MODERNIZING THE GOVERNMENT’S CLASSIFICATION SYSTEM

HEARING
BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED EIGHTEENTH CONGRESS
FIRST SESSION
MARCH 23, 2023


Printed for the use of the Committee on Homeland Security and Governmental Affairs
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, Chairman
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia
RICHARD BLUMENTHAL, Connecticut

RAND PAUL, Kentucky
RON JOHNSON, Wisconsin
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri
ROGER MARSHALL, Kansas

DAVID M. WEINBERG, Staff Director
ZACHARY I. SCHRAM, Chief Counsel
LENA C. CHANG, Director of Governmental Affairs
EMILY I. MANNA, Professional Staff Member
CARTER A. HIRSCHHORN, Research Assistant
WILLIAM E. HENDERSON III, Minority Staff Director
CHRISTINA N. SALAZAR, Minority Chief Counsel
ANDREW J. HOPKINS, Minority Counsel
LAURA W. KILBRIDE, Chief Clerk
ASHLEY A. GONZALEZ, Hearing Clerk
CONTENTS

Opening statements:
Senator Peters .................................................................................................. 1
Senator Paul ..................................................................................................... 2
Senator Blumenthal ......................................................................................... 16
Senator Marshall .............................................................................................. 18
Senator Hassan ................................................................................................. 21
Senator Lankford .............................................................................................. 23
Senator Johnson ............................................................................................... 26
Prepared statements:
Senator Peters .................................................................................................. 31
Senator Paul ..................................................................................................... 32

WITNESSES

THURSDAY, MARCH 23, 2023

Elizabeth Goitein, Senior Director, Liberty and National Security Program, Brennan Center for Justice ................................................................. 4
Thomas Blanton, Director, National Security Archive, The George Washington University ........................................................................................................ 6
John Fitzpatrick, Former Director, Information Security Oversight ................. 8
Patrick G. Eddington, Senior Fellow, Cato Institute ............................................ 10

ALPHABETICAL LIST OF WITNESSES

Blanton, Thomas:
  Testimony ........................................................................................................ 6
  Prepared statement ......................................................................................... 70
Eddington, Patrick G.:
  Testimony ...................................................................................................... 10
  Prepared statement ......................................................................................... 89
Fitzpatrick, John:
  Testimony ..................................................................................................... 8
  Prepared statement ......................................................................................... 85
Goitein, Elizabeth:
  Testimony .................................................................................................... 4
  Prepared statement ......................................................................................... 35

APPENDIX

National Coalition for History Statement for the Record ................................. 101
OPENING STATEMENT OF SENATOR PETERS

Chairman Peters. Good morning. The Committee will come to order.

Every year, a whopping 50 million new classified documents are created. Classified materials typically fall into one of three categories: confidential, secret, or top secret, based on their perceived sensitivity.

Although there are existing requirements to automatically declassify documents after 25 years, in practice that process is ineffective, and there is currently a backlog of hundreds of millions of pages that are awaiting declassification.

Along with outdated technology, the result is an overburdened classification system that costs taxpayers more than $18 billion a year to maintain.

Experts, both within and outside of the Federal Government, estimate that between 50 and 90 percent of all classified materials could be made public without compromising national security, and that the overclassification of documents reduces transparency and erodes public confidence in the Federal Government.

Today’s hearing is an opportunity for the Committee to hear from experts on how Congress can modernize the classification system to improve efficiency and promote better transparency for the American people.

We will be discussing proposed reforms, including several recommendations from the National Archives’ Public Interest Declassification Board (PIDB), to help streamline our nation’s classification and declassification processes. For example, investing in advanced technology, such as artificial intelligence (AI) and machine

---

1The prepared statement of Senator Peters appears in the Appendix on page 31.
learning, could help agencies better manage classified information, better serve the public, and meet the needs of the future.

Other proposed reforms could help reduce the number of classified materials and levels of classification, establish automated declassification tools, and provide an expedited declassification request process for lawmakers, all of which would improve transparency and ensure Congress and the public can help hold Federal agencies more accountable.

I am interested in pursuing bipartisan legislation to help tackle some of these concerns, and I hope my colleagues will join me in those efforts. I certainly fully appreciate the engagement of Ranking Member Paul and his staff, and believe we can find a bipartisan path forward on these important issues.

I look forward to having a productive discussion with all of you here today so we can begin this process of reform, and I look forward to the answers to our questions.

With that I would like to turn things over to Ranking Member Paul for his opening remarks.

OPENING STATEMENT OF SENATOR PAUL

Senator Paul. Twenty-six years ago, a bipartisan Senate Commission chaired by the late Senator Moynihan warned that excessive government secrecy and overclassification have significant consequences for the national interest. The Commission found that “secrecy is the ultimate mode of regulation . . . for the citizen does not even know that he or she is being regulated.”

What happened in the decades since the Commission recommended Congress reassert its authority and reform the Executive Branch classification system? The problem got even worse.

Executive Branch officials from both political parties continue to arbitrarily overclassify government information to prevent oversight and withhold information from the public. Both parties are guilty of this.

According to the National Archives and Records Administration (NARA), in 2017, over four million Americans with security clearances classified nearly 50 million documents, a system that cost American taxpayers over $18 billion. President Biden’s own Director of National Intelligence (DNI), Avril Haines, acknowledged the overclassification problem on numerous occasions. As Director Haines said in January of this year, “overclassification undermines the basic trust that public has in its government.”

There is no better example of the undermining of public trust than the Federal Government’s continued refusal to share with the American people information about the origins of the Coronavirus Disease 2019 (COVID–19) pandemic.

The Department of Energy (DOE) recently shifted its position on COVID–19’s origins, and joined the Federal Bureau of Investigation (FBI) in concluding that the pandemic was most likely the result of a lab leak. The FBI Director later publicly confirmed the FBI’s position that the pandemic most likely originated in a lab.

If not for transparency, if not for whistleblowing, if not for the media getting ahold of this information, it would still be classified.

1The prepared statement of Senator Paul appears in the Appendix on page 32.
Do you realize how crazy it is that they have a classified a conclusion, not the source, not even the data. They have classified the conclusion. They were not even telling us that the FBI and the DOE had come to this conclusion.

Recently, Congress showed strong, bipartisan support for the need for transparency on the origins of COVID–19 by unanimously passing a bill requiring the Director of the National Intelligence to declassify information from the Wuhan Institute of Virology (WIV) and the origins of COVID–19. I am glad that President Biden signed the bill into law earlier this week.

However, President Biden only committed to declassifying and sharing information “consistent with [his] constitutional authority to protect against the disclosure of information that would harm national security.” That sounds good, but it also might be an excuse for not declassifying a lot of information. Given the Administration’s track record on transparency, I am concerned that the President’s statement suggests he will not publicly release all the information that exists.

It is not just classified information the Executive Branch is withholding from the American people on COVID origins. Most of what I have asked for is unclassified and they are still resisting. Nearly a dozen Federal agencies, including the Departments of Health and Human Services (HHS), State Department, Defense Department (DOD), and the FBI refuse to disclose thousands of records in their possession relevant to the origins of COVID–19. Many of these records are not even classified.

I sent dozens of letters for over two years to Federal agencies requesting these records, only to be stonewalled. In fact, recently disclosed emails made available by the Freedom of Information Act (FOIA) actually show Defense Threat Reduction Agency (DTRA) employees, in private emails, were scheming to obstruct my request, mentioning me by name, and saying, “We are not going to give any information to this guy.”

The American people deserve transparency and accountability. If we are being asked to sacrifice those values in the name of “national security,” that definition should be narrowly tailored to protect only what is necessary to preserve our sources and methods.

In the Pentagon Papers case, Justice Potter Stewart remarked upon the wisdom of avoiding secrecy for its own sake. In his concurring opinion, Justice Stewart wrote, “When everything is classified, then nothing is classified. The system becomes one to be disregarded by the cynical or the careless and to be manipulated by those intent on self-protection or self-promotion.”

I want to thank our consensus witness panel for being here today. My hope is, Mr. Chairman, that we have a unique to address overclassification by the Executive Branch in a bipartisan way. I think any reform, though, has to be us taking back some power. If we leave it up to “Please, Executive Branch, please give us information,” it will not work. There has to be a hammer and we have to take back some of the power that originally was ours. We have let it drift away from us and we have to grab back that congressional authority.

Thank you.

Chairman Peters. Thank you, Senator Paul.
It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses, so if each of you would please stand and raise your right hand.

Do you swear that the testimony that you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. Goitein. I do.
Mr. Blanton. I do.
Mr. Fitzpatrick. I do.
Mr. Eddington. I do.
Chairman Peters. Thank you. You may be seated.

Our first witness is Elizabeth Goitein. Ms. Goitein is the Senior Director of the Brennan Center for Justice Liberty and National Security Program, and is regarded as a national expert in government transparency, Presidential emergency powers, and government surveillance.

Previously, Ms. Goitein worked as a Counsel to former Senator Russ Feingold and practiced as a trial attorney in the Federal Programs Bench of the Civil Division of the Department of Justice (DOJ).

Welcome to the Committee. You may proceed with your opening remarks.

TESTIMONY OF ELIZABETH GOITEIN, SENIOR DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM, BRENNAN CENTER FOR JUSTICE

Ms. Goitein. Chairman Peters, Ranking Member Paul, and Members of the Committee, thank you for inviting me here today to testify.

Overclassification is a fact, not a theory. Insiders have estimated that 50 to 90 percent of classified information could safely be made public, as you said, Chairman, and the current system for declassification has no hope of keeping pace with the petabytes of classified information that agencies generate each year.

The harms that result from this State of Affairs are every bit as real and as serious as those that can result from the unauthorized disclosure of sensitive information. Overclassification throws a wrench into the workings of democracy, it prevents the American people from weighing in on matters that affect their rights and their security, it undermines the rule of law by providing a shield for government misconduct, and it impedes oversight by Congress and the courts.

Overclassification also harms national security. It limits the sharing of threat information, both within and outside government. It also causes officials to lose respect for the system. That, combined with the sheer volume of classified information can lead busy officials to cut corners or simply make mistakes when it comes to the protection of classified information.

The causes of overclassification are easy to identify. There are multiple incentives unrelated to national security to keep information secret. Classifying by rote is easier and faster than giving careful thought to every decision. Classification can be a key weap-

---

1The prepared statement of Ms. Goitein appears in the Appendix on page 35.
on interface between agencies. It can be used to hide government conduct that is illegal, embarrassing, or just controversial. Perhaps above all, officials face harsh penalties for failing to protect sensitive information, but no official has ever faced serious consequences for overclassifying.

Solving this set of problems will require fundamental changes to the current system. Although classification policy is usually set by Executive Order (EO), Presidents have historically been reluctant to take the bold steps that are needed. That is why Congress should consider stepping in. The U.S. Constitution gives Congress shared power with the President over national security matters, and Congress has passed many laws regarding the handling of national security information.

Congress, thus, has ample authority to enact the measures we will be discussing today. Chief among these is the development and implementation of advanced technologies to facilitate declassification and derivative classification, namely applying markings to information that has already been designated as classified. There is broad consensus among experts that we cannot and will not solve the system’s problems without the help of technology. Pilot projects have shown that the use of machine learning and artificial intelligence to identify classified information and information that is subject to declassification has tremendous promise, but getting this off the ground will require leadership and resources. Congress can ensure that we have both.

Congress should also direct the President to convene a committee of senior agency officials tasked with narrowing the criteria for classification. Original classification authorities must be able to exercise discretion, but that discretion should not be unbounded. The criteria set forth in the current Executive Order are too broad to provide meaningful constraints.

In addition, pending the deployment of technological tools for declassification, Congress should authorize the National Declassification Center (NDC) to declassify documents at 25 years, without lengthy review by multiple agencies. This multi-agency review is inconsistent with the automatic declassification required by the Executive Order, and it has brought the system to its knees, producing long delays and massive backlogs that will continue to balloon as agencies generate more and more classified information.

Finally, Congress should build accountability into the system. It should direct agencies to implement systems to identify and hold accountable those officials who knowingly, willfully, or negligently overclassify. The designation of classified information, proper designation, should be part of the performance evaluations of all officials who handle classified information, and agencies should be required to implement spot audits, which will help to foster a culture of accountability.

My written testimony includes some other recommendations but I will stop there for now. Thank you again for this opportunity, and I look forward to your questions.

Chairman PETERS. Ms. Goitein, thank you. Thank you for your testimony.

Our next witness is Thomas Blanton. Mr. Blanton is the Director of the National Security Archive at George Washington University
The prepared statement of Mr. Blanton appears in the Appendix on page 70. In his role he has conducted numerous investigations and published reports, books, and articles related to government transparency. Mr. Blanton led the National Security Archive to be the top nonprofit user of the Freedom of Information Act, and the Archive has made more than 60,000 FOIA requests to the Federal Government.

Welcome to the Committee. You may begin with your opening remarks.

TESTIMONY OF THOMAS BLANTON,1 DIRECTOR, NATIONAL SECURITY ARCHIVE, THE GEORGE WASHINGTON UNIVERSITY

Mr. BLANTON. Thank you very much, Mr. Chairman, Ranking Member Paul and other Members of the Committee. I am here to make five points in five minutes: overclassification is out of control; declassification has collapsed; core functions of the National Archives that could help have been flatlined, budget-wise, for nearly 30 years, five different Presidents; key reform tools needed by this Congress and by the public are shriveling at the National Archives; and the key potential reform that could modernize the system is putting sunsets on secrets, on the front end, to force better thinking, and on the back end, to have automatic release. Those are my five core points.

I will not belabor the first one, Chairman Peters, Ranking Member Paul. Liza all made the case on overclassification. I do not need to go much further except to say one thing: I applaud that COVID origins bill but it has a giant hole that the intelligence community (IC) is going to run right through because the last phrase of it says we leave it up to the Executive on sources and methods. Congress can do a different standard on sources and methods. They did it in the John F. Kennedy (JFK) Assassination Records Review Board. They said you have to show harm and you have to weigh a cost and benefit between public benefit, congressional interest, public interest, and the damage done to any source and methods, but a flat sources and methods protection, which is built into so many statutes, is one of the main drivers of the overclassification crisis.

Declassification has collapsed. Last year, I filed a Freedom of Information request with the George W. Bush Library, for one meeting the President had with a bunch of outside experts, none of them with security clearances, to prep for his first meeting with Vladimir Putin. They wrote back, “Oh, we found 1,600 pages of classified documents on this meeting with uncleared outsiders. By the way, it is going to take us 12 years to get that into the queue at the National Declassification Center. So 20-year-old documents and 12 more years to wait, that is the core argument I would make. You have to have an automatic sunset or I will never see those documents.

Third, core functions of the National Archives have flatlined. We did an audit on the budgets. There are a lot of different ways to measure this, but we tried to take a consistent one over 30 years, and we see that five Presidents, the Congress, and the leadership of the Archives have flatlined the budget, literally, despite an exponential increase in the records that the National Archives is re-

---

1The prepared statement of Mr. Blanton appears in the Appendix on page 70.
sponsible for. Bush 41 left 80 gigabytes of records to the National Archives. Donald Trump left 250 terabytes. Meanwhile, the amount of money National Archives has to deal with that has been flatlined in real dollar terms, and that is starting—my fourth point—they key reform pieces of the National Archives that make a difference.

This gentleman was the head of the Information Security Oversight Office (ISOO). It is the best investment that Congress could make, is to give that office the resources it needs to be the inside watchdog on the secrecy system. That office staffs the Public Interest Declassification Board. That could be your go-to place. When you have a dispute with agencies on classified records, take them to that board for an objective judgment. But without staffing, without its own budget, without terms that continue until a new appointee is named, that board is withering away.

The Interagency Security Classification Appeals Panel (ISCAP)—is the best single secrecy forum. It came out of the 1990s. We got to appeal to this interagency group of bureaucrats when an agency stiffed us, and that panel ruled for us 75 percent of the time. That is a measure of the overclassification from the insiders. What they proved, that panel proved, was you take the decision out of the cold, dead hands of the originating agencies and you get some rationality. Right? Seventy-five percent was released.

But that panel has withered away. Its success became its doom. It is overloaded with requests, a backlog of 1,317 cases. I am sorry. It does not work. Got to have more resources. Got to have the Information Security Oversight Office pushing it.

The last, but not least, the National Declassification Center, it does not work. The original idea was that was going to be that interagency panel writ large. It was going to have the authority to declassify. All the agencies would send their people to that center, to sit at the same table and make decisions together. It does not work. Huge backlogs.

A recent quote from a former employee, “The National Declass Center is afraid of its own shadow. It does not have the power to push the agencies around so the agencies push it around.” Congress can change that and make a difference.

The last point, in my last 20 seconds, sunsets, sunsets on secrets. On the front end, to force original classifiers to establish a date. When does the risk diminish? When does it start to go away? We have had a test on that, this 10-year-or-less rule. I think it worked. We have not seen it in historic records, but it could work. On the back end it is only way to get rid of that enormous backlog of hundreds of millions of records.

I will leave it there, and in the questions I hope I can tell you about the machine learning experiment I ran yesterday, inspired by Liza’s optimism about how computers are going to make a difference, and we will come back to that. But thank you very much for your attention.

Chairman Peters. Thank you, Mr. Blanton.

The next witness is John Fitzpatrick. Mr. Fitzpatrick serves as the former Director of the Information Security Oversight Office, the office within the National Archives and Records Administration that leads efforts to standardize and assess our nation’s efforts to manage many aspects of the classification system. Mr. Fitzpatrick
has extensive experience within the Federal Government, including leadership positions dealing with classification policy. Previously, Mr. Fitzpatrick worked at the National Security Council (NSC) where he chaired the Interagency Security Classification Appeals Panel and the Records Access and Information Security Policy Coordination Committee.

Mr. Fitzpatrick, welcome to the Committee. You may proceed with your opening remarks.

TESTIMONY OF JOHN FITZPATRICK, FORMER DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

Mr. FITZPATRICK. Thank you, Chairman Peters, Ranking Member Paul, and Members of the Committee. I am grateful for the opportunity to discuss the changes needed to modernize the government’s classification system.

As noted, I served in the U.S. Government for 35 years, all of it in national security and intelligence, retiring in 2019, the last dozen or so of those years at the Office of the Director of National Intelligence (ODNI), as Director of ISOO, and on the National Security Council staffs of the Obama and Trump administrations, were concerned for the security and classification policies of the U.S. Government and their implementation.

