.* § 1.1(4).

> would prejudice future negotiations on unresolved issues or impair the U.S.'s ability to continue an intermediary role to resolve those issues. For this reason, it is important that information be classified when its release might cause or revive conflict or controversy, inflame emotions, or otherwise prejudice U.S. interests.[52]

When faced with the decision whether to classify information (for OCAs) or to mark information as classified (for derivative classifiers), there are multiple incentives, unrelated to protecting national security, that push in the direction of classification. These incentives, described in detail in the Brennan Center's report, *Reducing Overclassification Through Accountability*, are briefly summarized here.

First and foremost, there is a culture of secrecy that pervades many of the agencies that handle classified information. This culture took hold during the Cold War[53] and was premised on the notion that we knew who the adversary was; we knew that the adversary's spies were attempting to learn military secrets; and we knew exactly who, among trusted federal officials, needed to know the information that we were trying to keep out of enemy hands.[54] Today, these assumptions no longer hold. Deciding who has a "need to know" is a difficult and error-prone undertaking when our enemies include terrorist organizations that are in constant flux, and both the means and the targets of attack are unpredictable. Moreover, given the transnational nature of many modern threats and the focus on civilian targets (including targets of espionage and cyberattacks), information routinely must be shared among federal, state, local, and foreign governments, as well as partners in the private sector and even members of the public.[55] Nonetheless, as one member of the 9/11 Commission stated, the "unconscionable culture of secrecy [that] has grown up in our Nation since the cold war" remains.[56]

Second, it is easier and safer for busy, risk-averse officials to classify everything by rote, rather than giving each decision careful thought. This phenomenon was noted by the Project on National Security Reform, an independent organization that contracted with the Department of Defense, under instruction by Congress, to study the national security interagency system:

> [T]o decide not to classify a document entails a time-consuming review to evaluate if that document contains sensitive information. Former officials within the Office of the Secretary of Defense, for example, who often work under enormous pressure and tight time constraints, admit to erring on the side of caution by classifying virtually all of their pre-decisional products.[57]

---

[52] U. S. DEP'T OF STATE, PUB. NO. DSCG-05-01, CLASSIFICATION GUIDE 16 (1st ed. 2005).
[53] MOYNIHAN COMMISSION REPORT, *supra* note 3, at xliv.
[54] JAMES B. STEINBERG ET AL., BUILDING INTELLIGENCE TO FIGHT TERRORISM, BROOKINGS INSTITUTION POLICY BRIEF, NO. 125 1-2 (2003), http://www.brookings.edu/~/media/Files/rc/papers/2003/09intelligence_steinberg/pb125.pdf.
[55] STEINBERG ET AL., *supra* note 57, at 2.
[56] *2005 Overclassification Hearing*, *supra* note 17, at 89 (statement of Richard Ben-Veniste, former Commissioner, National Commission on Terrorist Attacks Upon the United States).
[57] PROJECT ON NATIONAL SECURITY REFORM, FORGING A NEW SHIELD 304 (2008), https://apps.dtic.mil/sti/citations/ADA491826; *see also* National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-181, § 1049, 122 Stat. 3, 317 (2008) (directing the Department of Defense to contract with an independent organization to study national security reform).

The practice of saving time and effort by defaulting to classification interacts with, and reinforces, the culture of secrecy. Classifiers feel safe to follow this practice because they work in a culture in which secrecy is expected, not challenged.

Third, even when officials do give time and thought to classification decisions, there is a natural tendency to err on the side of secrecy. In the words of a former head of ISOO, "There is no underestimating the bureaucratic impulse to 'play it safe' and withhold information."[58] After all, in matters of national security, the stakes are frequently high, and perceived failures are not looked upon kindly by the public. No government official wants to be responsible for releasing information that leads to the next terrorist attack, regardless of how remote that possibility might be. By contrast, the harms caused by overclassification, while grave and certain (as discussed in Part III of this testimony), are more dispersed and unlikely to be traced to any one government official. As the 9/11 Commission observed, "No one has to pay the long-term costs of over-classifying information, though these costs — even in literal financial terms — are substantial."[59]

Fourth, classifying a document elevates its importance, and by extension, the importance of the person who classifies it. As stated by one journalist in recounting a conversation with a retired intelligence official:

> [The retired official] . . . noticed that classification was used not to highlight the underlying sensitivity of a document, but to ensure that it did not get lost in the blizzard of paperwork that routinely competes for the eyes of government officials. If a document was not marked 'classified,' it would be moved to the bottom of the stack, eclipsed by more urgent business, meaning documents that carried a higher security classification. He observed that a security classification, by extension, also conferred importance upon the author of the document. If the paper was ignored, so too was its author. Conversely, if the materials were accorded a higher degree of protection, they would redound to their author's credit and enhance his or her authority and bureaucratic standing.[60]

---

[58] J. William Leonard, Dir., Info. Sec. Oversight Off., *Remarks at the National Classification Management Society Annual Training Seminar* (June 12, 2003), *available at* https://sgp.fas.org/isoo/ncms061203.html; *see also* Geoffrey R. Stone, *Government Secrecy v. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 192-93 (2007) ("[T]he classification process is poorly designed and sloppily implemented. Predictably, the government tends to *over*-classify information. An employee charged with the task of classifying information inevitably will err on the side of over-classification because no employee wants to be responsible for *under*-classification.").

[59] 9/11 COMMISSION REPORT, *supra* note 15, at 417.

[60] TED GUP, NATION OF SECRETS: THE THREAT TO DEMOCRACY AND THE AMERICAN WAY OF LIFE 44 (2007); *see also* Robert D. Steele, *Open Source Intelligence: What is It? Why is it Important to the Military?* OPEN SOURCE SOLUTIONS 337 (1997), https://www.academia.edu/9817888/1997_OSINT_What_Is_It_Why_Is_It_Important_to_the_Military_White_Paper_ ("Culturally there is a strong attitude, primarily within the intelligence community but to an extent within the operational community, that information achieves a special value only if it is classified. This is in part a result of a cultural inclination to treat knowledge as power, and to withhold knowledge from others as a means of protecting one's power.").

Fifth, classification can be an effective weapon in turf wars between agencies. A former national security official under President Reagan estimated that "protection of bureaucratic turf" accounted for as much as 90% of classification,[61] while Senator Moynihan's study of the issue led him to conclude that "[d]epartments and agencies hoard information, and the government becomes a kind of market. Secrets become organizational assets, never to be shared save in exchange for another organization's assets."[62] Agencies may deny access to other agencies by excessive compartmentation or simply invoking the "need to know" requirement.[63] Alternatively, they may restrict the dissemination of information by classifying it inappropriately or at too high a level. For example, former intelligence officers told *Washington Post* reporters that "[t]he CIA reclassified some of its most sensitive information at a higher level so that National Counterterrorism Center staff, part of the [Office of the Director of National Intelligence], would not be allowed to see it."[64]

Sixth, the fewer the number of people involved in any initiative, the more quickly and smoothly it can be implemented. Particularly when executive officials know that their desired course of action may raise eyebrows among colleagues, highly compartmented classification can be an attractive option. In the words of one former CIA official: "One of the tried-and-true tactical moves is if you are running an operation and all of a sudden someone is a critic and tries to put roadblocks up to your operation, you classify it and put it in a channel that that person doesn't have access to . . . ."[65]

Seventh, classification can be used to hide misconduct or to shield an agency or official from embarrassment or controversy. Indeed, some insiders consider this to be one of the most frequent causes of overclassification. Erwin Griswold, who served as Solicitor General under President Nixon and argued before the Supreme Court that the New York Times should be enjoined from publishing the Pentagon Papers, published an op-ed in the *Washington Post* nearly thirty years later in which he admitted that publication of the papers carried little if any risk to national security. He wrote, "It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental

---

[61] THOMAS P. CROAKLEY, C3I: ISSUES OF COMMAND AND CONTROL 68 (Nat'l Def. Univ. 1991) (quoting Rodney McDaniel, former Exec. Secretary of the Nat'l Sec. Council).

[62] DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 73 (1998).

[63] *See* HOMELAND SEC. ADVISORY COUNCIL, TOP TEN CHALLENGES FACING THE NEXT SECRETARY OF HOMELAND SECURITY 8 (2008) (noting that the "need to know" requirement can serve as a "barrier (and often an excuse) for not sharing pertinent information with homeland security partners."); *see also* M.E. Bowman, *Dysfunctional Information Restrictions*, INTELLIGENCER: JOURNAL OF U.S. INTELLIGENCE STUDIES 29, 32 (2007), http://www.fas.org/sgp/eprint/bowman.pdf (noting the "possessory instincts of agency employees who have worked hard to accumulate information").

