AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

EXAMINING THE COSTS OF OVERCLASSIFICATION ON TRANSPARENCY AND SECURITY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

DECEMBER 7, 2016

Serial No. 114–174

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

26–177 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
ANDREW DOCKHAM, *General Counsel*
KATHY ROTHER, *Senior Counsel*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on December 7, 2016	1

WITNESSES

Mr. J. William Leonard, Former Director, Information Security Oversight Office	
Oral Statement	5
Written Statement	8
Mr. Steven Aftergood, Director, Project on Government Secrecy, Federation of American Scientists	
Oral Statement	47
Written Statement	49
Mr. Tom Blanton, Director, National Security Archive, The George Washington University	
Oral Statement	57
Written Statement	59
Mr. Scott Amey, General Counsel, Project on Government Oversight	
Oral Statement	69
Written Statement	71

APPENDIX

2015 Report to the President ISOO-National Archives submitted by Mr. Chaffetz can be found here: *https://www.archives.gov/files/isoo/reports/2015-annual-report.pdf*

EXAMINING THE COSTS OF OVERCLASSIFICATION ON TRANSPARENCY AND SECURITY

Wednesday, December 7, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The committee met, pursuant to call, at 9:00 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Duncan, Jordan, Walberg, Amash, Farenthold, Massie, Meadows, DeSantis, Mulvaney, Buck, Walker, Hice, Russell, Carter, Grothman, Hurd, Palmer, Cummings, Maloney, Clay, Lynch, Connolly, Kelly, Lawrence, Watson Coleman, Plaskett, DeSaulnier, Welch, and Lujan Grisham.

Chairman CHAFFETZ. Good morning. The Committee on Oversight and Government Reform will come to order.

And, without objection, the chair is authorized to declare a recess at any time.

We have an important hearing this morning: "Examining the Costs of Overclassification on Transparency and Security." Sunlight is said to be the best disinfectant, and without knowing what our government is doing, we can't ensure it is operating efficiently and effectively. It is also important to remember that the American people pay for the Federal Government. The Federal Government works for the American people. It is not the other way around, and so it is, you would think, logical to make sure that we are as open and transparent and accessible as possible, but this is always a running battle. We always have to find the proper balance between safety and security and openness and transparency, but we can't give up all of our liberties in the name of security. And so we have this hearing today with four experts, people who have poured their time, effort, talent, their careers really, into this topic. There is a wealth of information that they are going to share with us, and that is what we are excited to hear about today.

Without knowing what our government is doing, we can't ensure it is operating efficiently and effectively, as I said. Transparency is the basis ultimately for accountability. At the same time, transparency into certain government activities can create an opportunity for those who wish to do us harm, and so Congress gives some agencies the authority to withhold certain information from public disclosure. This authority to classify information and create secrets is needed to protect our national security. I don't think anybody doubts that there should be a degree of this. The question is

what degree of this. But when you give the authority to classify certain information, Congress has a role to play in making sure that authority is being properly excercised.

Overclassification of information has become a concern. Estimates range from 50 to 90 percent of classified material is not properly labeled. In the 1990s, Congress established the Commission on Protecting and Reducing Government Secrecy to study those issues and develop recommendations. In 1997, the Commission issued a final report, including 16 recommendations. Three of those recommendations were implemented. Seven were partially implemented, and six remain open today. The Chairman of the Commission, the late Senator Patrick Moynihan, wrote, and I quote: "If the present report is to serve any large purpose, it is to introduce the public to the thought that secrecy is a mode of regulation. In truth, it is the ultimate mode for the citizen does not even know that he or she is being regulated," end quote.

Patrick Moynihan, hats off to him and his leadership in understanding and really helping to champion this effort to move forward and really examine the degree of which secrecy is needed in our Nation.

Here we don't even know what can hurt us. As the tendency to overclassify information goes, so does the lack of accountability to both Congress and the American taxpayer. The Commission also warned about the dangers of restricting information from those who actually do need it. Looking back, that point seems almost prophetic in light of the events that would unfold on September 11, 2001.