As demonstrated already, there is no shortage of opportunity for change and improvement in the government’s classification enterprise. I wish to make clear I believe the possibility for change and improvement of the system is real. I emphasize how congressional action, and specifically this Committee’s role, is urgently needed to send the demand signal for that change.

I draw an analogy to the role of the Intelligence Reform and Terrorism Prevention Act (IRTPA), of 2004, that it played in instigating improvements to the security clearance process across government. That law, and this Committee’s role in overseeing its implemented, presented a clear mandate for change. It required the President to designated a single official as responsible for driving that change, and established strict performance measures and reporting timelines. I played a role in designing the approach and implementing the structure put in place to respond to those IRTPA requirements, and witnessed the necessity of having both the congressional mandate and the single Presidential designee to drive change.

Any successful effort to modernize the classification system will require the concerted efforts of top administration functions to formulate and drive change. Specifically, the Office of Management and Budget (OMB) and NSC focus and drive will be required to sustain collective reform efforts among departments and agencies. I consider it essential that any legislative mandate should require a single responsible official be designated by the President as accountable for the governmentwide effort. Without top-of-government accountability, prospects for progress are few.

As Tom pointed out, another essential element of reform is strengthen ISOO’s position to meet the challenge of significant reform. Specifically, deliberate efforts are required to increase ISOO’s

1The prepared statement of Mr. Fitzpatrick appears in the Appendix on page 85.
prominence within and among the national security departments and agencies, specifically through greater utilization by NSC and OMB, and preferably that Presidential designee.

Increase ISOO’s own resources and ensure it has independent control of same. ISOO’s resources have dwindled over time, and a reform effort such as this would include right-sizing and empowering ISOO to ensure it is able to meet its mission.

Retaining ISOO’s role in administering both the Public Interest Declassification Board and Interagency Security Classification Appeals Panel, and designating the ISOO director to co-lead the development of a technology investment strategy with OMB and the Office of the Federal Chief Information Officer.

As the Committee is aware, the proportions of overclassification are practically immeasurable, and owes to a range of factors including the decades-long under-resourcing of the staffs and programs in place at departments and agencies whose jobs are to consider classification and declassification actions. I believe that the need to invest in technology to support improved classification and declassification is the single most important need in this modernization effort. The success of reform will depend on the creation of capabilities in the existing and future information environments across government. They must utilize emerging and maturing technologies such as artificial intelligence and machine learning to facilitate the review of classified current holdings, to engage classification decisions at the time of document creation with the intent of thwarting overclassification, and to suggest new ways to process digital records and alleviate future backlogs before they are built.

I do not portray these observations about the poverties of the current system nor the criticality of technological investment as in any way new, and as the board is already aware, I also commend the work of the Public Interest Declassification Board, what it has done to present a menu of opportunities to achieve strategy change. A prominent and fortified governance structure could use these ideas to guide the application of new technological capabilities to achieve reform.

I will close by thanking the Committee for its efforts and to bring attention and drive action to these needed reforms, and I welcome your questions. Thank you.
TESTIMONY OF PATRICK G. EDDINGTON, ¹ SENIOR FELLOW, CATO INSTITUTE

Mr. EDDINGTON. Mr. Chairman, thank you very much. Dr. Paul, Members of the Committee, my sincere thanks for inviting me to be here today with some old friends and hopefully some new ones as well, to offer my views on this absolutely critical issue of over-classification by the Executive Branch. Let me state at the outset that the views that I express here today are strictly my own and do not necessarily represent the views of the Cato Institute, its management, or its Board of Directors.

I got my first Secret clearance as a young armor officer in 1986, followed a Top Secret/Special Compartmented Information (TS/SCI) clearance for nearly nine years, as a CIA analyst, as the Chairman mentioned, and then a Top Secret clearance as a House staffer for over 10 years. I understand our classification system and its pitfalls very well.

In my longer prepared statement I provide the Committee with some key historical background on how we got to this point, some of which you have already heard from some of my fellow panelists today—how our government creates and fails to release, in a timely way, literally millions of pages of Federal records. You will also find in that statement a lengthy list of examples where Executive Branch secrecy has been used to hide major unconstitutional intelligence programs as well as the failures of those programs and others actually authorized under the Patriot Act.

Because the Congress has before it the pending business of whether to reauthorize or let die Foreign Intelligence Surveillance Act (FISA) Section 702, I want to use my remaining time to offer this warning.

When The New York Times exposed then President George W. Bush’s illegal Stellar Wind electronic mass surveillance program in December 2005, he and his key advisors assured the Nation that the program was both necessary and effective. In fact, it was neither, something we only learned from still more New York Times reporting that surfaced, and only through Federal Freedom of Information Act lawsuits, I will add, intelligence community inspector general (IG) reports that revealed clearly that Stellar Wind was an ineffective program and one that collected data on Americans with no connections to terrorist groups or hostile foreign intelligence services.

On June 6th it will be 10 years since the Guardian newspaper published National Security Agency (NSA) whistleblower Edward Snowden’s first major revelation—the Federal Government’s programmatic collection of telephone metadata on virtually every American. The program made a mockery, and I use that word advisedly, a mockery of the Fourth Amendment’s individualized, particularized, probable cause-based warrant requirement.

The Patriot Act’s Section 215 telephone metadata program was also a failure, something former Senate Judiciary Committee Chairman Patrick Leahy demonstrated in a 2013 oversight hearing in which after less than five minutes of cross-examination, the Chairman got then-NSA Deputy Director John English to admit

¹The prepared statement of Mr. Eddington appears in the Appendix on page 89.
that contrary to previous NSA claims, that 54 terrorist plots on America had been stopped by that Section 215 program. The actual number was zero. It would not be until 2019 that NSA would finally kill that failed program.

The Executive Branch’s reaction to Snowden’s revelations was to once again prosecute a whistleblower for exposing Federal Government domestic surveillance misconduct. Snowden, Thomas Tamm, The Stellar Wind whistleblower, and former Army Captain Christopher Pyle, who exposed long-running unconstitutional Army domestic surveillance in 1971, to the late Senator Sam Ervin in his Committee, all acted out of a belief that the Federal Government’s classification system was being used in a systematic way to conceal illegal or unconstitutional acts. They developed a contempt for a system that seemed designed to violate Americans’ rights, not protect them.

As an author and historian, I have a keen interest in getting the tens of millions of still-classified or otherwise unreviewed FBI, CIA, NSA, and related agency records into the public domain, and my statement for the record contains a model legislative proposal that I believe would accomplish that end.

But even more fundamental to the preservation of the rights of our citizens is the need for a statutory ban on the misuse of the classification system to conceal waste, fraud, abuse, mismanagement, or violates of statute or provisions of the Constitution. I believe that my proposal would achieve that goal as well.

I thank the Members for their time and attention, and I stand ready to answer your questions.

Chairman Peters. Thank you, Mr. Eddington.

Mr. Fitzpatrick, in your testimony you discuss the exponential increase in digital classified information, and all our panelists have concurred with that. I am always struck by the fact we are seeing an estimated 50 million new classified records each year. It is really hard to wrap your mind around the sheer volume of that. Most of all, these records are now electronic, not pieces of paper like think about the rules that existed not too long ago.

If you could tell the Committee, what are some of the major challenges that we face in managing classified information that is digital, specifically?

Mr. Fitzpatrick. Thank you for the question. One of the reasons those numbers are so high is because, in the post-9/11 era and just with the development of new technology and network technology in general, we have proliferated secret and top secret information networks to support the activities of a larger national security and homeland security portion of government, and the industrial base that participates in it.

There are simply more ways and more direct ways for the 4.5 million people that have a security clearance to create a classified record, and the template for every one of them on those networks says what is the classification level, and it provides a tool to assist in choosing to classify that record. It does not say “does this need to be classified? Yes, no. What harm would come from this?” It is simply a digital recitation of whatever the other document was. An email that comes to you already classified and I reply, I add no additional classified information to it, that email is also marked as
classified. In the counts that ISOO attempts to do with some accuracy, they get harder and harder to do because you have created, proliferated digital classified items.

That infrastructure and the culture that the users across government live in is one of protection. Your job is not to release this information. Your job is to protect this information. There is a one-way incentive structure in place.

There is a culture change needed that can only come from the top, that can only be reinforced by policy, practice, tools, and training. I commend the activities of DNI Haines and others in government who have begun to utilize the release of current classified information to influence the decisions that are made in national security and operational contexts such as we have seen in the run-up to Ukraine and in dealing with China as a rising power. That is a signal that it is a possible thing to consider, but it is only at the highest level that people are granted the privilege to think that way, and we have to figure out a way to train people and support the change in behavior that they can actually question, “Does this really need to be classified?”

I cannot tell you how many emails I received back in the day, when I was living every day in classified, “Hey, do you want to go to lunch?” and somebody has a default classifier. That is emblematic, I think, of the challenge and the drivers for it.

Chairman Peters. This Committee will look at all the different drivers that are involved, but I just want to ask specifically about one that you mentioned, Ms. Goitein mentioned as well, artificial intelligence and machine learning, something this Committee is investigating. We had a hearing last week about the promises of artificial learning but also the concerns and the challenges associated with it, and we have to think that through. You mentioned in your testimony how machine learning and artificial intelligence gives us a tool to manage a massive amount of data, which we know that is appropriate to be thinking about.

But tell the Committee not just the opportunities but talk to us about the pitfalls of using artificial intelligence and machine learning to deal with this issue.

Mr. Fitzpatrick. I think the greatest concern would be where decision rights lay on the product that the AI puts forth, to whether or not that would require review. If we have petabytes of data to search through to find the needle that is of the public interest, and then to have it considered as a needle found and not thinking about the whole haystack, I think that is ultimately a decision that rests with a human. But it has been served up through a process that is trusted and, demonstrably so in the technological ways, to then say here are the few needles that you need to think about and the argument to protect or not protect can be judged based on that.

Chairman Peters. Thank you. We will come back to you a little later. I want to get Ms. Goitein in here.

You talked about the classification or declassification process after 25 years and mentioned why we have a backlog that is not working effectively, in your opening comments. But I would like you to drill down more. Give us some specifics as to why that is failing and things that this Committee should consider changing,
and maybe not just having a flat 25 years or perhaps just enforcing that. I would love your thoughts.

Ms. GOTTIEIN. Absolutely. As I mentioned, the Executive Order says that all information of permanent historic value must be automatically declassified at years whether or not has been reviewed, and that is a quote. But in practice, a lot of the documents do not even get to the National Archives. They are not even accessioned until the agencies have performed their own manual review—nothing automatic about it—and there are nine categories of information that are exempt from automatic declassification. In theory, that is what they are looking for.

They are also looking to see if other agencies might have equities in those documents, and then they will send the documents to those other agencies. That often happens sequentially, which adds a lot of time. Some of these nine exemptions, if you add them all together they cover a lot of ground, probably too much ground, and some of them are worded extremely broadly, so they give the agencies a lot of discretion. If the agencies find a single word that needs to remain classified that is exempt, that will withhold the entire document rather than simply redacting that word. That is called a “pass-fail approach.”

In addition, there is a statute, the Kyl-Lott Amendment is what it is called, that requires agencies to do a line-by-line review of these documents unless they can certify that the documents are highly unlikely to contain any nuclear information. These agencies are extremely risk averse. They are not going to designate large categories of information as being highly unlikely.

The combination of this sequential, lengthy, manual review with a pass-fail approach with the Kyl-Lott Amendment means not only that this process takes years and years, but also that an extremely unimpressive percentage of documents come out the other side of this process declassified. Roughly half of documents that are reviewed end up being declassified, and there is a backlog of about 600 million pages of documents that have not even been reviewed. That is what automatic declassification looks like today.

Chairman PETERS. Great. Six hundred million pages, line by line.

Ms. GOTTIEIN. That is a lot of work.

Chairman PETERS. Yes. Good luck. So definitely we need reforms.

Ranking Member Paul, you are recognized for your questions.

Senator PAUL. This is a great panel today. We rarely have an issue where both sides seem to agree on it. I think one suggestion would be if we were to do a bipartisan bill trying to fix this problem that we constitute a working group, including the four members who have testified here today, since they probably have more experience in this issue than any Members of Congress, any Senators or any of our staff. If we had a working committee with these four and a few others, I think we would avoid the pitfall of having good intentions and then passing something that does not work, which is a pretty common occurrence in government.

I think there are a lot of reasons why it does not work. One of the fundamental things is the separation of power. In almost everything that we ever do here, where we give an exemption to the Executive to allow them to have the unilateral power they use it. It is well intended. We say, “You have to do this unless national secu-
rity superimposes,” but they always use that and they will always have the incentive to use it.

We either have to have congressional power over funding or some sort of independent agency. I almost would imagine sort of like a Federal judge or somebody that has judicial experience to sort of review these but has the power to make the decision. If the Executive makes the decision it has to be appealed by Congress, Congress has to somehow be able to override, or somebody has to be able to override the Presidential decision.

Then the question I had for Mr. Blanton was, you mentioned there was a committee that was working that was reviewing this. Was this just old documents, over 25 years, or was this more recent documents? You mentioned some oversight committee that seemed to be working that was now backlogged.

Mr. BLANTON. The Interagency Security Classification Appeals Panel.

Senator PAUL. ISCAP. OK.

Mr. BLANTON. Because it rules for the requestor. It got totally backlogged because it actually started ruling for the requestor.

Senator PAUL. Was it old, over 25 years, or newer?

Mr. BLANTON. Mandatory declassification review, so it can be new or old. New or old.

Senator PAUL. OK. It worked at first but now it is overwhelmed because they have too much staff.

Mr. BLANTON. Because the agencies did not take those decisions and plug them back into the classification guides. There was no learning. We had to fight those battles over and over, the same battles.

Senator PAUL. That could be part of the reform legislation——

Mr. BLANTON. Exactly.

Senator PAUL [continuing]. Is making sure that those decisions become a precedent for another decision, another similar decision.

Mr. BLANTON. Exactly. I just point back to your reference to the Moynihan Commission. The title of that commission was Protecting and Reducing Government Secrets. It sounds like a contradiction. It is not. If you protect the real secrets you have to disgorge the non-secrets.

Senator PAUL. I have been to hundreds of classified hearings and never heard anything classified, and most of the important stuff is already in the newspaper, and I read about it in the newspaper, and some of it is ridiculous. The idea that the FBI and the Department of Energy have concluded that they think this, in all likelihood, came from the lab in Wuhan is not a secret. If you had somebody’s name, that is a secret. I have never been to a hearing where I was told the name of a source or how somebody got something, and really, frankly, I do not want to know it for any possibility of that leaking. There are real secrets that we have but almost nothing that is classified is a real secret.

Ms. Goitein, you mentioned in your written testimony that a wedding ceremony in Dagestan, cables from that were classified, what kind of robes they wore and what they did over this wedding ceremony. That is ridiculous.

But I was told yesterday by the Secretary of State, he will not give me any cables and he will not give me any information that
is unclassified because the Executive Branch has unilaterally decided they will not give information unless the chairman of a committee signs off on it. I have four or five chairmen I am trying to get to sign records releases. They will not give any, but who made this decision? Not Congress. Not the people. They made the decision to protect it.

But this is the problem we have. I want to fix the classified problem, but even the unclassified information they are withholding from us. I want to see like government grants on people who applied for coronavirus research that were rejected and accepted, and the research proposal that involved the lab in Wuhan. I cannot get it because they deny this, and most of it is not supposed to be classified. We have a real problem.

It is even worse than that. Some committee chairmen will say, like the head of Armed Services will say, “We will sign a request for this information but it is not supposed to leave the committee.” There is report that they did in HELP Committee, and I am on both committees, and I wanted to bring it over here because I am the Ranking Member. The HELP Committee is preventing me from bringing that over so Senator Peters can see it. It is crazy the segmentation of the things we do.

But I think the best way to fix it is and I really think it would be a great idea to have a working group of people from the outside that would help us craft the information so we do not have the same pitfalls. What I would hate is we do a rubber stamp of something that looks good, sounds good, and does not work, and it really has to involve all of this.

The reforms, you talked about having them learn from the precedents. Any other reforms, Mr. Eddington, that you would suggest?

Mr. EDDINGTON. An awful lot of what my colleagues have already talked about I think is essential. But I will point to previous success stories. We have talked about a lot of failures here. But things happen when Congress decides they need to happen. This is how we get the JFK records, assassination material, out, the Imperial Japanese war crimes and Nazi war crimes records out. This is stuff coming directly from the Congress.

That is why, in my written statement, I propose a national declassification bill, that would mandate, essentially, that anything that is 25 years older or older shall be essentially presumed to be unclassified, unless there are very specific criteria that are met. Now the criteria that I talk about are drawn from the existing Executive Order 13526. But there are important words that are not in that Executive Order. Liza has pointed to some of them. My favorite word is “current.” That word does not appear in there, so that is what gives NSA and others the ability to hang onto stuff for 50, 75 years, or 100 years. That is the No. 1 thing.

On the issue of congressional prerogatives, let us remember that the word “secret” only appears in the Constitution in one place. It is not Article 2. It is Article 1, Section 5, dealing with this body, Congress. Congress was the original classification authority (OCA). It let that power essentially slip away to the Executive Branch, and in my judgment that is exactly the reason we have a problem.

The last group of your colleagues who I think really understood this well were Senator Church, Senator Tower, and the others on
the Church Committee, because when they were doing their report they made it very clear to President Ford, we are going to listen to you when we tell you what we are going to include in this report, but the final word about what goes into our product, our committee report, that is us. That is Congress.

That is exactly the standard you all need to return to. Do not turn your material, do not turn your reports over to the Executive Branch and let them tell you what is or is not classified. You are the original classification authority and that is in the black-letter text of the Constitution. Thank you, Dr. Paul.

Chairman Peters. Thank you.

Senator Blumenthal, you are recognized for your questions.

OPENING STATEMENT OF SENATOR BLUMENTHAL

Senator Blumenthal. Thanks, Mr. Chairman. Thank you to you and the Ranking Member for having this hearing.