[64] Priest & Arkin, *supra* note 36. Of course, the failure to share information among agencies is not entirely attributable to inter-agency competition. Much of the problem stems from more mundane administrative issues such as the maintenance of separate classified computer systems that are not sufficiently interoperable. *See id.* (noting that "[t]he data flow [at the National Counterterrorism Center] is enormous, with dozens of databases feeding separate computer networks that cannot interact with one another. There is a long explanation for why these databases are still not connected, and it amounts to this: It's too hard, and some agency heads don't really want to give up the systems they have"). The culture of secrecy is nonetheless indirectly responsible for such obstacles, as they presumably would have been overcome — or perhaps not have emerged in the first place — if agencies harbored different attitudes toward the relative value of secrecy and openness.

[65] GUP, *supra* note 60, at 28-29 (quoting former covert CIA operative Melissa Mahle).

embarrassment of one sort or another."[66] Similarly, in describing the classified documents he reviewed while serving on the Select Committee on POW/MIA Affairs, Senator John F. Kerry stated that "more often than not they were documents that remained classified or were classified to hide negative political information, not secrets."[67]

Finally, classifiers who fail to protect sensitive national security information face serious repercussions, and the specter of such consequences — combined with the lack of consequences for improperly classifying documents — provides a strong incentive to classify. This phenomenon has been noted by experts for half a century. The Coolidge Committee found that "[a] subordinate may well be severely criticized by his seniors for permitting sensitive information to be released, whereas he is rarely criticized for over-protecting it."[68] The Moss Subcommittee similarly found that "the Defense Department's security classification system is still geared to a policy under which an official faces stern punishment for failure to use a secrecy stamp but faces no such punishment for abusing the privilege of secrecy, even to hide controversy, error, or dishonesty."[69] And the 9/11 Commission observed that there are "risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information."[70] A former FBI official put it more bluntly: "[I]t is a truism that no one ever got in trouble for over-classifying."[71]

This criticism is particularly noteworthy given that, on paper, the sanctions for overclassification have grown stronger over time. President Nixon's executive order provided that "[r]epeated abuse of the classification process shall be grounds for an administrative reprimand."[72] President Carter's executive order expanded the possible sanctions beyond administrative reprimand, to include "reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations," and provided that officials would be subject to these sanctions if they "knowingly and willfully classif[ied] or continue[d] the classification of information in violation of this Order or any implementing directives."[73] Today's executive order contains similar provisions, and it strengthens sanctions by providing that negligent overclassification — in addition to knowing and willful overclassification — can subject the classifier to punishment.[74]

Even if agencies had an appetite for imposing such sanctions, however, there is no regular mechanism in place by which they could detect overclassification on the part of employees. The Stilwell Commission, studying the Department of Defense, reported in 1985

---

[66] Griswold, *supra* note 23.
[67] *Mark-up of Fiscal Year 1994 Foreign Relations Authorization Act: Hearing Before the Subcomm. on Terrorism, Narcotics and Int'l Operations of the S. Comm. on Foreign Relations*, 103rd Cong. 32 (1993) (statement of Sen. John Kerry).
[68] COOLIDGE COMMITTEE REPORT, *supra* note 4, at 3.
[69] MOSS SUBCOMMITTEE REPORT, *supra* note 7, at 158; *see also* Bowman, *supra* note 66, at 34 (noting that, in contrast to the absence of sanctions for overclassification, "revealing 'too much' generally has been considered career-threatening").
[70] 9/11 COMMISSION REPORT, *supra* note 15, at 417.
[71] Bowman, *supra* note 66, at 34.
[72] Exec. Order No. 11,652 § 13(A), 37 Fed. Reg. 5209, 5218 (Mar. 8, 1972).
[73] Exec. Order No. 12,065 § 5-502-03, 43 Fed. Reg. 28,949, 28,961 (Jun. 28, 1978).
[74] E.O. 13526 § 5.5(c) (2009) (requiring sanctions for those who "knowingly, willfully, or negligently" "classify or continue the classification of information in violation of this order or any implementing directive").

that "[c]urrent policy specifies that the signer of a classified document is responsible for the classification assigned but frequently, out of ignorance or expedience, little scrutiny is given such determinations."[75] In 1994, the Joint Security Commission proposed that each agency appoint an overclassification ombudsman who would "routinely review a representative sample of the agency's classified material" to enable "real-time identification of the individuals responsible for classification errors," with an eye toward "add[ing] management oversight of classification decisions and attach[ing] penalties to what too often can be characterized as classification by rote."[76] This recommendation, however, was not implemented.

The executive order governing classification does obligate each agency that has classification authority to maintain a self-inspection program, which must include a review and assessment of the agency's classified product.[77] But there is no requirement that the agency use this process to identify employees who are improperly classifying information, let alone hold them accountable. Moreover, in its on-site reviews, ISOO has consistently found that many agencies fail to maintain an adequate self-inspection program. In fiscal year 2017, for example, ISOO found that almost a quarter of relevant agencies did not conduct document reviews, "a fundamental requirement of self-inspection reporting."[78] Similarly, agencies frequently have failed in their obligation to include "management of classified information" as a critical element in the personnel performance ratings of those who regularly deal with classified information.[79]

Even strongly worded threats of punishment, such as those in the executive order, are ineffective unless there is a mechanism to measure compliance and a commitment to enforcing the rules. Remarkably, despite the increasing severity of the sanctions described in successive executive orders, it does not appear that a classifier has ever lost his or her classification authority or been terminated for overclassification.

When it comes to declassification, the problem of discretion once again rears its head. The executive order clearly states that information must be classified automatically at 25 years, "whether or not the records have been reviewed."[80] And yet, in practice, there is no such thing as automatic declassification. When documents reach 25 years, they are sequentially referred to every agency that is determined to have equities in the information for those agencies' review — a process that often takes years. In the course of this review, agencies frequently take a "pass-fail" approach: If they identify one word of information that is exempt from declassification, they terminate the review (rather than simply redacting the information) and the document must be re-reviewed in its entirety during the next declassification review, which generally takes place at the 50-year mark. In addition, a statutory provision enacted in 1998, known as the "Kyl-Lott amendment," requires line-by-line review of records to protect against the disclosure of certain types of nuclear information, unless the agency determines that the records are "highly unlikely

---

[75] COMM'N TO REVIEW DOD SEC. POLICIES, *supra* note 9, at 49.
[76] JOINT SECURITY COMMISSION REPORT, *supra* note 11, at 25.
[77] E.O. 13526 § 5.4(d)(4) (2009).
[78] ISOO 2017 REPORT, *supra* note 34, at 20.
[79] Exec. Order No. 12,958 § 5.4(d)(7), 68 Fed. Reg. at 15,313, 15,329 (Apr. 17, 1995) (as amended by Exec. Order 13,292); INFO. SEC. OVERSIGHT OFF., 2018 REPORT TO THE PRESIDENT 3 (Aug. 2019), https://www.archives.gov/files/isoo/images/2018-isoo-annual-report.pdf [hereinafter ISOO 2018 REPORT].
[80] E.O. 13526 § 3.3(a) (2009).

to contain" such information.[81] At the end of this laborious process, only around half of the documents that are reviewed are declassified;[82] the rest remain secret until they reach the 50-year mark and undergo review once again.

President Obama established the National Declassification Center with the goal of streamlining this process. His administration also issued guidance to encourage broad categorical determinations as to what types of records would be "highly unlikely" to require line-by-line review under Kyl-Lott. The NDC has had some success in centralizing the existing process and thus making it more efficient, but because the same basic steps are required, it still requires a tremendous expenditure of time and resources. And risk-averse agencies have been reluctant to designate broad categories of records that do not require Kyl-Lott review.

As long as "automatic" declassification continues to involve review by even a single agency, it will be physically impossible for declassification to keep pace with the tsunami of classified documents pouring into the system. As stated in a 2012 report by the Public Interest Declassification Board (PIDB), a presidential advisory board focused on classification policy:[83]

> At one intelligence agency alone, it is estimated that approximately 1 petabyte of classified records data accumulates every 18 months. One petabyte of information is equivalent to approximately 20 million four-drawer filing cabinets filled with text, or about 13.3 years of High-Definition video.
>
> Under the current declassification model, it is estimated that one full-time employee can review **10 four-drawer filing cabinets of text records in one year.** In the above example, it is estimated that one intelligence agency would, therefore, require **two million employees** to review manually its one petabyte of information each year. Similarly, other agencies would hypothetically require millions more employees just to conduct their reviews.[84]

---

[81] National Defense Authorization Act for Fiscal Year 1999, Pub. L. 105-261, § 3161 (1998); National Defense Authorization Act for Fiscal Year 2000, Pub. L. 106-65, §§ 1041, 3149, 3173 (1999).