After conducting an exhaustive study of the attacks, the 9/11 Commission issued its own report that found we need to move forward from a system of need-to-know to a culture of need-to-share. What we have learned is that overclassification can also be damaging to national security, or at a minimum, it can lead to second guessing what might have been if we were only able to get the information in the right hands at the right time.

According to a report by the Information Security Oversight Office at the National Archives, in the last 10 years, the Federal Government has spent more than $100 billion on security classification activities. In fact, I would ask unanimous consent to enter that report into the record.

Without objection, so ordered.

Chairman CHAFFETZ. Last year alone, classification is estimated to have cost $16 billion. It is unclear what exactly the taxpayers got in return for this expense. There was presumably some level of greater security as a result of restricting access to certain information. Again, no doubt that there needs to be classification that needs to be implicated, but at what level? This leads us to a number of basic questions. Does the billions of dollars spent to classify make us safer? How much money did we spend on security clearances for folks who probably didn't need them in the first place?

Earlier this week, the Washington Post reported the Department of Defense found $125 billion in savings over 5 years by simply streamlining bureaucracy—$125 billion. To give you an idea, the entire State of Utah, everything we do in Utah—it is a smaller State, granted—but everything we do, from education to the Na-

tional Guard to roads and paying teachers, is about $14 billion. And here at the Department of Defense, 5 years' savings, $125 billion, by simply streamlining bureaucracy.

The Department of Defense was sufficiently embarrassed by this, as they should be, and decided to bury the study, but trust me: we are going to look into this. According to the article, quote, "The Pentagon imposed secrecy restrictions on the data, which ensured that no one could replicate the findings," end quote. Not what we should be doing as a Nation. It is a prime example of why we are holding this hearing today. And when agencies have a tool to keep information from the public, Congress must ensure those tools aren't used for nefarious reasons.

I look forward to discussing those issues with the witnesses today. I thank the panel of experts for coming before the committee to help us better understand some of the complexities of the government secrecy. I think you will find that Congress, in particular this committee, has a keen interest on this. The committee has been has been a leader and a champion of the Freedom of Information Act, one of the tools that is important for the American public to understand what their government—their government is supposed to be working for them—is actually doing. So I look forward to this discussion.

Somebody I know who holds an equal passion for this is my colleague, Elijah Cummings, the ranking member, from Maryland, and I would like to recognize him for his opening statement.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Thank you very much for holding this hearing. Government transparency is a bipartisan issue. Over multiple sessions of Congress, our committee has made significant progress in making the Federal Government more open and accountable. We do this best when we work together.

During this Congress, we worked together to strengthen the Freedom of Information Act, and those amendments were signed into law by President Obama in June. Just this past Monday, we sent another bill to the White House to strengthen protections for employees working for contractors and grantees who blow the whistle on waste, fraud, and abuse.

We now have the opportunity to work together to address the flaws in our classification system. Over the past several years, our committee has conducted multiple investigations, including our review of Secretary Clinton's emails, that exposed serious flaws in our classification system. We have seen agencies disagree with each other on whether an email was classified. We have seen information that began unclassified later being retroactively classified. We have seen documents that were not properly marked as classified. And we have seen documents that were classified after they had already been publicly released. And, first and foremost, I believe that we in Congress should exercise our authority to improve the classification system and make government information more transparent. We can conduct oversight, such as these hearings, and we can investigate specific allegations of security breaches and unwarranted government secrecy. Congress can also legislate them. We can pass reforms that actually address the problems we will hear about today.

Twenty years ago, the Moynihan Commission provided a roadmap to improving the classification system. But too little has been done since that report was issued. For example, the Commission recommended that Congress enact a statute establishing the principles of classification, but Congress still has not taken that step. The fundamental purpose underlying all of our efforts today is to provide the American people with more information, especially when it impacts our national security. Our operating premise is that a better informed electorate leads to a better-functioning government on behalf of all of the American people.

Mr. Chairman, I thank you for calling today's critical hearing, but there is another national security area that I believe the American people should have much more information about from their government.

On November 17, 2016, I wrote a letter to the chairman requesting that our committee conduct a bipartisan investigation into Russia's role into interfering with and influencing the 2016 Presidential election. I specifically requested that we receive a classified briefing from the intelligence community. Today, nearly 3 weeks have now gone by. I have received no response, and the committee has taken no action.