We attend a lot of classified briefings, and I would say at the end of probably more than half of them I say to the briefers, often very high-ranking members at the Pentagon or in the intelligence community, “Our adversaries know we know what you told us.” We know our adversaries know that they know we know. We know they know. They know. The only one who do not know are the American people, and very often it is information that is vital to the American people assessing a threat to our national security. If I began to tell you now what those subjects are I would get in a lot of trouble. Nobody would shoot me, but I would be, in effect, shot on the floor of the U.S. Senate. It would become a major issue—Blumenthal discloses classified briefing.

The real losers here are the American people, not about some historic event 25 years ago but about current threats to our national security, where we could mobilize more support publicly for defense spending, in certain areas, if the American people knew what the ongoing threats are.

I am going to be somewhat adventurous here—the information we get is from aerial surveillance, where companies in the private sector are already producing the information because they have satellites just like our military does. I have seen aerial surveillance of the balloon that went over our country, the Chinese balloon, which traces it back to when it originated, not from the Pentagon but from a private company doing the same kind of aerial surveillance.

The present system is beyond broken. It is actually counter-productive. It promotes secrecy at the expense of our national interests and security simply to prevent sometimes embarrassment to public officials, who would prefer that the public not see what they are doing. We all would love to be the final arbiters of what the public knows about what we are doing, but it does not happen that way in a democracy. I have seen the history here. You go through it in your testimony. Nothing has happened after every one of these commissions. Nothing. None of the Moynihan recommendations adopted.

When we sort of preach here—meaning we on the panel preach, not you—it really is not necessarily a sign that we are going to accomplish something now. But I would like to take some of these
recommendations, for example, from the Moynihan Commission, and propose them in a more comprehensive way rather than piece-meal, in the way that we have adopted doing it. I do not know that it would require another commission.

But I would like to know from you if you were to prioritize five recommendations made by the Moynihan Commission or by one of the other numerous bodies that have made recommendations, what would they be? I know we will not have time necessarily to go into all of your suggestions or recommendations, but it would be helpful, I think, to get the five things, taking Senator Paul's apt remark that the experts are here. You do not need to form a commission with you folks on it, but something really ought to be done, and the American people want an end to this secrecy for all the reasons that have been stated in a very forceful, bipartisan way.

I am happy to begin going down the line. We will run out of time, and so your written responses, I think, would be very helpful.

Ms. Gottein. I will try to be quick because I know all of us are going to have ideas, and I was looking at the list that I had the summary of the recommendations that I made in my written testimony and I had basically 10 sets of recommendations. I was choosing the top five.

But certainly I think we need to start with technology development and implementation of advanced technologies. You are not going to find that in some of the older commissions' reports, but it is key to the success of the system now. I mentioned in my oral remarks that we should have a White House-led task force to narrow the criteria for classification, that we should require agencies to have accountability systems for overclassification. I think that is very important. There are other ways, as well, to rebalance the incentives that I mentioned in my written testimony.

Then reforming automatic declassification by empowering the National Declassification Center to declassify documents without lengthy agency review, but also to include what is called a "drop dead date." This is what Tom was speaking about earlier. It is a sunset, which is a period of time after which documents would simply cease to be classified. They would not have to be declassified.

Then the last one is that I think Congress should amend the provision of the National Security Act that talks about protecting against the unauthorized disclosure of sources and methods, because that provision has been misconstrued to allow and even require the withholding of sources and methods regardless of whether their disclosure would actually harm national security.

Those are my top five.

Mr. Blanton. I totally agree, and I could stop there, but I would add the top recommendation of the Moynihan-Helms-Combust Commission was for Congress to pass a statute to authorize the classification system and take that away from the Executive Orders that just make a mish-mash of the whole thing, a statute. Then in that statute, the core principles of that statute need to be what Liza just said, that any withholding of any kind, not just classified area but in the unclassified areas that Senator Paul is talking about, Executive should have to identify the harm from release and have a balance test against the benefit from release—cost-benefit analysis, harm test.
To come back to my own testimony, sunsets on the front end will compel better thinking by the original classifiers, because they have to make a risk assessment that right now is just a drop-down menu. Oh, want to go to lunch? Oh, is that secret or confidential? That is all it is. It is as reflexive as the old days when it was a rubber stamp, except it is a drop-down menu.

A statute and then those balancing pieces on the front end and on the back end, I think that is the core.

Mr. FITZPATRICK. Very briefly, I would suggest attention to one of the recommendations the PIDB made in an earlier report around prioritization. While we are working on capabilities that can deal with data and paper and digits in the aggregate, something needs to be done now, or one thing that can be done now is for the Congress to use its voice to indicate what the public interest, in the ways that Patrick was talking about with the JFK assassination records. It does not have to be an as auspicious and historical event as that, but if there is one that has not been addressed, put that out there as a priority for the NDC and the agencies to work on, to show a good outcome for the classification system. Prioritization is a difficult challenge, but I think a necessary one for separating the wheat from the chaff that is in the 600 million pages of unreviewed documents and other big piles. Thank you.

Mr. EDDINGTON. In my written statement, Senator Blumenthal, I have essentially model legislation that would do an awful lot of what Tom and Liza are talking about. I agree with Dr. Paul. If you put the four of us in a room over a weekend we could probably give you a pretty nearly finished version of what you might want to take a look at. I will leave it there.

Chairman PETERS. We will be continuing to work—we are working with all of you so far, and we are going to continue to work with you so we get something done. We will make sure that happens.

I need to step away for another committee hearing briefly, to ask some questions downstairs. Ranking Member Paul will take the gavel until I return.


OPENING STATEMENT OF SENATOR MARSHALL

Senator MARSHALL. Thank you, Mr. Chairman, Ranking Member. I do sincerely appreciate holding this hearing.

As Senators we all take an oath to defend the Constitution, and what I have seen as Senator that not only am I not allowed to see much of the information we need, whether it is classified or unclassified, but certainly America does not. Whenever we allow the Federal Government to live in darkness, it is a threat to our Constitution and a threat to our republic. I way underestimated how important this transparency issue is and how we are all more accountable when things are out in the open.

Certainly I am a frustrated Senator right now, and want to do what we can do—it seems like the de facto position is to classify things as opposed to the de facto position of let Americans see it.

My first question is for Mr. Fitzpatrick. Under President Clinton, it took a year for the NSC senior director to basically update this overclassification issue. I do not mean to make you defensive. I am
sure you wanted to do something as well. You had four years to make an impact on this. You had committees and meetings. What progress did you make? But more importantly, what were the obstacles for you to update the classification system?

Mr. FITZPATRICK. I served in the last year of the Obama NSC and two and half-ish years of the Trump NSC. The Obama NSC, my time there, that was that administration's Executive Order 13526. It was the State of the order that that administration wanted, and so it was not a priority to conduct another policy review on an Executive Order it had issued. Which is not to say it did not revise—any administration does not revise its own orders. That was not a priority. In fact, my timing coming into the administration was focused on wrapping things up for that administration and the transition to the next.

It was also not established as a policy priority in the Trump administration. The attention for my office, which came down through the chief of staff there, did not prioritize that work.

I point this out explicitly, and point back to my testimony which suggests that it will take an external force or a congressional mandate to establish a requirement that the President prioritize this work and report back on specific milestones and outcomes. That example worked, and I used the security clearance reform and example in my testimony. I often refer to the security clearance reform problem as the No. 1, second tier national security issue in government, and knowing that the national security community never gets out of tier one.

Overclassification, my opinion and estimate, is a tier three issue. It is a peripheral activity in government. Without somebody taking that and putting it at the center and within the focus of leadership——

Senator MARSHALL. Is it a priority for this Administration, do you think?

Mr. FITZPATRICK. I am not able to speak for this Administration. I am familiar that they have issued some guidance to agencies to bring ideas forth but I am not familiar with the status of those.

Senator MARSHALL. Mr. Blanton, my next question is for you. Would a two-tiered classification system work better than the current three? If so, would you force agencies to move all information currently classified as Confidential down to Unclassified or Unclassified for Official Use Only (OUO), as opposed to raising it to Secret? Would that diminish overclassification?

Mr. BLANTON. That is a great question, Senator. My view is we have to disgorge the confidential level material, not just change the label on it. It goes back to something I mentioned to Chairman Peters at the very beginning. Yesterday, inspired by Liza’s optimistic belief in machine learning, I asked Chat Generative Pre-Trained Transformer (ChatGPT) your question—how should we modernize this nation’s information security system.

Senator MARSHALL. I have been waiting for this.

Mr. BLANTON. Let me tell you, answer No. 1, this system is way too simple. It does not even begin to comprehend the multiple threats that we face, such as in cyber, that a limited number of labels. We need more of them. Then it ended with an error message.
We tasked it again. The second time ChatGPT says no, the problem with the security classification system is there are three levels of secrecy. There should only be two, Secret and Top Secret. Did not get an error message after that.

Senator MARSHALL. This system agrees with Senator Marshall, it sounds like. All right.

Mr. BLANTON. The problem there is just simply the bureaucratic imperative that we have all heard about.

Senator MARSHALL. Thank you so much. I am going to go back to Mr. Fitzpatrick. Why is ISOO been so ineffective overseeing the classification system and holding agencies accountable for over-classification?

Mr. FITZPATRICK. I think it is challenged on a resource basis. In order to actually oversee the activities of the classification system it is necessary to measure them, which ISOO does, but it is also necessary to go and visit agencies and conduct inspections and see exactly how the numbers that come back in reports are arrived at by the agencies. The staffing levels of ISOO have been reduced to a point where it cannot do that effectively.

Senator MARSHALL. OK. Yes, my next question, I will go back to you, Mr. Fitzpatrick, and others can chime in if they want to. How can we ensure that the United States government releases all the JFK records in our lifetime? This seems to be the bar that America—if this is shrouded in secrecy, this sad chapter of America’s life, if this is shrouded in secrecy, everything else is as well.

Mr. FITZPATRICK. I suppose a review of those statutory requirements in that law, in light of the releases that have come and the withholding that has resulted from that guidance, might produce a different set of criteria to force the outcome that you state.

Senator MARSHALL. Mr. Eddington, would you add anything?

Mr. EDDINGTON. Senator, you and your colleagues have the power, if necessary, to provide additional funding, if that is a problem. I do not know if that is necessarily the case or not. But if there is any doubt as to whether or not additional information is out there, give them a drop-dead deadline. I think Tom and I have a mind meld, a Vulcan mind meld on this practically. Give them an absolute deadline on this stuff.

I have to say, I am an Article 1 guy. Have the Government Accountability Office (GAO) literally climb all over them and take a look at whether or not they have actually been as thorough as they should have been in looking for documents.

We do not have enough—and Tom has talked about this a lot—we do not have enough back-end checks on this stuff. This is why we have a problem with surveillance in this country. I hate to keep coming back to this. I know this is supposed to be about dealing with the classification system. But there is almost never enough back-end checks on this stuff, and not enough auditing. That is one of the reasons why a lot of time you end up legislating in the dark. You have an opportunity to fix that here if you choose.

Senator MARSHALL. Thank you, Mr. Chairman. Thanks so much to the panel. Great answers.

Senator PAUL. Senator Hassan.
OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Ranking Member Paul, and thanks to all of our witnesses for being here today.

I want to start with a question to Ms. Goitein, please. Government’s top priority is to keep its citizens safe, secure, and free. Classifying certain information is important to protecting national security such as intelligence sources and methods, to be sure, but this Committee has also heard from experts in the public and private sectors about the challenges with information sharing between government agencies and critical infrastructure owners and operators. When we think about cyber in particular right now, what I hear from the private sector is, “We cannot get any information that would help us do what we need to do to keep safe.” It is information sharing necessary to help prevent terrorist attacks, combat cyber threats, and more.

In your experience, Ms. Goitein, how have you seen overclassification inhibit information sharing that is critical to public safety and security?

Ms. Goitein. Thank you for that question. I think it is a major problem, and in fact, the 9/11 Commission talked about overclassification and how overclassification had actually stood in the way of sharing information among intelligence agencies that could have helped to prevent the attacks. We paid a heavy price, possibly, for overclassifying information.

What the 9/11 Commission pointed to was a culture of secrecy that is a relic of a Cold War, and that culture, which pervades a lot of the agencies we are talking about, is rooted in assumptions from the Cold War about who the enemy was and what we had to do to protect ourselves against the enemy that no longer hold. As you are pointing out, in today’s threat environment sharing information is often critical to protecting national security. That really is an enormous problem, and it raises its head in all kinds of areas. My written testimony has some other examples of situations where failure to share information has been problematic.

I also, if I could, want to briefly respond to Dr. Marshall’s question about whether this is a priority for this Administration. I did want to point out that the National Security Council last June began an interagency process to look at the Executive Order and the classification system. That process, at least at the time, was given a year. If this Administration comes out with an Executive Order that includes all the reforms we are talking about today in June, that will greatly diminish the need for legislation, although Congress will still need to ensure that there are adequate funds. However, if it appears that no such order is forthcoming in the near future, or in the foreseeable future, or if the order does not have adequate reforms, then again that is the situation where I really think Congress needs to step in to protect democratic accountability, the rule of law, oversight, and as you said, national security.

Senator HASSAN. I appreciate that very much, and that is a good marker for us to look at.

I want to talk to you too, Ms. Goitein, about the financial costs here. I am Chair on the Subcommittee on Emerging Threats and Spending Oversight (ETSO), which is tasked with protecting and
saving taxpayer dollars. Toward that end, I am concerned about ways in which overclassification of Federal documents contributes to waste, fraud, and abuse.

What are the financial consequences of overclassification? Specifically, what factors contribute to those consequences?

Ms. G OITEIN. Overclassification greatly increases the amount of effort and resources that need to be put into protecting the information. It also requires costs to be spent on clearing secure personnel. I think the reason we have over four million people who have security clearance to access classified information is because even people who are performing relatively low-level or non-sensitive tasks actually need a clearance to do their work.

Certainly the systems that are used to process classified information, the physical storage for classified information, all of these cost money. I think we do not even know how much money they cost. The last figure that we have, which is from a few years ago, I think, is $18 billion, but the director of ISOO has flagged, in various ways, that he is not confident in the accuracy of that information. I think it is likely to actually be much more than that.

Of course, we are not talking about the indirect costs, the inefficiencies and the weaknesses in some of the policies that are a result of information not being shared and vetted and improved through transparency and public participation.

Senator HASSAN. Does overclassification allow Federal agencies to hide waste, fraud, and abuse?

Ms. G OITEIN. Absolutely. It is one of the main reasons, I think, why the classification system is misused.

Senator HASSAN. I want to follow up with you on that, but I want to get to a couple more questions. A question to Mr. Fitzpatrick. The backlog of government documents that are overdue for declassification is large, as you have noted, and likely too big to be addressed by human review alone, as we were just talking about.

You touched on this already with Senator Peters and with Senator Marshall, but we have talked about technology solutions that can assist Federal workers in addressing the backlog without jeopardizing ongoing security matters. Based on your experience in the Federal Government, which Federal agency should lead or be involved in developing these technology solutions?

Mr. FITZPATRICK. Thank you for the question. It is incredibly important. I believe that the information technology budget of the U.S. Government is already spending dollars on artificial intelligence and machine learning. One of the challenges here is to take the solutions that are being built for other purposes and apply them to this problem. It would take somebody at the Federal Chief Information Officer (CIO) level, and my recommendation, guided by an ISOO director that is charged with the responsibility to say, “Listen to these agencies. They are starved of these resources. If they had them, here is what they would do.”

The ideas are there, the technology application is, I think, the key thing, and it has to happen from the OMB budget level.

Senator HASSAN. OK. Thank you.

One last quick question to Ms. Goitein. You testified that the Federal Government’s current incentive and penalty structure encourages individuals to err on the side of overclassifying informa-
tion rather than declassifying information. At the same time, classification obviously is essential to protecting national security.

How do you recommend striking the right balance between reducing incentives to overclassify while protecting our national security?

Ms. GOITÉIN. I think we would have to go a long way in the other direction before we had to worry that we were making it too easy for people to not classify information. I think there is a lot of room to work with.

I do think, absolutely, there need to be administrative penalties for mishandling classified information, failing to protect classified information, in cases where it is quite clear that that information required protection.

But one thing that I think does need to be done is to provide a safe harbor for officials who make good-faith decisions not to classify or not to mark information in situations where the classification status of that information truly is ambiguous. Right now I do not think officials feel free to exercise their judgment, their reasonable judgment, in that direction.

Then on the flip side, as I was saying earlier, we need to have some kind of accountability for people who are misusing the classification system for reasons unrelated to national security.

Senator HASSAN. Thank you very much, and thank you, Mr. Chair.

Chairman PETERS [presiding.] Thank you, Senator Hassan.

Senator Lankford, you are recognized for your questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Chairman, thank you. Thank you all for bringing your testimony. Really appreciate your engagement. I was able to sit in earlier and be able to hear your oral statements, as I am back and forth in multiple hearings today. I appreciate your engagement and your thoughtfulness on this.

A quick story. I went to the National Archives several years ago and I said, “Show me something that people do not get to see.” They pulled out a hand-done drawing of Pearl Harbor, and it had X’s on it and markings on it. I said, “What am I looking at?” They said, “This was a radar operator at Pearl Harbor that was tracking the Japanese coming in, and everywhere there is an X is when he radioed in and said to the folks at Pearl, “I am picking up a radio signal.” They signaled back, “It must be people flying in from California.” There were like five X’s and then it stops. They said, “This document was highly classified for decades because it showed we knew the Japanese were coming and missed it, so it stayed classified for decades. Here it is.”

It was interesting dialog and it was also an educational moment for me to be able to hear classification and how it is used historically and how it can still be used today.

My questions are on a couple of things on this. There is a flip side of this. There are covert operations that do happen that protect our national security worldwide, that some of them do last decades, and as long as we have that penetration it stays classified. If we do an automatic declassification in 25 years that can threaten covert operations, but we also have the Pearl Harbor map that it
is just someone trying to cover up their mistake as well, that is out there.

There are multiple layers of classifications. You have Sensitive, you have Classified, you have Top Classified, you have Covert Operations, you have Compartmented, you have all these different pieces here. How do we strike a balance on automatic declassification and still protect covert operations that are still ongoing?

Ready, set, go.

Mr. EDDINGTON. As a CIA guy, why don’t I go first, or former CIA guy. I will go first here.