[82] The declassification rate ranged between 41 and 55 percent from 2010 to 2017. *See* ISOO 2017 REPORT, *supra* note 34, at 2; INFO. SEC. OVERSIGHT OFF., 2016 REPORT TO THE PRESIDENT 7 (2017), https://www.archives.gov/files/isoo/reports/2016-annual-report.pdf; INFO. SEC. OVERSIGHT OFF., 2015 REPORT TO THE PRESIDENT 9 (Jul. 2016), https://www.archives.gov/files/isoo/reports/2015-annual-report.pdf; INFO. SEC. OVERSIGHT OFF., 2014 REPORT TO THE PRESIDENT 7 (May 2015), https://www.archives.gov/files/isoo/reports/2014-annual-report.pdf; INFO. SEC. OVERSIGHT OFF., 2013 REPORT TO THE PRESIDENT 7 (Jun. 2014), https://www.archives.gov/files/isoo/reports/2013-annual-report.pdf; INFO. SEC. OVERSIGHT OFF., 2012 ANNUAL REPORT TO THE PRESIDENT 10 (Jun. 2013), https://www.archives.gov/files/isoo/reports/2012-annual-report.pdf; INFO. SEC. OVERSIGHT OFF., 2011 REPORT TO THE PRESIDENT 10 (May 2012), https://www.archives.gov/files/isoo/reports/2011-annual-report.pdf; INFO. SEC. OVERSIGHT OFF., 2010 REPORT TO THE PRESIDENT 15 (Apr. 2011), https://www.archives.gov/files/isoo/reports/2010-annual-report.pdf.

[83] The PIDB consists of nine members: five appointed by the President, and one each by the Speaker and Minority Leader of the House and the Majority and Minority Leaders of the Senate. The PIDB's founding statute requires the appointment of U.S. citizens who are preeminent in the fields of history, national security, foreign policy, intelligence policy, social science, law, or archival science. They are appointed for renewable three-year terms. *See* National Archives, *Public Interest Declassification Board (PIDB)* (Jan. 10, 2023), https://www.archives.gov/declassification/pidb.

[84] PUBLIC INTEREST DECLASSIFICATION BD., TRANSFORMING THE SECURITY CLASSIFICATION SYSTEM 17 (Nov. 2012) (emphasis in original) [hereinafter PIDB 2012 REPORT].

Classified information that is less than 25 years old is rarely subject to declassification review at all, even if its declassification date has been reached. One exception is "mandatory declassification review" (MDR), a process by which members of the public may request declassification review of a specified document. The agency's initial decision may be appealed within the agency, and the agency's final decision may be appealed to the Interagency Security Classification Appeals Panel (ISCAP), a body made up of senior-level representatives appointed by the Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor.

MDR is a surprisingly effective tool for declassifying information of interest to the public. Agencies reviewing MDR requests in 2021 decided to declassify some or all of the document in around 99 percent of cases, and a substantial majority of appeals to ISCAP tend to be successful.[85] MDR is thus a far more effective way than the Freedom of Information Act, under which judges rarely question agencies' classification decisions, for members of the public to secure the declassification of information. MDR's effectiveness, however, is greatly impeded by a lack of resources and any system for prioritization. As a result, MDR is painfully slow, and ISCAP faces a large and steadily growing backlog of appeals.[86]

III. The Costs of Overclassification

The appropriate classification of information is a key way in which the government protects and promotes public safety. If information that merits classification is released, whether by mistake or through leaks, the cost can be extraordinarily high. In extreme cases, lives may be endangered. This fact is well understood; indeed, it forms the underlying justification for the classification system.

The costs of overclassification are less evident, but they can be equally grave. Overclassification causes three principal sets of harms. First, it keeps voters and (at times) Congress and the courts uninformed about government conduct, thus impairing democratic decision making, the rule of law, and the Constitution's separation of powers. Second, it creates threats to national security by preventing government agencies from sharing information with each other; by straining officials' ability (and, in some cases, willingness) to maintain consistent compliance with the rules designed to protect classified information; and by unnecessarily expanding the pool of individuals who require access to classified information. Finally, classification is expensive—and overclassification wastes taxpayer money.

A. Harm to Democratic Decision Making, Rule of Law, and Separation of Powers

Information is the critical ingredient to responsible self-governance. James Madison famously wrote that "[a] popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both."[87] The people require knowledge of their government's actions in order to debate the issues of the day and help shape

[85] ISOO 2021 REPORT, *supra* note 39, app. B at 25; ISOO 2017 REPORT, *supra* note 34, at 16.
[86] ISOO 2021 REPORT, *supra* note 39, at 12; INFO. SEC. OVESIGHT OFF., FORUM (Nov. 18, 2019), slide 9, *available at* https://www.archives.gov/files/declassification/iscap/2019-11-18-iscap-presentation.pdf.
[87] Letter from James Madison to W.T. Barry (Aug. 4, 1822), *reprinted in* THE COMPLETE MADISON 337 (Saul K. Padower ed., 1953).

the policies developed by their elected representatives. They require such knowledge in order to hold their representatives accountable at the ballot box for choices that do not reflect their wishes. And they require such knowledge — as well as knowledge of the law under which the government operates — in order to seek redress in the courts for actions that contravene the law.

At the same time, Congress and the courts need access to government information to perform their constitutionally assigned roles and to serve as checks on the executive branch. Although members of Congress are deemed eligible to access classified information by virtue of the positions they hold, some categories of information are shared only with a handful of members.[88] Even when information is, in theory, available to all members, many members lack staffers who hold the requisite clearances, limiting those members' ability to meaningfully access and use the information.[89] As for courts, when a civil lawsuit involves classified information, the government generally asserts the state secrets privilege. Not only does that assertion deprive the courts of the benefit of that evidence; it often results in cases being dismissed in their entirety, precluding judicial oversight.[90]

In short, withholding information allows the executive branch to insulate itself from public criticism and, in some cases, congressional and judicial oversight, which in turn increases the likelihood of unwise, illegal, and improper activity. A case in point is the National Security Agency's (NSA) program to collect Americans' telephone records in bulk, conducted under Section 215 of the USA PATRIOT Act.[91] The program was classified and remained a closely-held secret for over a decade until Edward Snowden revealed its existence in 2013. Accordingly, the public had no knowledge of it; many lawmakers were unaware of it, given practical limits on their access to classified information; and the only court that could weigh in on the program was the Foreign Intelligence Surveillance Court ("FISA Court"), which, at the time, operated entirely in secret and heard only from the government.

No convincing argument was ever put forward for the program's classification. Indeed, after the program became public, then-Director of National Intelligence James Clapper acknowledged that the government should not have kept it secret — and strongly hinted that the secrecy was due to fears the American public would not accept the program:

> I probably shouldn't say this, but I will. Had we been transparent about this from the outset right after 9/11— which is the genesis of the [bulk collection] program — and said both to the American people and to their elected representatives, we need to cover this gap, we need to make sure this never happens to us again, so here is what we are going to

[88] 50 U.S.C. § 3093(c)(2).
[89] Mandy Smithberger & Daniel Schuman, *A Primer on Congressional Staff Clearances*, POGO (Feb. 7, 2020), https://www.pogo.org/report/2020/02/a-primer-on-congressional-staff-clearances#heading-3.
[90] *See generally* Elizabeth Goitein, *The State Secrets Sidestep:* Zubaydah *and* Fazaga *Offer Little Guidance on Core Questions of Accountability*, 21 CATO S. CT. REV. 391 (2022).
[91] USA PATRIOT Act, Pub. L. No. 107-56, § 215 (2001) (codified at 50 U.S.C. § 1861 (2018)), *allowed to sunset*, Pub. L. No. 116-69, § 1703(a) (2019).

> set up, here is how it's going to work, and why we have to do it, and here are the safeguards … We wouldn't have had the problem we had.[92]

The "problem" to which Clapper referred was the public outcry that immediately followed the program's disclosure. Civil society swiftly mobilized and clamored for an end to the NSA's bulk collection program.[93] The editorial boards of major news outlets around the country called for the program's termination.[94] Opinion polls showed that, for the first time since 9/11, more Americans were worried that the government had gone too far in sacrificing liberties for counterterrorism goals than that the government's counterterrorism policies did not go far enough.[95]

At the same time, the program's disclosure allowed independent oversight bodies to conduct an objective cost-benefit analysis, which revealed that the program had yielded scant national security benefit. In its review of the bulk collection program, the Privacy and Civil Liberties Oversight Board observed that the program did not make a "concrete difference" in *any* terrorism investigation, and what little value it had merely duplicated FBI efforts.[96] President Obama's separately-commissioned review group similarly found that the program yielded no unique benefit.[97]

The widespread calls for reform, combined with the recommendations of oversight bodies, culminated in the passage of the 2015 USA FREEDOM Act, which is generally acknowledged to be the most significant reform of surveillance authorities since FISA was enacted in 1978.[98] The USA FREEDOM Act disavowed the FISA Court's interpretation of Section 215 and ended the NSA's bulk collection of phone records. It also prohibited any other type of bulk collection under Section 215 and a range of other foreign intelligence authorities.