Now, Mr. Chairman, I know you have said that you do not want to do any oversight relating to President-elect Donald Trump until he is sworn into office, and I can understand that. But these attacks on our country have already happened. It already happened. This is not something of a future threat. This has already been done. And unless we act, it may very well happen again. For these reasons, yesterday, I joined Democratic whip, Steny Hoyer, and ranking members of the Committees on Armed Services, Homeland Security, Intelligence, Judiciary, and Foreign Affairs, and we did ourselves what this committee did not. We sent a letter to the President requesting that all Members, that all of us, all Members of Congress, Democrats and Republicans, be provided the opportunity to receive a classified briefing by the intelligence community with the most up-to-date information on this issue.

This is not a partisan issue, and it should not be. Republican Senator Lindsey Graham has called for this type of investigation in the Senate, essentially saying that Republicans should not sit on the sidelines and let allegations about foreign governments interfering in our election go unanswered just because it may have been beneficial to them in this instance. Republican Senator Marco Rubio put it even more bluntly saying, quote: "Today, it is the Democrats. Tomorrow, it could be us," end of quote.

The bottom line is that this is not a Democratic issue, and it is not a Republican issue. This is an American issue. Elections are a core American value and are central to our democracy, and any foreign interference with our elections should be of the greatest concern to every single Member of this Congress. The American people deserve as much information as possible about these threats and the actions their government is taking to address them. As I say to my constituents over and over again in the last election and during these times, this is bigger than Hillary Clinton. This is bigger than Donald Trump. This is about a struggle for the soul of our democracy, and so it is our job to ensure that we get this kind of in-

formation since it is our duty to make sure that our democracy stands strong and that our children's children can have a democracy just as strong as the one that we have experienced.

And, with that, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We will hold the record open for 5 legislative days for any members who would like to submit a written statement.

I will now recognize our panel of witnesses. I am pleased to welcome Mr. J. William Leonard, former Director of the Information Security Oversight Office; Mr. Steven Aftergood, director of the Project on Government Secrecy at the Federation of American Scientists; Mr. Tom Blanton, director of the National Security Archive at the George Washington University; and Mr. Scott—is it Amey?

Mr. AMEY. Yes, sir.

Chairman CHAFFETZ. I just want to make sure I pronounce that properly. Mr. Scott Amey, general counsel for the Project on Government Oversight.

We welcome you and thank you for being here.

Pursuant to committee rules, all witnesses are to be sworn in before they testify. If you will please rise and raise your right hand.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. You may be seated.

Let the record reflect that all witnesses answered in the affirmative. In order to allow time for discussion, we would appreciate your limiting your verbal comments to no greater than 5 minutes so members can have ample time to ask questions. Your entire written statement and extraneous materials will be entered into the record.

Mr. Leonard, you are now recognized for 5 minutes. And the microphones in this committee, you have got to straighten them up and put them right up uncomfortably close. Thank you.

WITNESS STATEMENTS

STATEMENT OF J. WILLIAM LEONARD

Mr. LEONARD. Thank you, Mr. Chairman, Mr. Cummings, members of the committee. I appreciate the opportunity to attend this meeting this morning. The ability and authority to classify national security information is a critical tool of the Federal Government and its leaders to protect our Nation and its citizens. However, when negligently or recklessly applied, overclassification of information can undermine the very integrity of the classification system and also create needless impediments to transparency that can undermine our form of government and its constitutional system of checks and balances.

I have come to the conclusion that, on its own, the executive branch is both incapable and unwilling to achieve true reform in this area. Incapable in that, absent external pressure from either the legislative or judiciary branches of our government, true reform within the executive branch when the matter involves the equities of multiple agencies can only be achieved with the direct leadership emanating from the White House.

Over the past 40 years, we have seen only one White House-led attempt at classification reform, and that was in the 1990s. Bureaucracy's response to those attempts at reform were typical—delay and foot drag—because agency officials know that, sooner or later, every administration eventually goes away, providing opportunities for rollback.