I wholeheartedly agree with you, Senator Lankford, which is why, in the proposal that I have put forward—and I will just talk about confidential human sources.

Senator LANKFORD. Yes. You have family members that can be exposed. If that person is gone their family is still around.

Mr. EDDINGTON. That is exactly right. In my proposal I am focusing here on current confidential human sources, and by “current” I mean whereby they have provided information on criminal activity, let us say in an FBI or other law enforcement context, or information of a foreign intelligence value within the last five years.

Now, if that is the case, that is going to get extended out for a very long period of time so long as that is an active source. It is possible that we would need to talk about maybe some tweaks to what I have discussed here, but I think that kind of approach that recognizes that when something ends and there is no life at stake, if you will, the information ought to be available in a much more timely way than it is right now.

But I absolutely take your point with respect to covert action, and I want to make sure that obviously we do not go anywhere other than the unclassified here. There are absolutely activities that take place that do stretch literally over decades, and we would want to make sure that those kinds of activities are protected.

That being said, one of the cores of my proposal here involves an absolutely prohibition on using the classification system in any circumstance to hide waste, fraud, abuse, criminal conduct, et cetera. I think you need to have that in place because as Liza has indicated—and I have many examples that I can share with the Committee—the classification system has been repeatedly misused to conceal those very kinds of things. That is my quick take on that. Thank you.

Senator LANKFORD. Yes, ma’am.

Ms. GOITEIN. The solution that I have advocated for declassification involves removing multi-agency equity reviews at the 25-year mark, but not getting rid of the exemption at that point. I have advocated having this steering committee, this working group, led by the White House, narrow those criteria because I think they are too broad, but certainly some of the examples you were giving, those would still be exempt from declassification. We just would not have a multi-year, endless process and these open-ended exemptions that result not enough information being declassified.

Even the drop-dead date that I mentioned, which is further on in time—roughly 40 years is what I put forward—even at that point there would be categories of information that should be exempted. Those would include confidential human sources and key
design concepts of weapons of mass destruction, and there would be an option for agencies to seek case-by-case exceptions beyond those, that could be approved by ISCAP. But the key distinction there, again, is that the information would not have to be declassified. If it did not fall within one of these exceptions that I have mentioned, it would simply cease to be classified, and that is the key there.

These solutions that we are talking about would absolutely preserve the government’s ability to keep secret the very narrow category of information that really does need to still be secret after 25 or 40 years.

Senator LANKFORD. We have had a new designation show up recently on documents that get brought over to our staff. It has “For Official Use Only (FOUO), Law Enforcement Sensitive.” The first time we saw it we were like, “What does that even mean?” This is not something that is in a sensitive compartmented information facility (SCIF). This is just something that appears as a new designation. Magically, there is a new setting, and basically like, we do not want this out so we are going to create a designation for this.

Now we have done what we should do with that. We have ignored that and said, “That is not a real designation on it.” But there is this constant push to say we are not going to be able to get information out and we do not want it released out to the public on it.

We understand the challenge that we are on, dealing with any administration. I do really like the concept of having a place of appeal, basically. I do not know how many documents that we get that are redacted, that the whole page is black, basically, with redactions on it, and we have no place to appeal to go fight for it. Often we end up FOIA-ing the documents, or some outside group does, and they get it and we do not, on it. That is absurd on it. But to have a place of appeal that is set up, what we were talking about before, would be helpful so we are not fighting an agency, saying, “It is my document and I will tell you what is classified and what is not.”

Mr. Fitzpatrick, you are leaning on the button like you want to say something.

Mr. FITZPATRICK. I think you make an excellent point about the realm of information control that happens outside of what is defined as classified national security information. I was smiling at your words because there is not a defined meaning for FOUO. Again, to the point Liza made about the post-9/11 information sharing, connect-the-dots efforts that happened in the early 2000s, realizing that the challenge of too much information control blinded, perhaps, our ability to see this threat coming.

But the discovery of that as a problem, the study, rather, of that as a problem revealed that there are 118 different FOUOs. The Bush Administration had some recommendations about controlled unclassified information. The Obama Administration had a different take that tried to limit the ability of a government agency to utilize a control like that and to make them more uniform.

What was discovered in that process, which was to say only agencies who have a law, regulation, or governmentwide policy can
put controls on information, if it says you can control this information, only you can do that, the number of times that that appears in statute and regulation is far more than anybody thought, and the oceans of information that it covers is far more than anybody thought. What was hoped to be a limiting and a transparency initiative actually uncovered this vast ability to control more, or what could be controlled. It has not succeeded in releasing more information.

Senator LANKFORD. OK. Thank you. Thank you, Mr. Chairman. Chairman PETERS. Thank you, Senator Lankford.

Senator Johnson, you are recognized for your questions.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman. Senator Marshall brought up the JFK files. I would recommend that anybody that is interested in that to read JFK and the Unspeakable by James Douglass, and you will find out why the agencies are probably still reluctant to actually release more of that information. Again, that is information from yesteryear that is important to reveal the truth about history.

I want to talk about information in the here and now, that we need to govern action in the here and now, to fix problems in the here and now. Let us also set aside classified information. Let us talk about unclassified information that we do not have access to. Mr. Douglass talked about how Congress has willingly given away its classification authority. We have also allowed our oversight capabilities to completely atrophy, or almost completely atrophy. We have allowed that to happen. There is no enforcement mechanism.

I want to use the example I used yesterday in the Senate Finance Committee with Secretary Becerra. I asked him, “First of all, Mr. Secretary, do you think it is important that we understand where the coronavirus came from?” He said, “Absolutely.” I said, “Is your agency, HHS, are you leading an effort to determine that?” He kind of said some gobbledygook and then he said, “But we are not getting cooperation.” I said, “Well, interesting you said that. We are not getting cooperation from your agency.” Then I gave him a couple of examples.

There are two areas that the American public can get information out of the government. One is FOIA requests, and unfortunately that often has to go through a court and have that be court-ordered, although it should not be, and then through congressional oversight, right? I have two examples of both.

This was a document—these are the famous Anthony Fauci emails, OK. Through a FOIA request people got them early, and what we did is shortly after we had five Members of this Committee—there is actually a law, 5 U.S. Code (USC) 2954, that says if five Members of this Committee requested information, the government shall provide it. Under that statute we wrote the letter. We got this document, OK? This is dated February 4th. The classification here is Exception 4, is why it is redacted. That has to do with trade secrets or confidential commercial or financial information.

This is the same document recently produced under FOIA, to the general public. It is not redacted. Now I know what is under the
redactions. “Serial passage in ACE2 transgenic mice.” That is what was covered up. Anthony Fauci with a question mark, is going, this is not—February 4th, he is already recognizing that maybe the coronavirus came from a lab, from experiments with those humanized mice. That was denied Congress in our oversight capability.

A couple of days earlier, a similar type of thing. This is what we got in congressional oversight, all redacted. This is what was obtained under FOIA request. Again, we can see under the redactions now, again, not because the agency gave it to us, but because a court ordered it.

It is interesting. This is classified under Exception Number 5, which is deliberative process, inter-or intra-agency communications. What is interesting about this email chain, it includes Jeremy Farrar of the Wellcome Trust. He does not work for a U.S. Government agency. You have already blown the privilege in terms of confidentiality. Again, they are not following the law.

Through the accommodation process we asked for all 4,000 pages. We narrowed it down to 400. They would not give them to us. They allowed us to read it in a reading room. We could take notes, no copies. Over the course of a year, up until about January 2022, we got 350 of the 400 pages we requested. Since January 2022, we have been fighting tooth and nail for the last 50 pages.

This is what the FOIA request got, OK. This is what it looks like. OK? There is obviously some important information in this last 50 pages, and we cannot get it.

Now I will say the only reason we got the 350 pages is because Chairman Ossoff, to his credit as Chairman of the Permanent Subcommittee on Investigation (PSI)—I am Ranking Member—signed a request for these documents and then made some phone calls to start the process of production to us.

My message is mainly targeted or directed to Chairman Peters and Chairman Blumenthal. Congress has to reclaim its oversight capability. We need some kind of enforcement mechanism. I would love to pass a law, but again, we have laws on the books. They are not complying with the laws. They are flagrantly not complying with the laws. But there is no enforcement mechanism. They know that. The Administration knows that, so this problem just gets worse.

The only mechanism we have right now is public pressure obtained by bipartisan efforts. My plea, Mr. Chairman, is join us in these requests for information that the American public deserves. There should be nothing partisan about the origin of COVID. Our response to COVID occurred under two administrations. There is nothing partisan about that. This is information the public deserves to know, but also policymakers need to know so we can act; so we can fix problems, because I do not think anybody can take a look at our response to COVID and say it was a dramatic success. No, it was a miserable failure.

Mr. Eddington, the question I have for you is, particularly in a political environment, when you have the White House controlled by one party and a branch of Congress controlled by that same party, If the Administration gives us the middle finger there is just no enforcement mechanism. We cannot even hold them in contempt. If we are to hold them in contempt, if you have a political
party in one chamber able to do that, the Department of Justice is not going to prosecute that.

What kind of enforcement mechanism can we have for Congress to reclaim its oversight authority?

Mr. EDDINGTON. Senator Johnson, thank you very much for the question. The impeachment mechanism can be used against any civil officer of the government, from the President of the United States on down to the most lowly general service (GS)–5 clerk.

To borrow your paradigm here, one of the things that frustrated me when I worked in the House of Representatives was learning that when Speaker Pelosi had the opportunity to put an end to the Stellar Wind program, the illegal, warrantless surveillance program, which FISA Section 702 is the grandchild of, she claimed that she had no authority to act, she did not have staff in the room, et cetera, et cetera, et cetera. She is a very bright woman, a very capable woman.

What I could not understand for the life of me is why she did not ask for everybody's business cards. Now you are probably wondering why. After she had collected those business cards she should have thanked them and said, “I just needed to make sure that I had your names right so I could get them spelled correctly by legislative counsel for the impeachment resolution that I am going to introduce against you, all of you.”

Respectfully, and I do mean this respectfully, you do have a tool, and I would be willing to bet that a certain gentleman from Ohio, who happens to be heading up a specific subcommittee or committee in the House of Representatives, would probably be willing to work with you to begin to incentivize bureaucrats within the Executive Branch, to follow the law. That is my recommendation, sir.

Senator JOHNSON. Thank you, Mr. Eddington.

Chairman PETERS. Thank you, Senator Johnson.

Ranking Member Paul has some remaining questions you are recognized for.

Senator PAUL. I join Senator Johnson in hoping we can get bipartisan requests for records. One of the arguments to do it on our side is the records eventually are going to come out on the other side, and basically Republicans only are going to lead the charge and the explanation and the expose of those records. If we were to do it on this side, in a bipartisan way, we would be able to access those records, and there would be another interpretation, both of us, together or separately, of those records. If we have to wait until the other sides gets out it will look like we have stonewalled them, they get the records, but then it is going to be all basically a Republican investigation.

One other item I just wanted to get to was while we all seem to agree on the problem, we all seem to agree on a lot of the solutions, the one thing that sometimes divides us is how we pay for things, and there was some mention of needing more resources. I think that is dollars.

When we look at this, it is my hope that instead of always, we just say, “We need $10 billion more,” well, where is someplace we could actually take it from? I hope you will think about that.

I think that it was sort of tangentially mentioned, if you have a sunset on things that might save some money because you do not
have to go through a gazillion records because you have sunsetted them. We might want to put a dollar aspect on that. If we are developing a bill over many months, let us put a dollar amount on automatic sunsets and getting through a lot of that. That could be a lot of savings that could be freed up to go to committee that has to review this, that does not have enough resources.

Also if we classified less on the front end. Now how do you get the Executive Branch to classify? One other thought I have is that maybe each executive branch that classifies things, it should come out of their existing budget. What if the budget of HHS—I do not know why they would be classifying things, but if HHS wants to classify things maybe they are going to say, “Oh no, it is going to cost me a billion dollars of my budget to do it,” so it is a disincentive to classify. But ways of shifting cost as opposed to all being new costs. I am not opposed to some cost, but I think if we can take it—we already give a gazillion dollars to everybody. Let us try to take something they are using inappropriately and make it used appropriately. Does anybody have an idea on that? Eliza?

Ms. GOITEIN. Yes. I think it is really striking that the security classification budgets that agencies have are devoted overwhelmingly to classifying and protecting information and not to declassifying information. The percentage of those budgets that are spent on declassification, the last set of statistics that are available I think the percentage was half of a percent is spent on declassification.

One possibility is to require 10 percent of an agency’s security classification budget to be spent on declassification, right there. That not only means more resources for declassification, it also means less resources for classification. It kind of takes on both.

I do not think that will be enough. I think there will have to be extra resources. But as you have pointed out, I think there are enormous savings on the back end of this as well, and we have to take that into account.

Chairman PETERS. Thank you, Ranking Member Paul, and I agree. I think this is a cost-saving mechanism, although there might be some transition cost if we are moving to AI systems, machine learning, and we have to explore the pros and cons of all of that as well, but you will need some investments. You have to sometimes make investment to save money, and as we are thinking that through I think is important, so thank you.

Keep thinking of those ideas. We are all about saving money and doing things more efficiently and thoughtful, and we appreciate the four of you continuing in this discussion. We will aggressively seek you out as we are working on legislation in a bipartisan way to accomplish this.

I want to first off just thank Ranking Member Paul, again, for holding this hearing with me here today. I would also like to thank all of our witnesses. Thank you for taking time and joining us in this very important discussion and for providing further insights into how we improve the classification system to improve both transparency and efficiency.

Today our government creates a greater volume and variety of classified documents than we ever have in history. As we heard from our witnesses, overclassification, outdated technology, ineffi-
ciencies in declassification all result in significant costs to the country, and an outdated classification system reduces public trust, inhibits government oversight, and threatens, quite frankly, our national security.

Today’s hearing has made clear that investing in technology, like artificial intelligence, making classification and declassification work more efficiently, and incentivizing transparency can restore trust in how the government safeguards sensitive information. Additionally, your testimony has shown that Congress must take a more active role in the classification policy, and as Chairman I am committed to working on bipartisan legislation, and I look forward to working with Ranking Member Paul on these issues in the coming weeks and months.

The record for this hearing will remain open for 15 days, until 5 p.m. on April 7, 2023, for the submission of statements and questions for the record. This hearing is now adjourned.

[Whereupon, at 11:34 a.m., the hearing was adjourned.]
Appendix

Chairman Peters Opening Statement As Prepared for Delivery Full Committee Hearing: Modernizing the Government’s Classification System March 23, 2023

Every year, a whopping 50 million new classified documents are created. Classified materials typically fall into one of three categories, confidential, secret, or top secret, based on their perceived sensitivity.

Although there are existing requirements to automatically declassify documents after 25 years, in practice that process is ineffective, and there is currently a backlog of hundreds of millions of pages that are awaiting declassification.

Along with outdated technology, the result is an overburdened classification system that costs taxpayers more than $18 billion a year to maintain.

Experts, both within and outside of the federal government, estimate that between 50 and 90 percent of all classified materials could be made public without compromising national security, and that the over-classification of documents reduces transparency and erodes public confidence in the federal government.

Today’s hearing is an opportunity for the Committee to hear from experts on how Congress can modernize the classification system to improve efficiency and promote better transparency for the American people.

We’ll be discussing proposed reforms, including several recommendations from the National Archives’ Public Interest Declassification Board, to help streamline our nation’s classification and declassification processes.

For example, investing in advanced technology, such as artificial intelligence and machine learning, could help agencies better manage classified information, better serve the public, and meet the needs of the future.

Other proposed reforms could help reduce the number of classified materials and levels of classification, establish automated declassification tools, and provide an expedited declassification request process for lawmakers, all of which would improve transparency and ensure Congress and the public can help hold federal agencies more accountable.

I’m interested in pursuing bipartisan legislation to help tackle some of these concerns, and I hope my colleagues will join me in those efforts. I appreciate the engagement of Ranking Member Paul and his staff and believe we can find a bipartisan path forward on these important issues.

I look forward to having a productive discussion with our expert witnesses today to help us get more information and begin that process.
Senator Rand Paul, M.D.

Opening Statement for HSGAC Hearing on “Modernizing the Government's Classification System”

Twenty-six years ago, a bipartisan Senate Commission chaired by the late Senator Moynihan warned that excessive government secrecy and overclassification have significant consequences for the national interest. The Commission found that “[s]ecrecy is the ultimate mode of regulation ... for the citizen does not even know that he or she is being regulated”.

So, what happened in the decades since the Commission recommended Congress reassert its authority and reform the Executive Branch classification system? The problem got even worse.

Executive Branch officials from both political parties continue to arbitrarily overclassify government information to prevent oversight and withhold information from the public.

According to the National Archives and Records Administration, in 2017, over four million Americans with security clearances classified nearly 50 million documents, a system that cost American taxpayers over $18 billion.

President Biden’s own Director of National Intelligence, Avril Haines, acknowledged the overclassification problem on numerous occasions. As Director Haines said in January of this year, “[o]verclassification undermines the basic trust that public has in its government.”

There is no better example of the undermining of public trust than the federal government’s continued refusal to share with the American people information about the origins of the COVID-19 pandemic.

The Department of Energy recently shifted its position on COVID-19’s origins, and joined the FBI in concluding that the pandemic was most likely the result of a lab leak. The FBI Director later publicly confirmed
the FBI’s position that the pandemic most likely originated from a lab leak.

If not for the transparency forced by the media reports, we wouldn’t be able to talk about these important developments today.

Recently, Congress showed strong, bipartisan support for the need for transparency on the origins of COVID-19 by unanimously passing a bill requiring the Director of the National Intelligence to declassify information from the Wuhan Institute of Virology and the origins of COVID-19. I am glad that President Biden signed the bill into law earlier this week.

However, President Biden only committed to declassifying and sharing information “consistent with [his] constitutional authority to protect against the disclosure of information that would harm national security.” Given the Administration’s track record on transparency, I am concerned that the President’s statement suggests he will not publicly release all the information that exists.

And it isn’t just classified information the Executive Branch is withholding from the American people on COVID origins. Nearly a dozen federal agencies – including the Departments of Health and Human Services, State, and Defense, as well as the FBI – refuse to disclose thousands of records in their possession relevant to the origins of COVID-19.

Many of these records are not even classified.