---

[92] Spencer Ackerman, *US Intelligence Chief: NSA Should Have Been More Open About Data Collection,* GUARDIAN (Feb. 18, 2014), https://www.theguardian.com/world/2014/feb/18/us-intelligence-chief-nsa-open-bulk-phone-collection.

[93] *See, e.g.*, Rebecca Bowe, *NSA Surveillance: Protesters Stage Restore the Fourth Rallies Across US*, GUARDIAN (Jul. 5, 2013), https://www.theguardian.com/world/2013/jul/04/restore-the-fourth-protesters-nsa-surveillance; Zeke J. Miller, *Privacy and Digital Groups Call on Congress to End NSA Surveillance Programs*, TIME (Jun. 11, 2013), https://swampland.time.com/2013/06/11/privacy-and-digital-groups-call-on-congress-to-end-nsa-surveillance-programs.

[94] *See, e.g.,* Editorial, *Bad Times for Big Brother*, N.Y. TIMES (Dec. 21, 2013), https://nyti.ms/3yuqajQ; Editorial, *Mr. President, Put These Curbs on the NSA*, L.A. TIMES (Dec. 20, 2013), https://lat.ms/3uhuyQ6.

[95] *See* PEW RESEARCH CENTER, FEW SEE ADEQUATE LIMITS ON NSA SURVEILLANCE PROGRAM (Jul. 26, 2013), https://www.pewresearch.org/politics/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

[96] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 11 (Jan. 23, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf.

[97] PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 104 (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("The information [gathered from bulk collection] was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.")

[98] *See, e.g.*, Peter Swire, *The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years*, IAPP (June 8, 2015), https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years/.

And it created a panel of *amici curiae* that could provide a perspective other than the government's in FISA Court proceedings.

The public disclosure of the program also prompted the FISA Court, seven years after the bulk collection program had come within its jurisdiction, to issue — and make public — its first written opinion explaining the legal reasoning behind its prior approval orders.[99] This allowed regular federal courts to examine, and ultimately reject, the court's legal analysis. Three separate courts, operating with the benefit of hearing from two parties in an open adversarial proceeding, held that the bulk collection program was unlawful.[100]

The NSA's bulk collection program is thus a case study in how unnecessary executive branch secrecy hinders the democratic process, undermines the rule of law, and prevents Congress and the courts from performing the roles that the Constitution assigns them. There are many other such examples from the recent and not-so-recent past, and likely many current examples that are unknown to the public or to this committee — because they are still classified.

B. Risks to National Security

Excessive secrecy harms national security in at least three ways. First, and most intuitively, it undermines intelligence efforts by inhibiting information-sharing. There are legitimate reasons why information is not shared in some cases, including not only national security concerns, but also privacy considerations that make the sharing of certain types of information inappropriate (e.g., personal information about individuals for whom there is no objective basis to suspect wrongdoing).[101] But needless or overly rigid restrictions on information-sharing can jeopardize national security. The 9/11 Commission, for example, catalogued failures by federal agencies to share information with each other in the months leading up to the September 11 attacks, including the CIA's failure to inform the FBI that one of the future hijackers had entered the United States, and that another had obtained a U.S. visa.[102] According to the Commission:

> What all of these stories have in common is a system that requires a demonstrated 'need to know' before sharing …. Such a system implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate.[103]

---

[99] *See* In re Application of FBI for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109, 2013 WL 5741573 (FISC Aug. 29, 2013).

[100] *See* United States v. Moalin, 973 F.3d 977, 984 (9th Cir. 2020); ACLU v. Clapper, 785 F.3d 787, 812 (2d Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013).

[101] For a discussion of privacy concerns raised by one information-sharing model, namely fusion centers, *see generally* MICHAEL GERMAN, RACHEL LEVINSON-WALDMAN & KAYLANA MUELLER-HSIA, ENDING FUSION CENTER ABUSES (Brennan Ctr. for Justice 2022), https://www.brennancenter.org/our-work/policy-solutions/ending-fusion-center-abuses.

[102] *See* 9/11 COMMISSION REPORT, *supra* note 15, at 355-56, 417.

[103] *Id.* at 417. As a member of 9/11 Commission would later testify, "The Commission found…that the failure to share information was the single most important reason why the U.S. Government failed to detect and disrupt the September 11 plot. There were bits and pieces of critical information available in different parts of the Government, in the CIA, the FBI, and the NSA….But pieces of the information were never shared and never put together in time

Similarly, a 2010 report by U.S. intelligence officials in Afghanistan, which recommended sweeping changes in intelligence gathering as part of counterinsurgency strategy, underscored the importance of limiting classification to promote information sharing. The report stressed the need for ground-level intelligence about conditions in Afghanistan and warned that "[s]ome reports … [become] 'stove-piped' in one of the many classified-and-disjointed networks that inevitably populate a 44-nation coalition."[104] The report called for the creation of information centers to collect intelligence on key districts in Afghanistan, with each center staffed with "a Foreign Disclosure officer whose mission will be to ensure the widest possible dissemination by pushing for the lowest classification."[105]

There is a second, less obvious way in which excessive secrecy undermines national security. As I wrote in *The Nation* two months ago:

> When so much information is classified, the burden of protecting it can become overwhelming. Officials must separately mark each classified paragraph in every e-mail or text message they send. Any conversation that might include even a passing reference to classified information must be moved to a secure facility, and colleagues without the requisite clearance must be excluded. All work involving any modicum of classified information must be performed on secure systems, without regard to travel or family demands that place those systems out of reach.
>
> Under these circumstances, it's no wonder that busy officials cut corners — or simply make mistakes. And they can rationalize these departures because they know that much of the information isn't particularly sensitive. Overclassification thus not only makes consistent compliance with the rules more difficult; it causes officials to lose respect for the system. The result is predictable. In rejecting the government's bid to stifle publication of the Pentagon Papers, Supreme Court Justice Potter Stewart wrote, "When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless."[106]

As early as 1956, the Coolidge Committee found a "casual attitude toward classified information" within the Defense Department[107] and went so far as to liken the overclassification problem to prohibition in the 1920s — people will not follow rules they do not respect:

> Generally speaking, it is very difficult in this country to enforce compliance with rules if those rules are not widely accepted as both necessary and reasonable. The failure of prohibition in the 1920's is the classic example.

---

to understand the September 11 plot." *2005 Overclassification Hearing*, *supra* note 17, at 88 (statement of Richard Ben-Veniste, Commissioner, National Commission on Terrorist Attacks Upon the United States).

[104] MICHAEL T. FLYNN, MATT POTTINGER & PAUL D. BATCHELOR, FIXING INTEL: A BLUEPRINT FOR MAKING INTELLIGENCE RELEVANT IN AFGHANISTAN 17 (Jan. 2010), https://www.wsj.com/public/resources/documents/AfghanistanMGFlynn_Jan2010.pdf.

[105] *Id.* at 19.

[106] Elizabeth Goitein, *The Original Sin Is We Classify Too Much*, NATION (Jan. 25, 2023), https://www.thenation.com/article/politics/biden-documents-overclassification/.

[107] COOLIDGE COMMITTEE REPORT, *supra* note 4, at 6.

…

> When much is classified that should not be classified at all, or is assigned an unduly high classification, respect for the system is diminished and the extra effort required to adhere faithfully to the security procedures seems unreasonable.[108]

The former head of ISOO echoed this sentiment: "The thing that protects information is not the markings, it's not the safes, it's not the alarms … it's people …. Once individuals start losing faith in the integrity of the process, we have an uphill road in terms of having people comply."[109] And while mishandling of *improperly* classified information generally poses little threat to national security, lack of respect for the classification system endangers necessary and unnecessary secrets alike. Accordingly, "[t]o allow information that will not cause damage to national security to remain in the classification system, or to enter the system in the first instance, places all classified information at needless increased risk." [110]

The issue of compliance has become particularly salient in light of recent disclosures that former president Donald Trump, President Joe Biden, and former Vice President Mike Pence had retained classified documents without authorization and stored them in non-secure locations. Attorney General Merrick Garland has appointed special counsels to investigate the actions of Trump and Biden, and no definitive conclusions can or should be drawn until these investigations have been completed. For now, though, there is no public evidence that Biden or Pence mishandled documents deliberately.[111] And while unintentional mishandling of classified information can put national security at risk, it's a common occurrence, for the very reasons discussed above. Even when officials are acting conscientiously, the sheer volume of classified information overwhelms the system designed to protect it.

---

[108] *Id.* at 9.