I sent dozens of letters for over two years to federal agencies requesting these records, only to be stonewalled. In fact, recently disclosed emails made available by the Freedom of Information Act actually show Defense Threat Reduction Agency employees scheming to obstruct my request for information on the origins of COVID-19.

The American people deserve transparency and accountability. If we are being asked to sacrifice those values in the name of “national
security,” that definition should be narrowly tailored to protect only what is necessary to preserve our sources and methods.

In the Pentagon Papers case, Justice Potter Stewart remarked upon the wisdom of avoiding secrecy for its own sake. In his concurring opinion, Justice Stewart wrote, “when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion”.

I want to thank our consensus witness panel for being here today.

Mr. Chairman, I believe we have a unique opportunity to address overclassification by the Executive Branch in a bipartisan way, and I look forward to working with you on restoring transparency and accountability in government.
STATEMENT OF

ELIZABETH GITTLEIN

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 GORSTEIN & 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.

1. 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, 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, warned that “overclassification has reached serious proportions.”

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. 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.”

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

---

4. DET. DEP’T COMM’N ON CLASSIFIED INFO., REPORT TO THE SECRETARY OF DEFENSE 6 (1956) (hereinafter COOLIDGE COMMITTEE REPORT).
of Defense. The report found “innumerable specific instances” of unnecessary secrecy “which ranged from the amusing to the arrogant.”

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.”

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.” In 1985, the Stilwell Commission reported that, at the Department of Defense, “too much information appears to be classified.”

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.” 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.”

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.”

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.”

---

4. Id. at 31.
6. Id. at 6.
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.” 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.

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. McDaniels, National Security Council Executive Secretary under President Ronald Reagan, estimated that only ten percent of classification was for “legitimate protection of secrets.” A top-ranking Department of Defense official in the George W. Bush administration estimated that overclassification stood at 50 percent. 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 . . . .” 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.”

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

---

14 See id. at 353, 355, 417.
15 See Mournbrian Commission Report, supra note 3, at 36 (quoting McDaniels); 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 McDaniels’s statement)).
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.’”

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,” 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.”

In *New York Times Co. v. United States*, 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.” 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.’”

---

21 Moss Subcommittee Report, supra note 7, at 125.
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

---


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.35

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).36 There were also more than 2,000 agency classification guides, many of which were hundreds of pages long.37 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.”38

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 2009.39

37 Id. at 2.
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.\(^\text{38}\) As of 2021, 1,491 officials had the authority to classify information in the first instance.\(^\text{39}\)

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,\(^\text{40}\) and the information must fall within a list of specified categories.\(^\text{41}\) 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.\(^\text{42}\) 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.”\(^\text{43}\) 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.\(^\text{44}\)

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.\(^\text{45}\) 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

\(^\text{38}\) See E.O. 13526 § 1.3 (2009).
\(^\text{40}\) E.O. 13526 § 1.1 (2009).
\(^\text{41}\) Id. at § 1.4.
\(^\text{42}\) Id. at § 1.2.
\(^\text{43}\) Id. at § 1.5(b).
\(^\text{44}\) See ISOO 2017 REPORT, supra note 34, at 44.
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 rememers 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
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 War53 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

---

53 Brennan Center Report, supra note 3, at siv.
54 JAMES B. STENBERG ET AL., BUILDING INTELLIGENCE TO FIGHT TERRORISM, BROOKINGS INSTITUTION POLICY BRIEF, NO. 125 1-2 (2003),
55 STEINBERG ET AL., supra note 57, at 2.
56 2003 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),
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 overclassifying 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://sup.fas.org/isoo/ogwnotes/2003.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.”).
60 TED G.P., 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_Pape r (“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

---

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, Intelligence: 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 Sub-committee 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 over-classification 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 classified or continued the classification of information in violation of this Order or any implementing directive.” 73 Today’s executive order contains similar provisions, and it strengthens sanctions by providing that negligent over-classification — in addition to knowing and willful over-classification — 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 over-classification on the part of employees. The Stillwell Commission, studying the Department of Defense, reported in 1985

66 Griswold, supra note 23.
68 COOLEGE 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 over-classification, “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.
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 expediency, little scrutiny is given such determinations.” 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 “adding management oversight of classification decisions and attaching penalties to what too often can be characterized as classification by rote.” 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. 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.” 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.

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.” 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 § 5.4d(4) (2009).
78 ISOO 2017 REPORT, supra note 34, at 20.
80 E.O. 13526 § 3.3(a) (2009).
to contain” such information. The end of this laborious process, only around half of the documents that are reviewed are declassified; 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,

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.

---

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 prominent 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.\(^8\) 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.\(^9\)

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.”\(^9\) The people require knowledge of their government’s actions in order to debate the issues of the day and help shape

---

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. 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. 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.

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 undue, 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. 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).
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.  

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. The editorial boards of major news outlets around the country called for the program’s termination. 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.  

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. President Obama’s separately-commissioned review group similarly found that the program yielded no unique benefit.  

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. 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.

---

94 See, e.g., Editorial, Bad Times for Big Brother, N.Y. TIMES (Dec. 21, 2013), https://nyti.ms/1vyaqfQ; Editorial, Mr. President, Put These Cards on the NSA, L.A. TIMES (Dec. 20, 2013), https://latimes.com/opinion/la-xag-oped-20131220  
95 See POWNEWSRESEARCHCENTER, FEW SEE ADEQUATE LIMITS ON NSA SURVEILLANCE PROGRAM (Jul. 26, 2013), https://www.pownewsresearch.org/politics/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/  
97 PRESIDENT’S REVIEW GROUP 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.”)  
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. 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.

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). 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. 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.

---

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).


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 Department107 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).


105 Id. at 19.


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.).
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.\textsuperscript{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.\textsuperscript{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.”\textsuperscript{114} Similarly, the Moynihan Commission reported that “[i]t is important to keep in mind that 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.”\textsuperscript{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

\textsuperscript{112} NAT’L COUNTERINTELLIGENCE AND SEC. CTR., FISCAL YEAR 2019 ANNUAL REPORT ON SECURITY CLEARANCE DETERMINATIONS, supra note 45, at 7.
\textsuperscript{113} ISOO 2017 REPORT, supra note 34, at 4.
\textsuperscript{114} JOINT SECURITY COMMISSION REPORT, supra note 11, at 94.
\textsuperscript{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. Sawyer, 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(b), 1(d), 1(g)(a), 2(c), 3(7a) (2009).
118 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 638 (1952) (Jackson, J., concurring).
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. 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.

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. 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. 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

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 years 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 11.
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. 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 PIB’s 2012 report and a 2020 RAND study on government secrecy).

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.

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). President Nixon’s executive order on classification addressed this latter issue by providing specific examples of what would constitute “exceptionally grave damage,” “serious

125 See, e.g., PIB 2012 REPORT, supra note 84, at 2, 56; 12-14, 19, 23; JAMES B. BRUCE ET AL., SECRECY IN U.S. NATIONAL SECURITY: WHY A PARADOX SHIFTS TH At 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.

126 See, e.g., PIB 2012 REPORT, supra note 84, at 5, 27; BRUCE ET AL., supra note 124, at 11, 13.

127 Public Interest Declassification Bd., Public Meeting (Jun. 2015), 34:14 et seq., 54:00 et seq., available at https://www.youtube.com/watch?v=2ApswafH4dQ.

128 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.

---

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(d)(1).

\(^{132}\) MOYNIHAN COMMISSION REPORT, supra note 3, at xcvii.
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). \textsuperscript{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. \textsuperscript{134} This system has been in place since 2017. \textsuperscript{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. \textsuperscript{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. \textsuperscript{137} Congress also should raise the

\textsuperscript{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. ISO 2017 REPORT, supra note 34, at 8; ISO 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.

\textsuperscript{134} NAT’L GEOFSPATIAL INTELLIGENCE AGENCY, THE CONSOLIDATED NGA (COINGA) SECURITY CLASSIFICATION GUIDE 8 (SCG) (Jun. 7)


\textsuperscript{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 GOTTIN, THE NEW ERA OF SECRET LAW 7, 64-65 (Brennan Ctr. for Justice 2016), https://www.brennancenter.org/outwork/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—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. 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


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. But according to ISOO’s 2018 report, many agencies have not implemented this requirement. 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 problem of lengthy equity reviews by multiple agencies.

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. 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., 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 forgo 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 guidelines and are entrusted to apply that guidance, without engaging in a multi-agency review process. If anything, the potential harm that

---

143 ISOO 2018 REPORT, supra note 79, at 3.
144 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.
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 order145 — 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).
As discussed above, the purpose of such guides is to facilitate derivative classification by identifying information that has been classified by OCAIs. In theory, the guide 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.\(^\text{17}\) and ISOO has specified that agencies must perform such reviews at least once every five years.\(^\text{18}\) 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”\(^\text{19}\) — 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.”\(^\text{20}\) 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 systematically 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.

---

\(^{17}\) E.O. 13526 § 1.9 (2009).

\(^{18}\) 32 C.F.R. § 2001.16a(3).

\(^{19}\) E.O. 13556 § 1.9(a) (2009).

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.”

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.” 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.” 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.

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. 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

116 E.O. 13526 § 3.1(d) (2009).
117 Id. § 3.5(c).
118 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://ssp.fas.org/news/2016-12/Aftergood-PIDB.pdf.
119 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.
Testimony of Thomas Blanton, Director, and Lauren Harper, Public Policy Director, National Security Archive, George Washington University
www.nsarchive.org

To the United States Senate Committee on Homeland Security and Government Affairs

Hearing on “Modernizing the Government’s Classification System”
Thursday, March 23, 2023
10 a.m., Dirksen Senate Office Building SD-562

Chairman Peters, and Ranking Member Paul, thank you very much for holding this hearing and focusing a searchlight on the deep-seated problem of over-classification. Historians and journalists founded our own non-governmental organization, the National Security Archive, way back in 1985 precisely because over-classification had already taken hold of our republic, diminishing Congressional oversight, disempowering citizens, and withholding evidence from historians and the more fact-based among journalists.

Our statement today, co-authored by me and the Archive’s director of public policy, Lauren Harper, with the invaluable help of the Archive’s senior historian, Dr. William Burr, rises from 35+ years experience with too many secrets, from our 70,000 Freedom of Information requests to some 200 federal agencies, and from more than 20 government-wide audits of Freedom of Information and secrecy processes. We’ve won the Emmy Award for news and documentary research, and the George Polk Award for “piercing self-serving veils of government secrecy.” We brought the lawsuit that saved the White House e-mail from the Reagan, Bush and Clinton administrations, and we’ve gone to court against every administration ever since, to preserve records and compel appropriate declassification.

We’re here today to make 5 points in our 5 minutes.

Over-classification is out of control.

Declassification has collapsed.

Core functions of the National Archives have flatlined budget-wise for 30 years.

Key reform tools, needed by Congress and the public, are shriveling.

The only potential reform that will actually modernize the system is automatic sunsets.
Let’s start with the over-classification crisis. You’re holding this hearing today so you don’t need to be convinced, but the data on over-classification is only getting worse. Years ago Donald Rumsfeld’s deputy at the Pentagon told a committee of the Congress that over-classification was about 50%. Half of the secrecy was overdone. But now we have 20+ years of statistics from the only interagency review panel that objectively tests agency secrecy claims against requesters who want that information, and the over-classification level was over 75%! Three quarters of the time, that group of agency officials ruled for declassification, and against the secrecy claim, from 1996 to now. During the last year for which we have data, the openness rulings amounted to 93%.

Reformers used to think that reducing the number of original classification authorities (OCAs) would ultimately reduce the amount of secrecy. But the opposite has happened. We have fewer of those original authorities than ever, and more secrets than ever. Why? Computers enable the infinite replication of secrets. A single original classification in the digital age drives unlimited derivative classification decisions. In effect, the advent of electronic records has created what inside experts call a “tsunami of classified digital records.” The tsunami is arriving and the system is already underwater.

At the National Security Archive, we’re seeing more and more absurd claims by agencies. The Pentagon, for example, is withholding 60-year-old documents about Jupiter missiles in Italy and Turkey during the Cuban Missile Crisis on the grounds that release would supposedly harm our foreign relations. Actually, the Italian archives show they wanted to get rid of those missiles, just made them a target for the Soviets. Maybe that’s what the Pentagon is hiding.

On our website at https://nsarchive.gwu.edu, we have a whole section of postings we call “Dubious Secrets” – multiple declassified versions of the same items, top half blacked out one time, bottom half the next, or released in full one year, censored a few years later. We published one of Colin Powell’s White House e-mails in two versions with almost completely different black-outs, released 10 days apart. Turned out it was the same reviewer both times, just forgot what he cut in his rush.

The point is, as the former Solicitor General of the United States, Erwin Griswold, lamented, years after he lost the Pentagon Papers case, most classification covers government embarrassment of one form or another, not actual damage to our security. So the challenge today is to force better decisions on the front end, to minimize the incoming classified, and to disgorge as much as possible on the back end. That’s not happening.

**Declassification has collapsed**

Sad to say, the normal declassification processes have collapsed so badly that we at the National Security Archive now have to go to court just to get a processing schedule on our Freedom of Information requests. The George W. Bush Library told
us last year that one of our FOIA requests, for the records from a single meeting the President held with outside experts, preparing for his first encounter with Vladimir Putin, would take **12 years before declassification review could even start**. These are already 22-year-old documents, and now we wait another decade?

We can cite far too many metrics like that one. That interagency panel that did such a good job overriding agency secrecy claims now is totally jammed up, with more than a thousand cases in their backlog. The State Department’s documentary history series, the *Foreign Relations of the United States*, has fallen years behind its statutory mandate of 30 years after the relations in question. Now we are lucky to see the volumes after 40 years, because the Pentagon and the intelligence agencies delay on their reviews and treat historic materials as if they were current records. The breakdown of the declassification system across the board is blocking Congressional oversight, depriving history of evidence, and stalling accountability. Analyzing the causes leads us and our colleagues among historians and journalists to the conclusion that resources and authorities are sadly lacking.

**The National Archives needs one more Marine One helicopter**

One of our audits, led by Lauren, found that the Congress, five Presidents, and most of the Archivists dating back to 1991 have effectively flat-lined the budget for the past 30 years of the National Archives – one key institution that can **channel the secrecy tsunami if it has the authorities and the resources**. A couple of budgetary bumps in the last two years don’t make up for decades in the poor house. Those decades saw the exponential increase in the amount of records the National Archives is responsible for. For example, the Bush 41 White House left 80 gigabytes of records; the Trump White House left 250 terabytes! (Roughly 12 terabytes equals the size of the Library of Congress.) Federal agencies hold even more.

Last year, I told CNN, somewhat flippantly, the entire budget of the National Archives was about equal to a single Marine One helicopter that flew the President around – and they fact-checked me. No, Tom, you’re wrong, it’s two Marine Ones.

Well, we’re here to tell you today that the National Archives needs at least another chopper. The Marines are ordering 23 of them, at about $217 million apiece. We’ve got nothing against comfortable, secure travel for the President, but the institutional memory of our country is at stake when the National Archives withers. We’re including with our testimony the full text of our audit showing the “30-Year Flatline” and an updated chart comparing the last two years of small increases to the sad story of the previous decade.

**Congress’s oversight depends on National Archives’ functions**

For Congress to fulfill its oversight responsibilities, the National Archives contains a whole toolbox that you need to have fully funded and on the case. We historians
and journalists also depend on this toolkit. Let us name the most useful pliers and wrenches (no hammers but our court cases will work on that):

-- The **Public Interest Declassification Board**, established by Congress in the first place, could be the go-to venue for examining classified documents Congress wants for its oversight but agencies claim you can’t have. That Board can report to and pressure the President, but it needs a budget, member terms that don’t expire until a new appointee is confirmed, and staff support. (Its original budget was only $650,000 a year, so this is a tiny investment with major payoff for oversight.)

-- The **Information Security Oversight Office** provides the staff support for the Board, but has a shrinking budget that is a shame and a sin. Doubling this Office’s budget is another tiny investment ($5-10 million) with huge payoffs. The Office (Eye-Soo in the jargon) is a tiny band of hardy security inspectors who know the innards of the secrecy system, used to collect and publish the most helpful data on the classification problem, have honchoed massive declassification projects, and could make a real difference, with Congress’s support and tasking.

-- That Office is also supposed to staff the single most consequential secrecy reform from the 1990s, the **Interagency Security Classification Appeals Panel** (Ice-Cap we call it). We mentioned earlier, over its 20+ years, the Panel has ruled for declassification more than 75% of the time – one very stark data point measuring the degree of over-classification across the government – overruling the agencies in favor of requesters. The Panel proved that taking the declassification decision out of the cold dead hands of the originating agency led to actually rational outcomes. But the Panel’s success became its doom: requesters went there instead of to court, and now – after Covid – there’s a 1,317 case backlog. Not enough staff support. Too many repeat requesters. And no agency learning from all those Panel decisions before, so the same battles come up over and over, the results never get incorporated into agency classification guides.

-- Then there’s the **National Declassification Center**. A great idea of the 1990s, put into effect in the 2010s, to centralize declassification review of older records instead of sending the documents around in a daisy chain referral process. But as T.S. Eliot wrote, between the idea and the reality, falls the shadow. In this case, the shadow of limited resources and even more limited authorities. That Center, and the National Archives overall, needs the authority to declassify all historic records – those over the 30 year mark, for example – rather than referring them back out to the agencies. If the National Archives and the Center have to keep deferring to agency “equities,” we’ll never see the end of the backlog. Right now, the backlog amounts to millions of classified agency and presidential records and thousands of unanswered declassification requests. But we can hope that ownership authority at the Center would incentivize agencies to detail their own reviewers to the Center to take part in review, thus bulwarking the work.
In the short term, as a result of giving ownership to the National Archives, some agencies may try to keep their records away from the Center and the National Archives instead of handing them over at the 25 or 30 year retirement mark. Working in the other direction, however, the June 2024 deadline for electronic records management across the federal government should force an automatic process for the hand-off of records, and Congress can make sure that is built in to the design of the IT systems government-wide.

**Congress’ rightful role in reducing classification**

The Constitution says Congress is supposed to set the rules for the government and the military (Article I, Section 8). But a whole succession of Presidents has elevated the Article II designation as commander-in-chief to write the rules for themselves when it comes to classification. The bipartisan Moynihan-Helms-Combett commission more than 20 years ago recommended Congress write a statute to govern classification instead of leaving the system up to White House whims. Never happened.