[109] *2005 Overclassification Hearing*, *supra* note 17, at 64 (testimony of J. William Leonard, Dir., Info. Sec. Oversight Off.).

[110] J. William Leonard, Dir., Info. Sec. Oversight Off., *Remarks at the National Classification Management Society's Annual Training Seminar* 4 (June 15, 2004), *available at* http://www.fas.org/sgp/isoo/leonard061504.pdf.

[111] By contrast, there is evidence in the public domain suggesting that Trump deliberately retained classified documents without authorization even after he was made aware that they were in his possession. The National Archives and Records Administration flagged missing documents for Trump in May 2021, triggering a fifteen-month-long battle over possession. Robert Legare, *National Archives Warned Trump Attorneys in 2021 about Missing White House Documents, Including Correspondence with Kim Jong-Un*, NBC (Oct. 3, 2022), https://www.cbsnews.com/news/national-archives-trump-warning-missing-white-house-documents-kim-jong-un-correspondence/. The FBI ultimately searched Trump's resort after his team first failed for months to return all the documents voluntarily and then failed to fully comply with a subpoena. Glenn Thrush et al., *Trump Search Said to Be Part of Effort to Find Highly Classified Material*, N.Y. TIMES (Aug. 11, 2022), https://www.nytimes.com/2022/08/11/us/politics/trump-fbi-subpoena.html. The Department of Justice reportedly possesses surveillance footage that appears to show documents being moved within Mar-a-Lago following receipt of the government's subpoena. Andres Triay & Robert Legare, *Trump Employee Seen Moving Boxes on Mar-a-Lago Security Footage Identified as Former White House Employee, Source Says,* CBS (Oct. 17, 2022), https://www.cbsnews.com/news/mar-a-lago-security-footage-trump-former-white-house-employee-seen-moving-boxes-source/; Glenn Thrush et al., *Documents at Mar-a-Lago Were Moved and Hidden as U.S. Sought Them, Filing Suggests*, N.Y. TIMES (Aug. 31, 2022), https://www.nytimes.com/2022/08/31/us/politics/trump-mar-a-lago-documents.html.

Finally, overclassification erodes information security by unnecessarily expanding the universe of people who have access to classified documents. When so much information is needlessly classified, even those government employees and contractors who perform relatively low-level or non-sensitive jobs may require access to classified information to do their work. That is one reason why the number of individuals who are eligible to have access to classified information has become so large — more than 4.2 million people, according to a 2020 report by the National Counterintelligence and Security Center.[112] The larger the pool of people who have access to national security information, the greater the chance that the pool will include some people who handle the information irresponsibly. Bad apples are simply inevitable in a barrel that contains so many apples.

C. Financial Costs

According to ISOO, the government spent $18.39 billion on security classification in fiscal year 2017, the most recent year for which this figure is available.[113] This estimate includes such functions as clearing government employees for access to classified information, physically safeguarding facilities that hold classified information, and blocking unauthorized access.

Experts studying classification have repeatedly noted that the government would save money by reducing overclassification. In 1994, the Joint Security Commission reported that "[o]verhauling the classification system will have cost-beneficial impacts on virtually every aspect of security …. [I]f we classify less and declassify more, we will have to clear fewer people, buy fewer safes, and mount fewer guard posts."[114] Similarly, the Moynihan Commission reported that "[t]he importance of the initial decision to classify cannot be overstated. Classification means that resources will be spent throughout the information's life cycle to protect, distribute, and limit access to information that would be unnecessary if the information were not classified."[115]

III. The Path Forward

A. Why Congress Should — and Can — Act

Over the years, presidents have made efforts to rein in overclassification and accelerate declassification. Most recently, President Obama issued executive order (E.O. 13526), which included several positive reforms. Under the order, no information may remain classified indefinitely; classifiers must not classify information if they have significant doubt about whether it merits protection; officials must receive training in avoiding overclassification; and agencies must perform periodic reviews of their classification guidance. The order also established the National Declassification Center to help coordinate and facilitate

[112] NAT'L COUNTERINTELLIGENCE AND SEC. CTR., FISCAL YEAR 2019 ANNUAL REPORT ON SECURITY CLEARANCE DETERMINATIONS, *supra* note 45, at 7.
[113] ISOO 2017 REPORT, *supra* note 34, at 4.
[114] JOINT SECURITY COMMISSION REPORT, *supra* note 11, at 94.
[115] MOYNIHAN COMMISSION REPORT, *supra* note 3, at 35.

declassification.[116] These measures helped to reduce both yearly classification numbers and the backlog of documents awaiting declassification.

Unlike most previous presidents, President Trump did not issue his own executive order on classification, and so the changes put in place by President Obama's order are still in effect. Yet it is clear that these changes, helpful as they were, have not been sufficient. In the fourteen years since the order was issued, both ISOO and the PIDB have continued to sound the alarm. Their reports point to the burgeoning amount of digital data produced by national security agencies and the persistence of bureaucratic impediments to declassification despite the best efforts of the National Declassification Center. Without stricter criteria for classifying information, accountability for improper classification, and truly "automatic" declassification, the system is headed for catastrophic failure.

In the past, executive branch-driven reforms that move beyond incremental change have run up against bureaucratic resistance and inertia. The system has reached a point of dysfunction, however, where fundamental reform is not only appropriate but necessary. That is why Congress should step in and pass legislation to establish certain basic requirements and launch a process within the executive branch to develop further reforms.

There is no question Congress has the authority to enact such legislation. Although the president's "authority to classify and control access to information bearing on national security … flows primarily from [the Commander-in-Chief Clause's] constitutional investment of power in the President,"[117] it does not follow that Congress lacks any power in this area. Under the famous three-part test Justice Robert Jackson set forth in his concurrence in *Youngstown Sheet & Tube Co. v. Sawye*r, Congress is barred from constraining a president's exercise of constitutional powers only where those powers are "conclusive and preclusive," and Congress itself is without any constitutional authority to act.[118] In the many areas in which the president and Congress share power, Congress may exercise its own constitutional authorities even if they tread on those of the president.

The protection of national security falls into this shared-power category. This conclusion flows from the multiple national-security authorities the Constitution assigns to Congress, including the power to provide for the common defense; to declare war; to raise and support armies; to provide and maintain a navy; to make rules for the government and regulation of the land and naval forces; to call forth the militia to execute the law, suppress insurrections, and repel invasions; and to provide for organizing, arming, and disciplining the militia.[119]

Consistent with this understanding, Congress has passed many laws over the past century that bear directly on the handling of national security information. These include the National Security Act of 1947 (requiring protection of national-security information but also requiring disclosures to Congress), the Atomic Energy Act of 1954 (establishing a system for protecting

[116] E.O. 13526 §§ 1.1(b), 1.5(d), 1.9(a), 2.1(d), 3.7(a) (2009).
[117] Dep't of the Navy v. Egan, 484 U.S. 518, 527 (1988).
[118] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 638 (1952) (Jackson, J., concurring).
[119] U.S. CONST., art. I, § 8; *see also* Stephen I. Vladeck, *The Separation of National Security Powers: Lessons from the Second Congress*, YALE L. J. FORUM 610 (Feb. 15, 2020); Rebecca Ingber, *Congressional Administration of Foreign Affairs*, 106 VA. L. REV. 395 (2019).

information about nuclear weapons and capabilities), and the Freedom of Information Act (authorizing courts to review governmental withholding of classified information). Of particular relevance here, Congress in 2010 passed the Reducing Overclassification Act, which imposed training and reporting requirements, permitted the use of cash awards as incentives for employees to use the classification system responsibly, and required the Director of National Intelligence to standardize formats for intelligence products to promote wider sharing.[120] Congress similarly included several provisions relating to classification in the National Defense Authorization Act for Fiscal Year 2020, including requiring the Department of Defense to adopt classification standards and supporting metadata that better enable information sharing and directing reforms to how the government conducts background investigations and adjudicates personnel security clearances.[121]

B. Reforms Congress Should Enact

There are several commonsense reforms that would directly address the underlying causes of overclassification. Many of these reforms have long been recommended by expert commissions, ISOO, and/or PIDB, and versions of some of these reforms appear in bills that have been introduced in recent years.[122] Taken together, the measures described below could make a significant dent in the problems of overclassification and inadequate declassification.

1. Direct the White House to oversee the development and implementation of technologies to assist in derivative classification and declassification.

There is broad consensus among those who study the classification system (including ISOO and PIDB) that solving the system's problems will require much greater use of advanced technologies. With respect to declassification in particular, there is simply too much classified information being generated to rely on human effort alone.[123] The process of identifying material subject to declassification should be automated to the maximum extent possible, deploying advanced analytics, machine learning, and context accumulation technology. These technologies can also assist in the act of derivative classification, as they are likely to be faster and more accurate in matching newly-generated information to already-classified information set forth in other documents or described in security classification guides. (Original classification decisions, by contrast, require human judgment and are not amenable to automation.)