Even today, on useful declassification bills like the new one on Covid origins, Congress misses the mark by leaving redactions up to the Executive. Back in 2016, Congress smartly added to the Freedom of Information Act the requirement of “demonstrable harm” before government could apply an exemption for a redaction. Congress needs to add the same requirement to all the withholding statutes, on sources-and-methods, on organization-and-functions, and more.

The goal should be to compel a real deliberation on the front end and the back end of the secrecy life-cycle. Does this need to be classified in the first place? Would there be any real harm from release? Would the harm outweigh the Congressional and public interest in this release? **What’s the cost of keeping this classified, and what’s the benefit from making it open?** Is there any way to “gist” this information so it can be unclassified, thus reducing costs and increasing information sharing? Can we minimize the upfront classification?

**The only no-cost modernization reform: Sunsets on secrets**

The only NO COST reform that would really work, both for the backlog and for better front-end classification decisions, is to set real sunsets on secrets. The first post-Cold War insider review, by the Information Security Oversight Office under Steve Garfinkel, recommended a 40-year “drop dead” date for secrets, meaning release without review for everything other than nuclear weapons design and human sources where a demonstrable harm would come from release. The reason, said Garfinkel in 1996, was “When we looked at material that was 40 years old, or older, we were ending up declassifying just about every bit of it, far more than 99 percent of it.”
We at the National Security Archive opposed the 40-year sunset at the time, arguing for a much shorter deadline, like 25 years. But the 25-year idea that ultimately appeared in the Clinton executive order on classification had so many exemptions it produced no sunset action at all, just an endless twilight. So we were wrong and Garfinkel was right.

Now, Garfinkel’s successors and other well-meaning reformers recommend that we get rid of the Confidential category. We don’t think so. There’s a strong argument that doing so will just absorb tons of bureaucratic energy and resources instead of actually reducing secrecy. Worse, with no Confidential stamp to deploy, classifiers will drive their information upwards into an already bloated Secret level. Confidential serves a real purpose in the current secrecy system. It signals that any damage here is time-limited, that the records don’t endanger sources or weapons design but more temporarily sensitive matters. Confidential material is the best candidate for automatic sunsets.

Instead of eliminating the Confidential category, let’s test the sunset proposition. Instead of bumping Confidential material up to Secret, let’s automatically declassify, without review, all historic Confidential records that are 15 years old. Let’s also include all the Confidential records whose original classifier set a “declassify by” date that has passed, often shorter than 15 years. No review for classification, perhaps some automated review to catch privacy matters like Social Security numbers. But again, by definition, Confidential records do not include weapon design information or sources-and-methods information.

Such bulk sunset releases should help un-gum the backlogged review system, and compel more thoughtful original classification decisions and categorization. Initially, having a drop-dead sunset may indeed push classifiers to assign higher levels of classification, or to set longer sunsets than 15 years even for Confidential-level material. But the pay-off for no-cost no-review declassification down the road would be worth the initial increases in over-classification. This core reform would signal the end of costly labor-intensive page-by-page declassification review or at least its reservation for the most sensitive records. This core reform would put teeth in the executive order’s rhetorical commitment that no secret is forever.

We need to disgorge the Confidential documents, not just get rid of the Confidential label. Then, we need to apply a “demonstrable harm” standard and a cost-benefit balancing test to all the rest, along with real “drop dead” dates for release. Machine learning and new technologies can help, but computers are no magic wand. Secrecy reformers have talked about applied IT for more than a decade, but real computerized effectiveness is still years and many dollars away, just like the self-driving car. Meanwhile, the secrecy crisis is now.

Thank you for your time and attention, and we welcome your questions!
U.S. National Archives’ (NARA) Budget: The 30-Year Flatline

National Security Archive’s 21st Sunshine Week Audit Shows Zero Real Dollar Increase at NARA Since 1991 Despite Exponential Rise in Records

Nation’s Historical Memory Systematically Starved by Congress, Five Presidents, and Agency’s Own Leadership

President Biden’s Pick for Archivist Must Double the Budget and Fix the Enormous Declassification Backlogs – 12-Year Wait on One Freedom of Information Act Request

Published: Mar 11, 2022
Edited by: Lauren Harper
For more information, contact: 202-488-0700
www.archives.gov

This report was made possible by generous funding from the CS Fund, the Open Society Foundation, and the Knight Foundation.

Washington, D.C., March 11, 2022 - The National Archives and Records Administration’s (NARA) budget has remained stagnant in real dollars for nearly thirty years. At roughly $220 million dollars when adjusted for inflation, its budget represents 0.005% of the federal budget — this, according to a National Security Archive Audit released today to mark the beginning of Sunshine Week.[1]

While its budget has flattened, the number of records NARA must preserve, particularly electronic records, has increased exponentially over three decades. The George H.W. Bush library, for example, has 28,000 cubic feet of electronic records in its holdings, whereas the Obama library has 200 cubic feet.[2] This explosion of electronic records is a huge part of the growing backlog for Freedom of Information Act (FOIA) and Mandatory Declassification Review (MDR) requests at the presidential libraries, which constitute only part of NARA’s holdings.

A recent letter to our office from the George W. Bush library encapsulates the gravity of the state. In response to an estimated date of completion query for a FOIA request, the library replied “we estimate that your FOIA request may be completed in 12 years. We apologize for this inconvenience and appreciate your understanding and patience.” (Emphasis added.)
The Budget

NARA’s current budget is a recipe for disaster for an agency whose sole mission responsibilities include preservation of government records (which includes more than 13 billion pages of textual records alone and hundreds of terabytes of electronic records), providing public access to its holdings; running a government-wide records management program; maintaining a sprawling network of records facilities; and administering the presidential libraries.

Budget woes are not new for the agency. There have been seven Archivists of the United States (including three acting) since the agency gained independence from the General Services Administration in 1985. The agency has been given more responsibility in that time (in the form of more presidential libraries and standing up the National Declassification Center), and few additional resources.

The chart below, which was compiled by obtaining NARA’s gross total outlays in a given fiscal year (FY) and then adjusting the figures for inflation using a budget offset (which used FY2012 as a baseline), shows how little the budget situation has changed.
<table>
<thead>
<tr>
<th>Year</th>
<th>Salary</th>
<th>Performance Bonus</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 2017</td>
<td>$352,000</td>
<td>$38,045</td>
<td>4,172 Increase</td>
</tr>
<tr>
<td>FY 2016</td>
<td>$381,000</td>
<td>$36,873</td>
<td>14,707 Increase</td>
</tr>
<tr>
<td>FY 2015</td>
<td>$363,000</td>
<td>$35,115</td>
<td>14,715 Increase</td>
</tr>
<tr>
<td>FY 2014</td>
<td>$346,000</td>
<td>$35,401</td>
<td>17,800 Decrease</td>
</tr>
<tr>
<td>FY 2013</td>
<td>$350,000</td>
<td>$38,281</td>
<td>88% Increase</td>
</tr>
<tr>
<td>FY 2012</td>
<td>$353,000</td>
<td>$35,000</td>
<td>3,450 Decrease</td>
</tr>
<tr>
<td>FY 2011</td>
<td>$355,000</td>
<td>$39,479</td>
<td>11,079 Increase</td>
</tr>
<tr>
<td>FY 2010</td>
<td>$375,000</td>
<td>$35,825</td>
<td>4,496 Increase</td>
</tr>
<tr>
<td>FY 2009</td>
<td>$325,000</td>
<td>$34,679</td>
<td>16,075 Increase</td>
</tr>
<tr>
<td>FY 2008</td>
<td>$290,000</td>
<td>$11,404</td>
<td>3,500 Increase</td>
</tr>
<tr>
<td>FY 2007</td>
<td>$273,000</td>
<td>$39,061</td>
<td>11,260 Decrease</td>
</tr>
<tr>
<td>FY 2006</td>
<td>$276,000</td>
<td>$31,161</td>
<td>10,155 Decrease</td>
</tr>
<tr>
<td>FY 2005</td>
<td>$276,000</td>
<td>$32,246</td>
<td>9,316 Increase</td>
</tr>
<tr>
<td>FY 2004</td>
<td>$260,000</td>
<td>$92,050</td>
<td>63,962 Increase</td>
</tr>
<tr>
<td>FY 2003</td>
<td>$252,000</td>
<td>$248,188</td>
<td>31,646 Decrease</td>
</tr>
<tr>
<td>FY 2002</td>
<td>$227,000</td>
<td>$279,834</td>
<td>22,065 Increase</td>
</tr>
<tr>
<td>FY 2001</td>
<td>$276,000</td>
<td>$256,769</td>
<td>16,185 Increase</td>
</tr>
<tr>
<td>FY 2000</td>
<td>$305,000</td>
<td>$240,584</td>
<td>89,906 Decrease</td>
</tr>
<tr>
<td>FY 1999</td>
<td>$248,000</td>
<td>$330,490</td>
<td>70,491 Increase</td>
</tr>
<tr>
<td>FY 1998</td>
<td>$231,000</td>
<td>$311,069</td>
<td>3,980 Increase</td>
</tr>
<tr>
<td>FY 1997</td>
<td>$377,000</td>
<td>$367,089</td>
<td>6,794 Decrease</td>
</tr>
<tr>
<td>FY 1996</td>
<td>$377,000</td>
<td>$313,683</td>
<td>35,313 Increase</td>
</tr>
<tr>
<td>FY 1995</td>
<td>$345,000</td>
<td>$345,216</td>
<td>83,288 Increase</td>
</tr>
<tr>
<td>FY 1994</td>
<td>$295,181</td>
<td>$2,664</td>
<td>20,962 Increase</td>
</tr>
<tr>
<td>FY 1993</td>
<td>$270,000</td>
<td>$39,662</td>
<td>7,465 Decrease</td>
</tr>
<tr>
<td>FY 1992</td>
<td>$266,000</td>
<td>$46,167</td>
<td>47,060 Increase</td>
</tr>
<tr>
<td>FY 1991</td>
<td>$195,000</td>
<td>$318,757</td>
<td>10,077 Increase</td>
</tr>
</tbody>
</table>
Budget Shortfalls at the National Declassification Center and the Presidential Libraries

Decreasing budgets and staffing shortages have impacted some of the most critical offices within NARA, particularly at the National Declassification Center (NDC) and the presidential libraries. The chart below shows the total budget requested for NARA’s “Legislative, Presidential Libraries, and Museums” program – for which the presidential libraries make up the bulk of total costs – and the NDC. These figures have also been adjusted for inflation.

<table>
<thead>
<tr>
<th>FY</th>
<th>NARA Budget Actual Dollars</th>
<th>Legislative, Presidential Libraries, and Museums Budget Request (in thousands of $)</th>
<th>LPA Full Time Employee Request</th>
<th>NDC Budget Request (in thousands of $)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020</td>
<td>327,403</td>
<td>610,420</td>
<td>403</td>
<td>95,616</td>
</tr>
<tr>
<td>2019</td>
<td>395,977</td>
<td>595,412</td>
<td>403</td>
<td>96,119</td>
</tr>
<tr>
<td>2018</td>
<td>398,975</td>
<td>575,824</td>
<td>460</td>
<td>95,788</td>
</tr>
<tr>
<td>2017</td>
<td>395,945</td>
<td>613,568</td>
<td>492</td>
<td>58,524</td>
</tr>
<tr>
<td>2016</td>
<td>395,873</td>
<td>614,675</td>
<td>489</td>
<td>58,526</td>
</tr>
<tr>
<td>2015</td>
<td>393,116</td>
<td>610,840</td>
<td>511</td>
<td>56,035</td>
</tr>
<tr>
<td>2014</td>
<td>335,401</td>
<td>616,290</td>
<td>542</td>
<td>57,241</td>
</tr>
<tr>
<td>2013</td>
<td>353,281</td>
<td>616,971</td>
<td>538</td>
<td>57,536</td>
</tr>
</tbody>
</table>

The National Declassification Center was established during the Obama administration to streamline the declassification process and improve the release of historically valuable permanent records. It is responsible for processing tens of millions of pages, many requiring declassification processing and/or review annually, and developing processes to review more than 190,000 cubic feet of classified paper records, as well as large volumes of classified electronic records. Its budget in real dollars has decreased steadily in the time since NARA began reporting the amount requested for the Center, which has only 38 employees to carry out this task (the FSDB/WIB staff has only 9 people, meaning there are more presidential libraries than declassifiers).

Staffing is certainly not the only challenge the NDC faces. The extraordinary inefficiency of current declassification procedures is another large problem. The NDC also must be granted the authority to explicitly any record over 25 years old on its own (as long as redact classification does not impair confidential sources and nuclear weapons details or personal privacy) and stop the current wasteful equity referral and consultation re-review process, whereby multiple reviewers from multiple agencies are allowed to re-review the same document multiple times. The rule
Limited Oversight of Records Retention Schedules and Important Records Management Policies

Staffing issues play out in less obvious ways, too. One pernicious example is that it results in limited oversight of agency records retention schedules. These are the forms every agency must submit to NARA that, if approved, allow the agency to destroy information or withhold it for unreasonably lengthy periods. Numerous alarming approvals of dangerous records retention policies point to NARA’s limited oversight capabilities. They include:

- In 2018, NARA formally approved a CIA records retention schedule that allows the agency to destroy information that is more than 30 years old — in spite of the warnings from public interest groups and others that this will likely result in the permanent loss of an untold number of potentially important documents. The records schedule — and NARA’s apparent rubber-stamp approval of it — was doubly concerning considering the agency’s widely acknowledged history of destroying important records.
- In 2017, NARA approved an outrageous request by the Defense Threat Reduction Agency (DTRA) granting the agency unreviewed control over historical reports on nuclear weapons stockpile. Specifically, DTRA can, thanks to NARA’s approval, keep its reports on the U.S. nuclear weapons stockpile closed to the public for 40 years or more after they were created — a move that the American Civil Liberties Union described as an “draconian action... contrary to the public interest as well as to NARA’s mission and its organizational interests.”
- In 2017, NARA’s Records Appraisal and Agency Assistance branch recommended the ATF approve a controversial immigration and Customs Enforcement records schedule that would have allowed the agency to designate its temporary (and then legally destroy) a wide array of sensitive immigrant alien information. The proposed schedule would have included records on sexual abuse claims filed by detainees at ICE facilities and investigative records on detainees deaths. After a public outcry and letters signed by members of both the Senate and the House, NARA re-opened a 15-day public comment period.

Not only are these not isolated incidents, they account for only part of the problem of historical materials being lost to the American people — a problem greatly exacerbated by the lack of resources for oversight. NARA’s “unauthorised disposal of federal records” chart catalogues all of the cases NARA investigated concerning the “accidental, inadvertent, or unlawful disclosure, removal, alteration, corruption, deletion, or other destruction or disposal of records.” A quick look shows that the departments of State, Interior, Agriculture, and Justice are frequently investigated agencies, and that improperly disposing records and encrypted messaging applications are a common theme.

Limited oversight capabilities also make it far more difficult to ensure that agencies comply with records management policies, like guidance on managing all email electronically and managing all permanent electronic records in electronic format, which were the subject of the Archivist’s Synopsys Week audits in 2016 and 2018 respectively. Our audits of contracted agencies’ self-reported assessments and results — which NARA had been unable to independently verify — and agency
responses showed that FOIA requesters are often not seeing the benefit of any improved electronic records management.

Our audits make clear that NARA needs to actively oversee the electronic records management process, as opposed to letting agencies self-assessments at their own risk. The Next Archivist Needs to Speak Bluntly and Demand More Statutory Authority

The next Archivist needs more than just resources. They will need to maximize the authority they have and be granted more.

One of the most frustrating episodes of President’s tenure concerned the Senate Intelligence Committee’s full, scathing report on the Central Intelligence Agency’s torture program. Despite pleas from the public and Members of Congress, former CIA refused to use its clear statutory authority to label the report a federal record, which would have made it subject to Freedom of Information Act disclosure requirements. Our audit was the first time the Justice Department told the CIA not to. According to a November 5, 2015, letter written by Senator Patrick Leahy of Vermont and Diane Feinstein of California, “individuals at the National Archives and Records Administration have stated that, based on guidance from the Department of Justice, they will not respond to questions about whether the study constitutes a federal record under the Freedom Records Act because the FOIA case is pending.”

The Presidential and Federal Records Act Amendments of 2014 explicitly grants the Archivist the power to designate documents as federal records even if they cannot currently be released to the public, and the Archivist should have used it. While the record was preserved as a presidential record, which is arguably another reason former CIA officials refused to the over the fate of the report, the Trump administration experience has shown that we cannot blindly trust the Chief Executive to do the right thing.

The Trump administration’s disastrous handling of its presidential records underscores the need for NARA to have more real-time input into the White House’s preservation policies, including the ability to review administration policies at the beginning of each presidential term, as well as the right to receive regular reports from the White House Office of Administration on the Executive Office of the President’s compliance with the Presidential Records Act.

This is the Archivist’s 21st FOIA Audit. Modeled after the California Sunshine Survey and subsequent state “FOIA Audits,” the Archivist’s FOIA Audits use open-government laws to test whether or not agencies are obeying those laws. Recommendations and findings from previous Archivist FOIA Audits have, directly led to FOIA flows in both the 2016 FOIA Improvement Act (25-year (5) year) and the Open Government Act of 2007 (requiring agencies to report their ‘most’ pending requests), exposed NARA’s lack of action on FOIA fee regulations, ultimately prompting an Administrative Procedure Act lawsuit filed by Cause of Action that forced the agency to craft new (allow facilitator) regulations; forced agencies to craft explicit open governance guidelines; mandated FOIA backlog reductions; institutionalized the use of individuals by FOIA tracking numbers; led to importing requirements on the average number of days needed to process requests; and revealed the (often embarrassing) gap of the circular FOIA requests – like FOIA requests so old they could not be arbitration. The surveys include:

- The Archivist’s Theme: “Diaspora” Change or “More Thunder Than Lightning”? (2017)
- File Not Found: 10 Years After 9-11, Most Federal Agencies are Ineligible (2007)
- 40 Years of FOIA, 20 Years of Delay (2007)
- Mixed Signals, Mixed Results: How President Bush’s Executive Order on FOIA Failed to Deliver (2008)
• 2015 Knight Open Government Survey: Only Half of Federal Agencies Have FSIA
  Requests in a Decade (2015)
• 2015 Knight Open Government Survey: Only Half of Federal Agencies Have FSIA
  Requests in a Decade (2015)
• Freedom of Information Regulations Still Unchanged, Still Unchanging
  Operation (2015)
• Half of Federal Agencies Still Use Outdated Freedom of Information
  Regulations (2014)
• More Agencies Falling Short on Mandate for Online Records (2015)
• Saving Government Email an Open Question with December 2015 Deadline
  Looming (2016)
• There is a Fine Line between Agencies and FOIA Issues (2013)
• Agencies Struggling to Respond to FSIA Requests for Email (2015)
• FOIA’s 25th Birthday: Requester Confirms FSIA Delayed Judicial
  Oversight (2016)
• New Transparency is Potentially strangest Audit Shows Three Categories of
  His Questions More than 100% for Transparency (2015)
• “Still Insecure” Lessons After Draft of Topology of Long Ignored FOIA
  Requests (2011)

NOTES
[1] These figures are based on the actual outputs from FOIA, which are the most
more actual budget data is available.
[3] One terabyte equals one thousand gigabytes. It is estimated that 15-16 terabytes

National Security Archive
Suite 700 / G timeline Library
The George Washington University
212 G Street, NW
Washington, DC 20052
Office: 202/789-7365
Fax: 202/789-7065
Contact by email
<table>
<thead>
<tr>
<th>FY</th>
<th>Actual outlays, gross (total) - in thousands of $*</th>
<th>Adjusted with budget deflator - in thousands of $</th>
<th>Real change from prior year - in thousands of $</th>
<th>Archivist</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY2022</td>
<td>385,000</td>
<td>336,627</td>
<td>8,700 increase</td>
<td>Ferriero/Debra Steidel Wall</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(acting)</td>
</tr>
<tr>
<td>FY2021</td>
<td>368,000</td>
<td>327,627</td>
<td>6,264 increase</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2020</td>
<td>362,000</td>
<td>321,663</td>
<td>16,077 decrease</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2019</td>
<td>373,000</td>
<td>337,740</td>
<td>12,265 decrease</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2018</td>
<td>380,000</td>
<td>350,005</td>
<td>19,040 decrease</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2017</td>
<td>392,000</td>
<td>369,045</td>
<td>4,172 increase</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2016</td>
<td>381,000</td>
<td>364,873</td>
<td>14,757 increase</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2015</td>
<td>363,000</td>
<td>350,116</td>
<td>14,715 increase</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2014</td>
<td>346,000</td>
<td>335,401</td>
<td>17,880 decrease</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2013</td>
<td>359,000</td>
<td>353,281</td>
<td>281 increase</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2012</td>
<td>353,000</td>
<td>353,000</td>
<td>3,450 decrease</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2011</td>
<td>349,000</td>
<td>356,450</td>
<td>2,625 increase</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2010</td>
<td>339,000</td>
<td>353,825</td>
<td>4,346 increase</td>
<td>David Ferriero</td>
</tr>
<tr>
<td>FY 2009</td>
<td>329,000</td>
<td>349,479</td>
<td>38,075 increase</td>
<td>Adrienne Thomas (acting)</td>
</tr>
<tr>
<td>FY 2008</td>
<td>293,000</td>
<td>311,404</td>
<td>11,503 increase</td>
<td>Allen Weinstein</td>
</tr>
</tbody>
</table>

*These figures are found in the official Budget of the United States that is issued by the Office of Management and Budget (OMB) and published on GovInfo.gov. The budget numbers for NARA are found in the appendix of a given FY’s budget. The actual outlays, gross (total) for a given FY are found in the FY report two years following; so, for example, the FY2020 actual outlays are found in the FY2022 report: [https://www.govinfo.gov/content/pkg/BUDGET-2022-APP/pdf/BUDGET-2022-APP.pdf](https://www.govinfo.gov/content/pkg/BUDGET-2022-APP/pdf/BUDGET-2022-APP.pdf) (see page 1314).
Biographies of National Security Archive witnesses for Senate Homeland Security and Governmental Affairs Committee hearing, March 23, 2023

**Thomas Blanton** is the director since 1992 of the independent nongovernmental National Security Archive at George Washington University (www.nsarchive.org), which won the George Polk Award in 2000 for “piercing self-serving veils of government secrecy.” He was the Archive’s first Research Director starting in 1986, and he has also served as the Henry M. Jackson Lecturer at Whitman College, the Lazerow Lecturer at Long Island University, and the Henderson Lecturer at the University of North Carolina at Chapel Hill. Educated at Harvard University, he is series co-editor for the Archive’s online and book publications of more than a million pages of declassified U.S. government documents obtained through the Archive’s more than 70,000 Freedom of Information Act requests. His books have been awarded the Link-Kuehl Prize from the Society for Historians of American Foreign Relations, and “Outstanding Academic Title” designation from the Association of College and Research Libraries. His honors include the Emmy Award (2005) for individual achievement in news and documentary research, the Jean Mayer Global Citizenship Award (2011) from Tufts University, Harvard University’s Newcomen Prize in History (1979), and the American Library Association’s James Madison Award Citation (1995) for “defending the public’s right to know.”

**Lauren Harper** is the Director of Public Policy & Open Government Affairs at the National Security Archive. She has been with the Archive since 2011, and in her current role helps develop the Archive’s public policy positions, maintains key relationships within the federal government and open government community, and serves as one of the organization’s chief public spokespersons on access to information and secrecy issues. Harper has led or co-authored eleven of the Archive’s FOIA audits, including 2022’s “U.S. National Archives’ Budget: The 30-Year Flatline,” and 2019’s “25-Year-Old FOIA Request Confirms FOIA Delays Continue Unabated.” She has authored or contributed to dozens of other National Security Archive Electronic Briefing Books, writes regularly for the Archive’s blog, Unredacted, on a wide-range of FOIA and national security issues, and manages all of the Archive’s social media accounts. Harper also oversees the Archive’s Afghanistan Project, and edited a 2,000-document reference collection on the 20-year U.S. war in Afghanistan. She holds a Master of Arts degree in Middle Eastern Studies and a Master of Public Policy degree, both from the University of Chicago, and received her Bachelor of Arts degree from Scripps College. She is a member in good standing of the American Society of Access Professionals, and has just been appointed by the Acting Archivist to the Freedom of Information Advisory Committee.

The National Security Archive is a non-profit non-governmental organization based at the George Washington University and recognized by the IRS as a public charity. The Archive receives no government funding or contracts, and instead relies on publication royalties and donations from individuals and foundations for its $3 million annual budget.
United States Senate Committee on Homeland Security and Government Affairs
Hearing on Modernizing the Government’s Classification System
Statement for the Record
Mr. John P. Fitzpatrick
Former Director, Information Security Oversight Office
March 23, 2023

Thank you, Chairman Peters, Ranking Member Paul, and members of the Committee, for the opportunity to discuss potential changes needed to modernize and improve the effectiveness of the U.S. Government’s classification and declassification system, and in particular the roles performed by the National Archives and Records Administration (NARA), and its components the Information Security Oversight Office (ISOO) and the National Declassification Center (NDC).

I served in the U.S. government for thirty-five years, all of it in national security and intelligence, retiring in 2019. My service included leadership positions at the Central Intelligence Agency, the National Reconnaissance Office, the Office of the Director of National Intelligence (ODNI), ISOO, and the National Security Council (NSC) staffs of the Obama and Trump administrations. The last dozen or so years, at ODNI, ISOO, and the NSC were concerned with the security and classification policies of the U.S. Government, the implementation of those policies in Departments and Agencies, and efforts to continuously improve government performance in this area. My testimony today represents my personal views as informed by that experience, and not that of any employer or industry group with which I have engaged after retiring.

There is no shortage of opportunity for change and improvement in the government’s classification enterprise. I wish to make clear that I believe the possibility for change and improvement of the classification system is real, and I emphasize how Congressional action, and specifically this committee’s role, is urgently needed to send the demand signal for that change.

I draw an analogy to the role the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 played in instigating improvements to the security clearance process across government.
That law, and this committee’s role in overseeing its implementation, presented a clear mandate for change. It required the President to designate a single official as responsible for driving that change and established strict performance measures and reporting timelines. I played a role in designing the approach and implementing the structure put in place to respond to those IRTPA requirements and witnessed the necessity of having both the Congressional mandate and the single Presidential designee to drive change.

Any successful effort to modernize the classification system will require the concerted efforts of top administration functions and key policy and operational entities to formulate and drive change. The Office of Management and Budget’s (OMB) role not only in budgeting broadly, but in shaping the information technology investment and development priorities of all departments and agencies, will be critical. The NSC’s mission to convene departments and agencies to identify policy changes and implementation paths while aligning with the U.S. national security interests, is necessary to obtain buy-in from departments and agencies that comprise the government’s classification enterprise. Working together, OMB and NSC focus and drive will be required to sustain collective efforts among departments and agencies to implement the changes directed. For these reasons, I consider it essential that any legislative mandate should require a single, responsible official be designated by the President as accountable for the government-wide effort. Without top of government accountability, prospects for progress are few.

Another essential element of reform is to fortify ISOO, whose policy and oversight functions are elevated and made central to this effort. While ISOO has a rich history of steering policy and oversight in this area, strengthening its position is key to meeting the challenge of significant reform. Specifically, deliberate efforts are required to:

- Increase ISOO’s prominence within and among the National Security Departments and Agencies, specifically deriving this through active sponsorship from, and utilization by, NSC & OMB, and, if adopted, the single official designated to drive the classification reform.
- Increase ISOO’s own resources and ensure it has independent control of same. In the competition for scarce resources across the executive branch and within NARA, ISOO’s resources have dwindled over time, and a reform effort such as this should include
rightsizing and empowering ISOO and its Director to a level that can ensure it is able to meet its missions.

- Retaining ISOO’s roles in administering both the Public Interest Declassification Board (PIDB) and Interagency Security Classification Appeals Panel (ISCAP). ISOO’s independent perspective on classification across government complements the PIDBs statutory role. The same independence, as well as its staff expertise, makes the ISCAP a fair and neutral arbiter in carrying out its reviews.

- Designating the ISOO Director to Co-lead the development of a technology investment strategy with OMB and the Office of the Federal Chief Information Officer (CIO). ISOOs subject matter expertise and ties to the classification/declassification organizations in departments and agencies are a necessary complement to OMB and the Federal CIO guidance of information technology investment and implementation government wide.

As the Committee is aware, the expanse of information that has been classified, that remains classified, and that will be classified going forward, is practically immeasurable. The crisis of overclassification stems from decisions to classify information that need not be classified, to classify it at levels higher than it deserves, and to retain it as classified longer than the risk of potential harm reasonably requires. Critical contributors to this state are the expansion of classified information in the post-9/11 age, the explosion in classified networks, which both facilitate critical information sharing, and enable classified document creation at an ever increasing scale; the policies for declassification that give deference to departments’ and agencies’ often risk-averse preference to extend classification reflexively, so as not to consider the actual management of risk, nor acknowledge that sensitivity wanes over time; and, finally, the decades-long under resourcing of the staffs and programs in place at departments and agencies whose jobs are to consider classification and declassification actions, but who are overwhelmed both by seas of paper that must be handled manually and serially, and vast oceans of digital records for which there are no tools to automatically sift, sort, and decide what to classify.

I believe that the need to invest in technology to support improved classification and declassification is the single most important piece of this modernization effort. Any effort that only seeks to revise policy, to heighten the importance of public interest, or to otherwise
prioritize the work among agencies or the NDC, all worthy of focus and attention, will still depend upon the manual, serial, paper-oriented capabilities that limit the systems’ abilities today.

My emphasis on a statutorily-directed and administration-led reform effort relies entirely on the need to create capabilities in the existing and future information environments across government that utilize emerging and maturing technologies, such as artificial intelligence and machine learning, to facilitate the review of classified current holdings, to engage classification decisions at the time of document creation with the intent of thwarting overclassification, and to suggest new ways to process digital records in the aggregate and alleviate future backlogs before they are built. Investment will also be needed to give access to classified information environments where they do not currently exist. The truth of the matter is that some declassification review offices lack classified network access, further confining them to a paper-only, manual review process.

I do not portray these observations about the poverties of the current system nor the criticality of technological investment as new, but as key components of the imperative for change. As the committee is no doubt aware, the Public Interest Declassification Board has articulated these needs along with specific focus areas in its reports over the last decade. Its May 2020 report A Vision for a Digital Age: Modernization of the U.S. National Security Classification and Declassification System, presents a menu of opportunities to achieve strategic change. A prominent and fortified governance structure could use these ideas to guide the application of new technological capabilities not only toward the goal of reducing the vast backlog of classified information, but at critical topics in the public interest that merit release to inform public policy and the public’s understanding of how the government works.

I will close by thanking the committee for its efforts to bring attention and drive action to these needed reforms. I welcome your questions and am grateful for the opportunity to contribute ideas as you formulate the way ahead.
Statement for the Record

of

Patrick G. Eddington
Senior Fellow
Cato Institute

before the

Senate Committee on Homeland Security and Government Affairs

Hearing on Modernizing the Government’s Classification System

March 23, 2023
Chairman Peters, Dr. Paul, Members of the Committee, my sincere thanks for inviting me to be here today to offer my views on the very serious problem of the Executive branch's penchant for overclassifying federal records. Let me state at the outset that the views I express here today are strictly my own and do not necessarily represent the views of the Cato Institute, its management, or its board of directors.

By way of background, I got my first SECRET clearance when I was a young Army 2nd Lieutenant in 1986, followed by a full Top Secret/Special Compartmented Information (TS/SCI) clearance when I joined the Central Intelligence Agency two years later. I also held a TS clearance from 2007-2014 when I worked for then-Rep. Rush Holt (D-NJ), who was subsequently named to the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community. I staffed him on the committee, during which I regained my TS/SCI plus a Q clearance.

Accordingly, I know the necessity of keeping some things secret. I also know, from the historical record and direct, personal experience inside and outside of government, that often times Executive branch secrecy, administrative control measures, or Freedom of Information Act (FOIA) noncompliance is used as a legal cloak to hide waste, fraud, abuse, mismanagement, and even criminal conduct.

Today, I'll share some of those key illustrative experiences with you and offer what I hope you'll find to be potentially workable solutions to the problem. First, let me address in brief the history of how we got to where we are with our overclassification crisis.

**Background**

As I noted in a piece in *The Hill* earlier this year, the word “secrecy” appears only once in the Constitution — and not in Article II, which deals with the presidency. Instead, it appears in Article I, Section 6, Clause 3: “Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy...”
Thus, Congress was the original classification authority in the federal government. Indeed, nowhere in Article II of the Constitution will you find explicit language that permits the president or his designees to classify a single document. How then did the Executive branch become the dominant player in the world of federal secret keeping?

Throughout most of our nation’s history, Congress never asserted its constitutional prerogatives or authority in this area. As a result, successive presidents claimed the authority to decide what would or would not be kept secret.

During the Taft administration, the 1911 Defense Secrets Act\(^1\) represented the first effort to codify national defense-related secrets and it featured stiff penalties for violations of the Act: at least a year in jail and a $1,000 fine.

Once the United States declared war on Germany in April 1917, the military services, as well as the Departments of State, Justice, and Treasury (via the Secret Service), all engaged in domestic surveillance operations that were shielded from public view behind a veil of secrecy. Penalties for exposing things deemed secret were made ever more draconian through the passage of the Espionage Act.\(^2\)

From the end of World War I to the present day, internal practices and procedures for creating and keeping secrets within the executive branch have grown and evolved, with a 1953 Supreme Court landmark case creating the “state secrets privilege” seemingly legitimizing a de facto Executive branch monopoly on creating and keeping secrets.\(^3\) Only rarely has Congress been active in legislating select aspects of the national secrecy system, such as the Atomic Energy Act,\(^4\) National Security Agency Act,\(^5\) and the Classified Information Procedures Act.\(^6\)

Ironically, by enacting these bills, Congress effectively yielded further ground to the executive branch vis-a-vis deciding what is, or is not, classified information.

What is more, not even the major intelligence scandals unearthed by the Church Committee during the Ford administration motivated Congress to prohibit the misuse of the classification system to conceal waste, fraud, abuse, mismanagement, or criminality. Instead, Congress allowed presidents, via executive orders, to self-police any potential Executive branch classification overreach, the current version being EO 13526.\(^7\) That decision to allow the
Executive branch to effectively "go it alone" on managing the nation's classified information has been a costly mistake with real-world consequences.

**The Financial Price of Excessive Government Secrecy**

When the national Commission on Protecting and Reducing Government Secrecy issued its final report in March 1997, it estimated that in 1995 the total cost to taxpayers and industry for maintaining and protecting classified data was at least $5.6 billion. Nearly 15 years later (in 2011), the cost had doubled, to $11.36 billion but just one year later the Information Security Oversight Office (ISOO) estimated that the 2012 financial costs of maintaining federal government secrets had actually decreased to $10.96 billion, a 13 percent reduction largely attributable to improved reporting requirements that excluded unclassified data management costs. For FY2017, the estimated costs wer $18.39 billion. That figure excluded classification costs for industry, which was estimated at $1.49 billion. I note that ISOO has not published a comprehensive cost report since 2017, and that in the 2021 report to the President, ISOO Director Mark Bradley stated that, "...my staff and I determined that the cost information that we had collected about the CNSI system for years was neither accurate nor reliable."

**FOIA and MDR: A Bifurcated, Dysfunctional Records Release Process**

On a daily basis, if a member of the public or the press seeks federal government records, they have only two pathways to obtain them: FOIA or the Mandatory Declassification Review (MDR) process. FOIA is of course a statute, whereas the MDR process is governed by Executive Order 13526, Classified National Security Information. The very fact that the government has allowed two different—and fundamentally disparate—systems for responding to government records request to exist is our first major clue that the system is dysfunctional.

Under FOIA, if a requester exhausts administrative appeals and the agency or department still refuses to release the material at issue, the requester can sue in federal court. The MDR process precludes litigation.