Even though the use of technology is likely to improve accuracy in declassification and derivative classification decisions, embracing automation will require agencies to abandon the

[120] Pub. L. 111-258, §§ 5(a)(3), 6(a), 6(b), 7 (2010).
[121] National Defense Authorization Act for Fiscal Year 2020, Pub. L. 116-92, §§ 1627, 1651, 1718, 1759, 6721, 6741 (2019).
[122] Some of the bills propose additional measures, beyond those identified in this testimony, that are also worth consideration. For instance, the Clearance and Over-Classification Reform and Reduction Act, introduced in the 113th Congress, would require the president to set a goal of reducing classification activity by 10% within five year's of enactment. *See* H.R. 5240, 113th Cong. § 103 (2014); S. 2683, 113th Cong. § 103 (2014). The idea of setting goals for the reduction of classification activity has significant merit (although the goal should be more ambitious than 10%). There could be practical obstacles to such a measure, however. Accurately measuring classification activity in the digital environment has proven to be a major challenge, to the extent that the current director of ISOO ceased collecting and reporting these statistics in 2017. *See* ISOO 2018 REPORT, *supra* note 79, at ii.
[123] See Part II.B, *supra*.

(unattainable) goal of "no risk" in favor of a "risk management" approach—an imperative long recognized by internal and external studies of the classification system.[124] It will also require an investment of time and resources, not only on researching and developing the programs themselves, but on front-end tools to enable metadata standardization and data-tagging in the original classification process, including the creation of a government-wide metadata registry (as suggested in the PIDB's 2012 report and a 2020 RAND study on government secrecy).[125]

Toward the end of the Obama administration, the CIA partnered with the University of Texas to develop and pilot the use of technology to identify sensitive content in emails held by the Reagan Presidential Library. The pilot showed great promise; however, the resources were not in place to enable follow-up, and the effort stalled.[126]

The critical elements to move this effort forward are leadership and resources. To ensure that these are in place, Congress should direct the Office of Management and Budget (OMB) to incorporate the development and deployment of technologies to assist in derivative classification and declassification into OMB's information technology modernization program. OMB should coordinate with ISOO, the senior agency officials designated under section 5.4(d) of Executive Order 13526, and the agencies' chief information officers to develop implementation plans and budgets, with the goal of including government-wide implementation of technology-assisted classification/declassification in the FY 2024 budget. Most important, Congress must provide the resources necessary to support development and implementation of these technologies.

2. Create a White House-led task force to narrow the substantive criteria for classification, create a more specific definition of "damage to the national security," and limit exemptions from automatic declassification

As discussed above, overclassification is enabled by a lack of objective criteria to guide original classification decisions. While OCAs must be able to exercise discretion and judgment, these should not be unbounded. The classification categories listed in section 1.4 of the executive order are too broad to provide meaningful constraints. Moreover, the concept of "damage to the national security" is not defined and is extremely elastic (a point noted in the 2020 RAND study).[127] President Nixon's executive order on classification addressed this latter issue by providing specific examples of what would constitute "exceptionally grave damage," "serious

---

[124] *See, e.g.,* PIDB 2012 REPORT, *supra* note 84, at 2, 5n.vi, 12-14, 19, 23; JAMES B. BRUCE ET AL., SECRECY IN U.S. NATIONAL SECURITY: WHY A PARADIGM SHIFT IS NEEDED 8-10 (RAND Nov. 2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE305/RAND_PE305.pdf. In addition, at least in the short term, derivative classification should be technology-*assisted*, not technology-*driven*. In other words, the technologies should be used to flag information for the authorized holder, who then makes the decision about what to mark as classified. With respect to declassification, the goal should be to move to a fully automated system. However, to reassure agencies, there could be a phase-in period during which the technology could be further tested to demonstrate its accuracy. If the technology was not shown to be consistently as accurate or more accurate than human declassification, the full adoption of automated declassification could be pushed back until the requisite level of accuracy was achieved.

[125] *See, e.g.,* PIDB 2012 REPORT, *supra* note 84, at 5, 27; BRUCE ET AL., *supra* note 124, at 11, 13.

[126] Public Interest Declassification Bd., Public Meeting (Jun. 2015), 34:14 *et seq*., 54:00 *et seq.*, available *at* https://www.youtube.com/watch?v=2ApwyaB4ldQ.

[127] BRUCE ET AL., *supra* note 124, at 11.

damage," and "damage to the national security," but this helpful feature was not adopted by subsequent presidents.[128]

A similar problem exists at the back end of the process: there are multiple categories of information exempted from automatic declassification pursuant to section 3.3(b) of the executive order, and these categories are in some cases too vague (for instance, any record that could "reveal information . . . that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States"). Such records are generally not revisited until the 50-year mark.

In its 2020 report, the PIDB states that "[c]ritical reforms to the system will include a tightening of definitions and greater specificity for categories requiring protection in the first place."[129] Accomplishing this goal responsibly will require input from senior agency officials who can expertly assess the trade-offs between specificity and discretion.

Congress should thus direct the president to establish a White House-led committee of senior officials at those agencies most affected by classification policy. The committee should be charged with developing recommendations to narrow the criteria for classification, to provide guidance on what constitutes "damage to national security," and to refine the exemptions from automatic declassification. The recommendations should be submitted to both the president and Congress for further action.

There is precedent for such a committee: President Obama established a White House-led Security Classification Reform Committee consisting of senior agency officials to consider reforms to the classification system beyond those contained in his 2009 order.[130] The committee did not issue any public recommendations, however, and no significant changes were made to the classification system. A congressional mandate to deliver recommendations will ensure that the effort does not simply lapse.

---

[128] Exec. Order No. 11,652 § 13(A), 37 Fed. Reg. 5209, 5218 (Mar. 8, 1972).

[129] PUBLIC INTEREST DECLASSIFICATION BD., A VISION FOR THE DIGITAL AGE: MODERNIZATION OF THE U.S. NATIONAL SECURITY CLASSIFICATION AND DECLASSIFICATION SYSTEM 10 (2020), https://www.archives.gov/files/declassification/pidb/recommendations/pidb-vision-for-digital-age-may-2020.pdf [hereinafter PIDB 2020 REPORT].

[130] THE OPEN GOVERNMENT PARTNERSHIP: SECOND OPEN GOVERNMENT NATIONAL ACTION PLAN FOR THE UNITED STATES OF AMERICA (Dec. 5, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/us_national_action_plan_6p.pdf. In addition, in 2020, the PIDB recommended that the president designate an "Executive Agent…and Executive Committee with authorities and responsibilities for designing and implementing a transformed security classification system." PIDB 2020 REPORT, *supra* note 129, at 2. The board suggested designating the Director of National Intelligence as the Executive Agent and advised that the Executive Committee should be "made up of appropriate senior leaders at those departments and agencies most impacted." *Id.* A similar approach is embodied in the Declassification Reform Act, a bill introduced by Senators Ron Wyden (D-OR) and Jerry Moran (R-KS). *See* S. 3733, 116th Cong. (2020).

The proposal set forth above differs in two key respects. First, there is sufficient information about many of the problems that plague the classification system for Congress to take action on them now, rather than tasking a committee with solving them. A committee should instead focus its time and attention on the area where its expertise is needed to fill in the contours of reform: revising the criteria for classification. Second, the committee should be led by the White House, rather than the Director of National Intelligence, to ensure the buy-in of agencies (such as the Department of Defense) that have deep equities in classification policy but are not members of the intelligence community.

3. Clarify that intelligence sources and methods may be classified only if their disclosure would harm national security

The National Security Act of 1947, as amended, states that the Director of National Intelligence "shall protect intelligence sources and methods from unauthorized disclosure,"[131] and the executive order on classification includes "[i]ntelligence sources and methods" among the categories of classifiable information. A persistent problem over the decades has been lack of clarity regarding the scope of "sources and methods." Interpreted literally, the term could include extremely general and well-known information about the ways intelligence agencies operate (for instance, the fact that the CIA uses confidential human sources). As Senator Moynihan stated in his 1997 study of the classification system: "Too often, there is a tendency to use the sources and methods language contained in the National Security Act of 1947 to automatically classify virtually anything that is collected by an intelligence agency — including information collected from open sources."[132] Relatedly, the law has been interpreted to allow — or even require — the classification and non-disclosure of intelligence sources and methods, regardless of whether their disclosure would cause national-security harm.