Under FOIA, entire documents must be released in full unless the agency or department can sustain their burden of proving that one of the nine statutory exemptions covers the information sought. The MDR process only deals with purely classified information (i.e., things that under FOIA would fall under exemptions b1 and/or b3). Thus, requesters seeking records on defense,
intelligence, or law enforcement related activities are almost always better served by using FOIA vice the MDR process.

And despite the fact that EO 13526 mandates declassification reviews at the 25-year point for classified documents, those reviews include nine broadly (and often poorly) worded carveouts that agencies or departments can invoke to deny the release of records. Even ISOO Director Mark Bradley has acknowledged the current MDR system is hopelessly broken.

In ISOO’s 2021 annual report to President Biden, Bradley noted the need to overhaul, if not eliminate, the automatic declassification system currently in use because it “is unable to meet the requirements for existing paper records and will never keep up with the tsunami of digital CNSI [classified national security information] being created daily, making it likely that most of it will never be reviewed for declassification.”

American taxpayers seeking information on what their government is up to in their name should not be forced to navigate a needlessly bifurcated, byzantine federal records request process. The MDR process as it exists should be eliminated. Individual citizen requests for all federal agency and department records should be subject to and processed through a revised and far more user-friendly FOIA statute (about which I will have more to say below).

The costs to taxpayers of needless government secrecy and duplicative records requests and processing structures are measurable not just in dollars and cents, however. The federal government’s frequent misuse of the classification system and FOIA obstructionism to conceal waste, fraud, abuse, mismanagement, or even criminal conduct comes with an even higher cost—public trust and the violation of constitutional rights.

Secrecy and Redaction as Misconduct Shield

For over 50 years and counting, American taxpayers and Congress have learned—most often through whistleblowers—of multiple, devastating examples of federal agency and department misconduct carried out under color of law or regulation in secret.
The first major episode was exposed in January 1970 by former Army Captain Christopher Pyle, who revealed a massive Army domestic spying campaign targeting political dissidents dating from at least 1965.  

Eighteen months later, a group of Philadelphia-area academics and anti-war activists, suspicious that they had been targets of FBI surveillance, broke into the FBI office in Media, Pennsylvania and liberated thousands of FBI reports that confirmed their suspicions. It was the first time that any information on the FBI’s infamous Counterintelligence Program (COINTELPRO) had been made public.  

These episodes led to multiple Congressional investigations between 1971 and 1975, the results of which exposed even more details of Army and FBI domestic surveillance and disruption operations against Americans engaged in First Amendment protected activities, as well as unconstitutional surveillance operations and mail intercepts carried out by NSA and the CIA, respectively.  

Those hearings led to legislation designed to prevent such abuses in the future. The Foreign Intelligence Surveillance Act (FISA), the Inspector General Act, and the creation of dedicated, standing House and Senate intelligence committees were all enacted in the hope that nothing like COINTELPRO or other unconstitutional acts could be perpetrated in the future. While well-intentioned, those reforms have clearly failed.  

Less than four years after the reforms I mentioned were enacted, the FBI once again began a secret, illegal, nationwide criminal predicate-free surveillance operation targeting the Committee in Solidarity with the People of El Salvador (CISPES), which was opposed to Reagan administration policies involving several Central American countries. The operation was eventually exposed and subsequently ended, but no FBI personnel were prosecuted.  

During the Clinton administration, the FBI would again open, in secret, a nationwide investigation without a valid criminal predicate, this one targeting Arab and Muslim Americans in the Chicago area under the code name VULGAR BETRAYAL. One of the reasons the full details on this FBI surveillance scandal remain unclear is because the Bureau has only provided Cato roughly 35,000 of the nearly 1.3 million pages of material it has on the episode.  

Unfortunately, Cato had to abandon that FOIA request. The reason is that since the Bureau will never release more than 500 pages per month to a FOIA requester...
in the D.C. Circuit (absent the very rare order from a federal judge to produce more per month), it would take 215 years for Cato to receive all the records. This is a de facto form of constructive denial of Cato’s request. It also allows the Bureau to continue to hide the magnitude of its misconduct and failures in the VULGAR BETRAYAL episode.

During the Bush 43 presidency, one of the most consequential secret and unconstitutional government surveillance programs of the last 50 years only came to light because of yet another government whistleblower—then-Justice Department attorney Thomas Tamm.

Tamm’s revelations about the STELLAR WIND warrantless mass electronic surveillance program to the New York Times resulted in its exposure in December 2005 and Tamm initially being targeted for prosecution. That threat of jail time—for exposing a completely illegal domestic spying program—hung over Tamm’s head for years, and he nearly lost his law license in the process.19

Later in the Bush 43 administration would come another Army secrecy scandal, this one exposed by then-Army soldier Chelsea Manning. Manning allegedly provided the WikiLeaks organization with secret Army documents implicating Army personnel in war crimes in Iraq, including murder. This was yet another case in which the whistleblower was prosecuted for exposing criminal conduct by the federal government.20

The last in my string of examples of the classification system being used to conceal misconduct by federal agencies and departments involves still another whistleblower—a former NSA contractor by the name of Edward Snowden.

On June 6, it will be 10 years since the Guardian newspaper published Snowden’s first major revelation—the federal government’s programmatic collection of telephone metadata on virtually every American.21 The program made a mockery of the 4th Amendment’s individualized, particularized, probable cause-based warrant requirement. The Executive branch’s reaction to Snowden’s revelations was to once again prosecute a whistleblower for exposing federal government domestic surveillance misconduct.

I note that every time Executive branch officials have claimed that these kinds of surveillance authorities are necessary and effective, subsequent investigation—either by the press, Congress, or civil society groups utilizing FOIA—those claims
have almost invariably been proven false. That was the case with the STELLAR WIND program revealed by Tammm and the PATRIOT Act’s Section 215 telephone metadata program revealed by Snowden. Those are critical facts to bear in mind as the Congress contemplates whether or not to renew the deeply controversial and scandal ridden FISA Section 702 program, set to expire on New Year’s Eve 2023.

The fact that the federal secrecy system has been and continues to be used to conceal Executive branch malfeasance should be seen for what it is: an intolerable pattern and practice that Congress should end via legislative and oversight actions. Yet preventing the abuse of the traditional classification system may not be enough to ensure the kind of government transparency required in a functioning republic. Under then-President Obama, a new effort was initiated to keep even unclassified information from the American people.

**Administrative Control Measures: Controlled Unclassified Information Edition**

Created by Executive Order 13556 on November 4, 2010, the ostensible purpose of establishing the "Controlled Unclassified Information" program was to mandate "an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended."  

As one recent commentator has observed:

> The idea behind CUI was initially a good one: eliminate the alphabet soup of FOUO [For Official Use Only] and related designators being applied to unclassified documents by different agencies and unify everything under one label. Unfortunately, the same bureaucracy that gave us the widely known over-classification problem quickly got its teeth into the fledgling CUI program. Now, we have yet another unwieldy system that some critics argue is being used primarily to hide information from public scrutiny.  

In preparation for this hearing, I searched in vain for a credible contemporary explanation as to why, in 2010, the existing exemptions under the FOIA and the Privacy Act (PA) were somehow deemed to be inadequate to protect things like
the names of non-public federal employees, their Social Security numbers, clearance status, etc. I found none.

What’s more, there has never been a Government Accountability Office (GAO) examination of the rationale for the CUI program, whether existing FOIA & PA exemptions are somehow inadequate to protect potentially sensitive but unclassified information, and whether much of the information under the CUI umbrellas is not already in the public domain.

And we already have a prominent example of an attempt to use the CUI designator to keep the public in the dark about a very recent, and deadly, incident: the August 29, 2021, U.S. drone strike on Kabul, Afghanistan that killed 10 civilians, including seven children.26

A subsequent New York Times FOIA lawsuit revealed that the CUI designator had been used on a document listing 24 key pieces of documentary and related evidence about the strike, which the Pentagon initially defended but later acknowledged was a "tragic mistake."27

It’s worth noting that this and the many other episodes I’ve described thus far have been exposed only because certain specific, well-resourced institutions in our society (be it the New York Times, a prominent think tank like Cato, or a large, well-financed civil liberties group like the ACLU) have been willing to litigate in court and slug it out for the documents. What about the average requester without access to qualified FOIA counsel seeking records on a still-embarrassing-to-the-government but not-in-the-headlines issue?

**A Classification and Records Management Reform Proposal**

The massive request backlogs at federal agencies and departments have only grown worse over the past decade, with more than 150,000 backlogged requests in 2021 alone, and a third of those belonged to the department charged with implementing FOIA: the Justice Department.28

The FOIA and MDR model of handling individual requests is not working. We need a new statutory framework that, while still allowing and encouraging individual requests,
1) mandates disclosure of all federal agency and department records 25 years old or older within five years of enactment and continue such disclosures annually henceforth;

2) disallows the release of information that would:

   A) constitute a clearly unwarranted invasion of personal privacy of a living, natural United States Person (defined as a U.S. citizen or alien admitted for permanent residence);

   B) reveal the identity of a current confidential human source (herein defined as a source that has provided verified information on potential or actual criminal activity or of foreign intelligence value within the last five calendar years), or reveal information about the application of a current intelligence source or method not previously publicly acknowledged or revealed in court proceedings, or reveal the identity of a current human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably place the health or life of that source in imminent danger, States Person (defined as a U.S. citizen or alien admitted for permanent residence);

   C) reveal the workings of a current cryptologic system in use by the United States government or by a government of foreign intelligence interest to the United States;

   D) reveal information on a state-of-the-art technology within a United States weapon system;

   E) reveal actual United States military war plans that remain in effect;

   F) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

   G) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;
I) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

J) violate a treaty or international agreement.

3) In no event would any information covered under subsections A through J be withheld from public release if the records in question reveal evidence of waste, fraud, abuse, mismanagement, violation of any statute or provision of the Constitution by a United States government official or contractor.

4) In all cases in which a plaintiff brings a civil action against a federal agency or department under the Freedom of Information Act involving any of the records covered under subsections A through J of this Act, the presiding judge shall conduct an in camera de novo review of the records at issue with the assistance of a Special Master with appropriate security clearances and in the employ of the Court.

Administrative control measures like CUI, SBU, etc. should be expressly prohibited. Information is either classified because it is a genuine secret (i.e., not in the public domain and its exposure would jeopardize one of the interests covered by subsections A through J, above) or it is not.

The revamped system I am proposing would not only ensure historically valuable documents are released expeditiously and on a fixed schedule, it would also ensure that more contemporary national security and law enforcement records of potentially major public significance are not forever kept secret because a federal judge believes he or she must show "due deference" to Executive branch claims of secrecy. At the same time, my proposed framework would give federal agencies and departments the legal basis to protect genuine secrets from untimely exposure.

I thank the committee for its time and attention, and I look forward to your questions.

---

5 PL 86-36, 1959.
7 Available online at the National Archives website at https://www.archives.gov/ooia/policy-documents/cnsi-
eo.html.
9 National Archives Information Security Oversight Office 2011 Report to The President: Cost Estimates for Security
   Classification Activities, p. 2.
10 ISOO letter to the President transmitting its FY 2012 report, June 20, 2013.
11 ISOO Annual report to the President for 2017, p. 4.
12 ISOO Annual report to the President for 2021, p. 11.
13 Ibid., p. 5.
15 For the best account on this episode, see Betty Medsger, The Burglary: The Discovery of J. Edgar Hoover’s Secret
16 The most sweeping of these investigations was carried out by the Senate committee led by the late Senator
   Frank Church (D-ID). See Senate Select Committee to Study Governmental Operations with Respect to Intelligence
17 See The FBI and CISPES, Report of the Select Committee on Intelligence together with Additional Views, S. Prt.
20 See Patrick G. Eddington, “Assange Espionage Indictment: Classified Hypocrisy and a Prosecutorial Trojan Horse,”
   Inside Sources, June 2, 2019.
21 Glenn Greenwald, “NSA collecting phone records of millions of Verizon customers daily,” The Guardian, June 6,
   2013 (online edition).
   April 24, 2015, p. A12.
23 Spencer Ackerman and Paul Lewis, “US senators rail against intelligence disclosures over NSA practices,” The
26 Charlie Savage, Erich Schnitt, Amat Khan, Evan Hill and Christoph Koetti, "Newly Declassified Video Shows U.S.
27 "Read U.S. Central Command’s Investigation Into Botched Aug. 29, 2021 Kabul Drone Strike,” New York Times,
   January 6, 2023 (online edition).
April 7, 2023

The Honorable Gary C. Peters  The Honorable Rand Paul
Chairman Ranking Member
Committee on Homeland Security and Committee on Homeland Security and
Governmental Affairs Governmental Affairs
340 Dirksen Senate Office Building 442 Hart Senate Office Building
United States Senate United States Senate
Washington, DC 20510 Washington, DC 20510

Dear Chairman Peters and Ranking Member Paul,

We want to thank you for convening the recent hearing on the federal government’s
declassification system. It was made clear from the witness testimony and questions from
committee members that the current system is dysfunctional and there is bipartisan support for
extensive reforms.

The National Coalition for History (NCH) is a consortium of 43 organizations that advocates and
educates on federal legislative and regulatory issues affecting historians, archivists, researchers,
educators, students, documentary editors, preservationists, genealogists, political scientists,
museum professionals and others. Many of our members rely heavily on the declassification of
federal records in their work.

We would like to submit for the record recommendations prepared by one of our member
organizations, the Society for Historians of American Foreign Relations (SHAFR), on reforming
the declassification process. NCH has endorsed the statement.

We appreciate this opportunity to submit these recommendations and offer our assistance as you
craft these reforms.

Sincerely,

Lee White
Executive Director
National Coalition for History
The continued classification of so many historical records held by the U.S. government has created a major crisis of government accountability. Declassification is currently a series of autonomous fields, operating by their own agency instructions rather than by a government-wide policy. The result has become chaos. The U.S. National Archives and Records Administration (NARA) has jurisdiction over millions of pages of classified presidential and federal agency records dating back to the early years of the Cold War, yet it lacks authority to declassify them. NARA has centralized control of the classified presidential records but no known plans to initiate their systematic declassification review.

President Barack Obama established NARA’s National Declassification Center (NDC) in 2009 to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training for declassification of records. It is routinely deluged with huge numbers of classified records (both paper and electronic) transferred whose processing it must balance with a backlog of thousands of declassification requests for specific records. It lacks both the resources and the authority to take timely action on any of these responsibilities. Moreover, complicated coordination requirements delay timely action on Freedom of Information Act (FOIA) and Mandatory Declassification Review (MDR) requests.

The Executive Order (E.O.) on national security information policy that President Obama signed in 2009 is long out of date, and its language gives undue scope to the agencies to overclassify and even block declassification of historical records. The Department of Defense can unilaterally withhold from declassification historical records that are 50 years old or older on the grounds that declassification will hurt U.S. diplomatic relations with another country.

The Interagency Security Declassification Panel (ISCAP) makes important decisions on final MDR appeals, and it also has a tremendous backlog of cases. Its decisions reflect careful deliberations and have important implications. But ISCAP, too, confronts a tremendous backlog of cases. Further, its decisions do not become precedents that could inform and facilitate future declassifications by the agencies.

Moreover, rules governing Formerly Restricted Data under the Atomic Energy Act enable the Department of Defense and the Department of Energy to preserve the classified status of overseas deployments of nuclear weapons from the earliest days of the Cold War. Presently, the NDC and ISCAP lack the technology they need to share declassified documents with agencies; instead of e-mailing them they must use compact discs or couriers. In addition they lack the technology to hold classified online meetings with other agencies. To a great extent this is a
NARA budget issue outside of the scope of the Executive Order, but an E.O. should include
hortatory language to encourage NARA to make improvements and initiate necessary action.

RECOMMENDATIONS

To address these shortcomings of current declassification policy, a revised Executive Order
should include arrangements to expedite the release of classified historical records and to provide
ground rules to help agencies prepare for transferring their records to NARA. For the purpose of
achieving these goals, SHAFR supports the following improvements in the Executive Order:

• To reduce future backlogs, the E.O. should establish a “drop dead” date for automatic
declassification of records over 30 years old. Exceptions should be limited and expressed
explicitly and narrowly. The burden should be placed on the agencies to justify withholding a
record from automatic declassification.

• The agencies should expedite automatic declassification so that it minimizes the need for
the public to file FOIA or MDR requests. Any exemptions from automatic declassification will
require the approval of the National Security Advisor to the President and should be made
publicly available.

• The National Declassification Center must be vested with the authority to declassify
information subject to automatic declassification without having to refer the records back to the
originating agency. The NDC must be authorized to make decisions on MDR and FOIA appeals
involving NARA records. Toward this end, included on the NDC staff should be representatives
from all agencies that generate classified documents. Collaboration between these
representatives and NARA personnel should enable the NDC to make decisions on the spot.

• ISCAP decisions should be incorporated into agency declassification guidance. This
incorporation must be mandatory.

• The Departments of Energy and Defense should be required to begin reviewing Formerly
Restricted Data and converting and redefining it either as Restricted Data or as national security
information. This is necessary to differentiate information about historical locations of nuclear
weapons that should be treated differently than technical information about nuclear weapon use.

• The use of the foreign relations exemption (exemption 6) by agencies and offices other
than the State Department and National Security Council should be limited by requiring them to
seek the Department’s approval before applying it to archival documents. This procedure will
prevent abuse of the exemption in declassification decisions on historical records.

• NARA should be directed to initiate the systematic review of classified presidential
records, potentially modeled after the CIA’s former Remote Archives Capture (RAC) program.
• NARA should receive sufficient resources to build up staff support for NDC and ISCAP staff and to secure up-to-date technology so that the NDC and ISCAP can better share classified information with other agencies.

• A specific procedure must be formulated for the public to seek declassification of properly classified information that is of high public interest along the lines proposed by the Federation of American Scientists. This calls for a procedure to allow the public to request declassification of properly classified records from an entity other than the original classification authority (OCA), similar to ISCAP.

• Along these lines, OCA must be given the option not to classify information in cases where the public interest outweighs the potential harm from disclosure. OCA must also be granted the discretion to declassify information that has been the subject of unauthorized disclosure.

• Because the effectiveness of these recommendations requires oversight with the authority to implement its decisions, the Executive Order must designate an executive agent to oversee declassification policy, standardize procedures, and review and approve agency guidelines. The logical source for the executive agent is the Information Security Oversight Office (ISOO) or the Office of the Director of National Intelligence (ODNI).