Congress should address this problem in two ways. First, it should amend the relevant provisions of the National Security Act to clarify that "intelligence sources and methods," like any other category of classifiable information, may be classified only if their disclosure could reasonably be expected to harm national security. For instance, if a particular collection technique does not rely on secrecy for its effectiveness, there is likely no valid basis for classifying it. In addition, Congress should task the Director of National Intelligence with issuing guidance regarding the proper scope of the requirement to protect "sources and methods," along with the reasons for that requirement (as recommended by the Moynihan Commission). This would assist OCAs in assessing whether information falls within the intended reach of the provision.

4. Require OCAs to describe briefly the reasonably-expected harm to national security

Under the existing executive order, OCAs must be "able to identify or describe the damage" to national security that could reasonably be expected to result from disclosure. In practice, however, they are almost never called upon to provide any such identification or description. OCAs instead mark classified documents with the subsection of the executive order that corresponds to the relevant category of classifiable information — e.g., 1.4(d) if the information pertains to "foreign relations or foreign activities of the United States," or 1.4(e) if it pertains to "scientific, technological, or economic matters relating to the national security." These categories are too broad to shed any light on the specific reasoning behind the classification decision.

Congress should require OCAs to briefly describe in writing the damage to national security that could reasonably be expected to result from disclosure; those descriptions would then be incorporated into security classification guides. This practice would have several benefits. It would be a forcing mechanism to prevent classification by rote. It would assist

[131] 50 U.S.C. § 3024(i)(1).
[132] MOYNIHAN COMMISSION REPORT, *supra* note 3, at xxvii.

derivative classifiers in assessing whether a given piece of information is covered by an original classification decision. And it would enable accountability for improper use of the classification system (discussed further below).[133]

As proof of concept, the National Geospatial-Intelligence Agency (NGA) already has implemented an expanded version of this recommendation. Every classified line item in the consolidated NGA security classification guide must include three "enhancement statements." These include (1) a "value statement," which explains why the information is being classified; (2) a "damage statement," which describes the potential impact to national security should an unauthorized disclosure occur; and (3) an "unclassified statement," which outlines how the user can address the classified line item in an unclassified manner.[134] This system has been in place since 2017.[135]

5. Restrict the classification of legal authorities

In recent years, public attention has focused on the phenomenon of "secret law." The term is best understood to encompass rules, directives, or legal opinions that set binding standards for government conduct but are not published or otherwise made publicly available. Well-known examples include unpublished opinions of the FISA Court or the Department of Justice's Office of Legal Counsel. Within the intelligence community, however, the phenomenon is broader: many of the issuances that would qualify as "rules" under the definitions of the Administrative Procedures Act (APA) are classified and/or not published in the Federal Register, despite not being covered by any apparent exception to the APA's publication requirements.

As explained in a 2016 Brennan Center report, secret law raises constitutional concerns and triggers practical harms beyond those implicated by other types of government secrecy.[136] Congress should recognize these unique considerations and establish a heavy presumption against classification of any rules, directives, guidelines, or legal opinions that are binding within an agency. The most effective way to operationalize this presumption is to create a higher substantive standard for classifying such materials.[137] Congress also should raise the

---

[133] Although this requirement would create an additional burden on OCAs, that burden would not be excessive. Based on the last few years of available statistics, there are nearly 1,500 OCAs, and they make around 50,000 original classification decisions each year. ISOO 2017 REPORT, *supra* note 34, at 8; ISOO 2021 REPORT, *supra* note 39, at 14. The average OCA thus makes approximately 25 original classification decisions in a year, or roughly two per month. Providing a brief written justification in each such instance should not be an overwhelming task.

[134] NAT'L GEOSPATIAL INTELLIGENCE AGENCY, THE CONSOLIDATED NGA (CONGA) SECURITY CLASSIFICATION GUIDE 8 (SCG) (Jun. 7)

[135] ALLISON W. HALL, NAT'L GEOSPATIAL INTELLIGENCE AGENCY, MEMORANDUM FOR DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE, FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW – FINAL PROGRESS REPORT (Jun. 12, 2017), https://irp.fas.org/agency/nga/fcgr-2017.pdf.

[136] Dakota S. Rudesill, *It's Time to Come to Terms with Secret Law: Part I*, JUST SEC. (Jul. 20, 2016), https://www.justsecurity.org/32120/time-terms-secret-law-part/.

[137] For instance, the Brennan Center for Justice has recommended that "[l]egal rules and authoritative legal interpretations should be withheld only if it is highly likely that their disclosure would result, either directly or indirectly, in loss of life, serious bodily harm, or significant economic or property damage." ELIZABETH GOITEIN, THE NEW ERA OF SECRET LAW 7, 64-65 (Brennan Ctr. for Justice 2016), https://www.brennancenter.org/our-work/research-reports/new-era-secret-law.

procedural bar for classification of legal authorities by requiring sign-off from an inter-agency body of senior officials (either the committee recommended above or ISCAP).

To the extent some authorities that may fairly be characterized as "law" would remain subject to classification, Congress should put in place three measures to mitigate the effects of this secrecy.

- Congress should require that any classified legal opinion which concludes that a statutory constraint on executive action is unconstitutional or otherwise not binding on the executive branch must be provided to the appropriate congressional oversight committees within a set period of time (e.g., 30 days) of issuance. If the opinion addresses covert operations as defined in the National Security Act, disclosure could be limited to the "Gang of Eight."

- Congress should direct agencies to compile, on an annual basis, any classified issuances that would otherwise qualify as "rules" and be subject to the APA's publication requirement. These compilations — akin to the "classified Federal Register" proposed by Senate select committees examining executive branch abuses in the 1970s[138] — should be made available to Congress, agency Inspectors General, the Privacy and Civil Liberties Oversight Board, and others with appropriate clearances and a lawful oversight function.

- Congress should direct agencies to maintain public indices of their unpublished legal rules and opinions; the indices, which should be updated on a semi-annual basis, should contain the date of issuance and the general subject matter of the rules or opinions, as well as any other information that can be made public.

6. Rebalance the incentives that lead to overclassification

Almost every study to examine the problem of overclassification has observed the skewed nature of the incentives driving classification decisions. One major aspect of this imbalance is the fact that agency employees face severe penalties for failing to protect sensitive information, while penalties for unnecessary classification — although theoretically available — are never imposed. Both sides of the equation require adjustment in order to properly rebalance the incentives.

In its 2012 report, the PIDB recommended creating a "safe harbor" for officials who, when in doubt, make good-faith decisions not to classify information.[139] Congress should codify this approach. In a similar vein, it should prohibit penalizing derivative classifiers who fail to apply classification markings in cases where classification is not unambiguously required by either a properly marked source document or a current security classification guide that was provided to the classifier along with appropriate training in its contexts. This would not only

---

[138] *See* SPECIAL COMM. ON NATIONAL EMERGENCIES AND DELEGATED EMERGENCY POWERS, 93D CONG., EXECUTIVE ORDERS IN TIMES OF WAR AND NATIONAL EMERGENCY 10 (Jun. 1974), https://li.proquest.com/elhpdf/histcontext/CRS-1974-AML-0031.pdf; *Excerpts from Report on Intelligence Unit*, N.Y. TIMES (Apr. 27, 1976), https://www.nytimes.com/1976/04/27/archives/excerpts-from-report-of-intelligence-unit-excerpts-broader.html.

[139] PIDB 2012 REPORT, *supra* note 84, at 3.

remove a major driver of overclassification; it would also incentivize greater care in the marking of documents and in the preparation and distribution of classification guides.

In addition, Congress should charge agencies with developing systems for identifying and holding accountable individuals who misuse the classification system by willfully, knowingly, or negligently classifying information that does not meet the standards for classification. The current order requires agencies to include "the designation and management of classified information" as a critical element in the performance evaluations of staff whose duties involve creating, disseminating, or safeguarding classified information,[140] but according to ISOO's 2018 report, many agencies have not implemented this requirement.[141] Congress should make clear that this measure is not optional, and it should transfer responsibility for implementing it to the heads of agencies. Congress also should require agencies to conduct spot audits for the purpose of identifying employees or contractors who classify irresponsibly. Although such audits necessarily would capture only a small percentage of an agency's classification activity, they would help to foster a culture of accountability.

7. Reform "automatic" declassification

The most important reform to the automatic declassification process is likely to be the application of technological tools, as discussed above, that would literally automate declassification. Pending broad implementation of such tools, however, Congress should address the problem of lengthy equity reviews by multiple agencies.[142]

One option is to eliminate multiple-agency equity review, as many have proposed. In its place, either a single agency or the National Declassification Center would be responsible for declassification.[143] Alternatively, Congress could stop short of ending equity review entirely, but instead (1) require agency review efforts to be coordinated and simultaneous rather than sequential, and (2) empower the National Declassification Center to declassify records if agencies have not completed their equity reviews within a reasonable period of time (e.g., within six months). This would not only prompt quicker action by the agencies; it would incentivize them to focus their reviews on the records most likely to need them.

The argument will no doubt be raised that it is risky to forego or cut short multi-agency equity review. There could indeed be some risk. However, that risk is routinely accepted on the front end of the classification process. Before transmitting information, agency employees who hold security clearances must determine whether that information has been classified by *any* agency. Agency employees who work on matters in connection with other agencies are provided access to all of the relevant security classification guides and are entrusted to apply that guidance, without engaging in a multi-agency review process. If anything, the potential harm that

---

[140] E.O. 13526 § 5.4(d)(7) (2009).
[141] ISOO 2018 REPORT, *supra* note 79, at 3.
[142] In its 2020 report, the PIDB advised that "[t]he current analog process of sequentially referring classified records to multiple agencies with equities under review must be minimized to the greatest extent possible." PIDB 2020 REPORT, supra note 129, at 8.
[143] Herbert Briick, *Simplifying the Declassification Review Process for Historical Records*, PUBLIC INTEREST DECLASSIFICATION BD. (Mar. 29, 2011), https://transforming-classification.blogs.archives.gov/2011/03/29/simplifying-the-declassification-review-process-for-historical-records/.

could result from incorrectly applying another agency's guidance is lower in the declassification context, as the information is likely to be significantly older.

There are four other steps Congress should take to facilitate automatic declassification. First, Congress should prohibit "pass-fail" review and require agencies to redact any information that is exempt from declassification rather than using it as a basis to remove the entire document from the process.

Second, Congress should instruct the Department of Energy and the Department of Defense to convert "Formerly Restricted Data" (FRD) (a category of nuclear information that Congress has determined can be adequately protected through the non-statutory classification system) either to national security information or to "Restricted Data" (RD), thus taking it out of an unnecessary information-protection limbo.[144]

Third, Congress should repeal the Kyl-Lott amendment. The provision was enacted more than 20 years ago in response to instances in which agencies failed to identify sensitive information in declassification reviews. Declassification processes and practices today are very different, and agencies have had ample time in the interim to segregate out the information that is likely to contain RD and FRD. The continued need for the legislation is thus questionable. But even if there were still concerns, the Kyl-Lott amendment epitomizes the "no risk" approach that has brought the declassification system to its knees and that experts agree must be discarded in favor of a "risk management" approach.

Finally, even if the exemptions from automatic declassification are narrowed (as recommended above), some documents will remain classified beyond the 25-year threshold. The review that takes place at 50 years also leaves a significant percentage of documents classified. To prevent the indefinite classification of information — which is prohibited under the executive order[145] — Congress should establish a "drop dead" date at which the classification of all information that does not reveal the identity of a confidential human source or key design concepts of weapons of mass destruction would simply expire (in other words, no declassification would be required). Any exceptions would have to be approved on a case-by-case basis by ISCAP. The idea of a forty-year drop-dead date was endorsed by ISOO during the Clinton administration, but it was rejected in favor of "automatic" declassification,[146] which is subject to nine exemptions and is not in any sense automatic. Congress should resurrect this idea and codify it.

8. Improve Agencies' Security Classification Guidance

As with declassification, the most effective solution to overclassification by *derivative* classifiers is likely to be the development of technologies that can assist in derivative declassification decisions. Pending the implementation of such technologies, Congress should supplement an existing requirement in the executive order for agencies to review their security classification guides.

---

[144] For more on this recommendation, *see* PIDB 2012 REPORT, *supra* note 84, at 22-23.
[145] E.O. 13526 § 1.5(d) (2009).
[146] *See* Steven Aftergood, *A "Drop Dead" Date for Classified Info*, FEDERATION OF AMERICAN SCIENTISTS (Jan. 25, 2021), https://fas.org/blogs/secrecy/2021/01/drop-dead-date/.

As discussed above, the purpose of such guides is to facilitate derivative classification by identifying information that has been classified by OCAs. In theory, the guides should be sufficiently clear and specific that two derivative classifiers could not reasonably reach different conclusions about whether a given document contains classified information. In practice, however, some guides describe broad categories of classified information, leaving the derivative classifier to make her own judgment about how and whether the guidance applies.

The executive order requires agencies to periodically review their security classification guides,[147] and ISOO has specified that agencies must perform such reviews at least once every five years.[148] But the purpose of these reviews, as stated in the order, is to "to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified"[149] — not to ensure that the guides are clear and unambiguous in the direction they provide.

Nonetheless, the Director of ISOO, in his 2019 report, noted that his team had encountered guides "that lacked sufficient specificity to facilitate proper and uniform derivative classification decisions."[150] He stated that ISOO, in FY 2020, would begin a "multi-year oversight project to assess [security classification guides] throughout the executive branch," to determine whether the guides are correctly prepared and updated as well as whether they are sufficiently specific.

Given ISOO's resource limitations and a long history of agencies failing to fully comply with ISOO regulations and directives, Congress should put the force of statutory law behind this important effort. Specifically, Congress should require agencies to conduct a review of their security classification guides for the purpose of ensuring that the guides (1) accurately reflect current classification decisions and do not include categories of information that are no longer eligible for classification; and (2) provide clear, specific, and unambiguous guidance to users regarding the classification status of information. Congress should also provide the resources that will be necessary for this review.

9. Bolster Mandatory Declassification Review (MDR)

As discussed above, MDR is a valuable process, but it is under-resourced and does not systemically prioritize public-interest considerations. Congress should address these problems in the following ways.

First, Congress should codify MDR and ISCAP (which are currently rooted only in the executive order) and ensure that they are adequately resourced. In doing so, Congress should leave enough flexibility for the president to redesign aspects of the process (including, for instance, the size or composition of ISCAP) to improve its functionality without Congress having to amend the law.

---

[147] E.O. 13526 § 1.9 (2009).
[148] 32 C.F.R. § 2001.16(a).
[149] E.O. 13526 § 1.9(a) (2009).
[150] Info. Sec. Oversight Off., 2019 REPORT TO THE PRESIDENT 7 (Jun. 2020), *available at* https://www.archives.gov/files/isoo/reports/2019-isoo-annual-report.pdf.

Second, Congress should establish a "fast-track" process, similar to FOIA's provision for expedited review, that would apply when there is a "compelling need," defined (as in FOIA) as "urgency to inform the public concerning actual or alleged Federal Government activity."[151]

Third, Congress should specify that members of the public may use MDR to request public-interest declassification of specified documents. Under the executive order, even if information meets the criteria for classification, agency heads and senior agency officials are authorized to declassify the information if they conclude that "the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure."[152] There is no mechanism, however, for members of the public to request such a review, and agencies in the MDR process may declassify information only if it "no longer meets the standards for classification under this order."[153] Congress should provide that MDR requests may be used to trigger a public-interest declassification review and should authorize ISCAP to render final and binding decisions in these cases, reversible only by the president.[154]

10. Adopt a flexible approach to declassification following unauthorized disclosures

The unauthorized public disclosure of classified information does not itself render the information declassified. There may be good reasons to continue the documents' classified status — for instance, if it is unclear whether the leaked information is authentic, or if official acknowledgment of the information would cause tensions with foreign governments. The government's approach, however, has been too rigid.[155] Retaining the information's classified status has the paradoxical result that enemies of the United States are able to access, share, and make use of the information more freely than U.S. officials. In addition, it can impede efforts to minimize the harm stemming from disclosure, as government officials cannot publicly disclose mitigating information relating to a still-classified topic.

Congress should require agencies to conduct a declassification review, in which all relevant considerations will be brought to bear, of any information that is the subject of an unauthorized public disclosure. The OCA responsible for classifying the information should be authorized to declassify such information on a discretionary basis if consistent with national security and approved by the agency head or senior agency official.

Conclusion

Overclassification is a longstanding and increasingly urgent problem that threatens the proper functioning of our democracy as well as national security. There are readily available solutions, however, that could make significant inroads into the problem. In theory, many of

[151] 5 U.S.C. § 552(a)(6)(E)(v)(II).
[152] E.O. 13526 § 3.1(d) (2009).
[153] *Id.* § 3.5(c).
[154] Steven Aftergood, Director of the Project on Government Secrecy at the Federation of American Scientists and an expert in classification policy, made a recommendation along these lines in his invited testimony before the Public Interest Declassification Board in 2016. *Modernizing the National Security Classification and Declassification Systems Through the Next Administration's Executive Order* (Dec. 8, 2016) (comments of Steven Aftergood), https://sgp.fas.org/news/2016/12/Aftergood-PIDB.pdf.
[155] The executive order states simply, "Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." E.O. 13526, § 1.1(c) (2009).

these solutions could be implemented by the executive branch — but to date, presidents have shied away from the far-reaching systemic changes that are necessary. Congress can and should fill the gap with legislation to ensure that our nation's true secrets, and only its true secrets, are robustly protected.

Thank you again for this opportunity to testify.