With respect to the executive branch's unwillingness to implement real classification reform, I believe it is unreasonable to expect it to do so primarily since the unconstrained ability to classify information is such an attractive tool for any administration to facilitate implementation of its national security agenda. In this regard, especially in the years since 9/11, we have seen successive administrations lay claim to new and novel authorities and to often wrap these claims in classification. This can amount to unchecked executive power. While the President must have the ability to interpret and define the constitutional authority of the office and at times to act unilaterally, the limits of the President's authority to act unilaterally are defined by the willingness and the ability of Congress and the courts to constrain them.

Of course, before the Congress or the courts can constrain Presidential claims to inherent unilateral powers, they must first be aware of those claims. Yet a long recognized power of the President is to classify and thus restrict the dissemination of information in the interest of national security, to include access by Congress or the courts. The combination of these two powers, that is when the President lays claim to inherent powers to act unilaterally but does so in secret, can equate to the very open-ended noncircumscribed executive authority that the Constitution's Framers sought to avoid in constructing a system of checks and balances.

Thus, absent ongoing congressional oversight or judicial review of executive assertions of classification, no one should ever be surprised that the authority to class information is routinely abused in matters both big and small.

I have attached to my formal statement specific examples of classification abuse relating to three criminal cases in which the prosecution ultimately did not prevail in large part due to government overreach in its claims that certain information was classified. In each of these cases, the government abused the classification system and used it for other than its intended purpose.

I believe that there are steps that Congress can take in order to address this matter. The first deals with enforcing accountability. Over the past several decades, a significant number of individuals have rightly been held accountable for improperly handling classified information. To my knowledge, during the same period, no one has ever been held accountable and subjected to sanctions for abusing the system and for improperly classifying information, despite the fact that the President's executive order governing this authority treats unauthorized disclosures of classified information and inappropriate classification of information as equal violations of the order, subjecting perpetrators to comparable sanctions. Absent real accountability, it is no surprise that overclassification occurs with impunity.

A second area worthy of possible legislative attention is that of providing a mechanism for routine, independent expert review of

agency classification decisions, especially as a tool to be made available to the executive's two coequal branches of government when exercising congressional oversight or judicial action and to which they could come to their own independent judgment as to the appropriateness of executive assertions of classification. Traditionally, both Congress and the courts are understandably deferential to such assertions. Nonetheless, when applying the controls of classification, government officials are obligated to follow the standards set forth by the President and not exceed the governing orders, prohibitions, and limitations.

Thus, it is not only possible but entirely appropriate to conduct a standards-based review of classification decisions. I have attached to my formal statement one potential methodology for such reviews.

I applaud this committee for focusing on this critical topic to our Nation's well-being, and I thank you for inviting me here today, Mr. Chairman. I will be happy to answer any questions you or other committee members might have.

[Prepared statement of Mr. Leonard follows:]

FORMAL STATEMENT

J. William Leonard

Former Director, Information Security Oversight Office

before the Committee on Oversight and Government Reform

U.S. House of Representatives

"Examining the Costs of Overclassification on Transparency and Security"

December 7, 2016

Chairman Chaffetz, Mr. Cummings, and members of the Committee, I want to thank you for holding this hearing on the costs of overclassification on transparency and security and for giving me the opportunity to testify. The ability and authority to classify national security information is a critical tool at the disposal of the federal government and its leaders to protect our nation and its citizens. However, when negligently or recklessly applied, overclassification of information can undermine the very integrity of the system we depend upon to ensure that our nation's adversaries cannot use national security-related information to harm us and can place at increased risk truly sensitive information. Overclassification also creates needless impediments to transparency that can actually undermine our form of government and the constitutional system of checks and balances intended to preclude, among other objectives, overreach by the executive branch.

I have over 40 years of experience in dealing with classified national security information. This includes overseeing the implementation of the president's executive order governing the classification of information within the Department of Defense (DoD) as a Deputy Assistant Secretary in the Clinton and Bush administrations and within the entire executive branch as Director of the Information Security Oversight Office in the Bush administration. As a result of this experience I have come to the conclusion that on its own, the executive branch is both incapable and unwilling to achieve true reform in this area. I also believe it is unreasonable to expect it to do so.

With respect to the executive branch's incapability to achieve self-reform in this area, I believe most observers would agree that absent external pressure from either the legislative or judiciary branches of our government, true reform within the executive branch when the matter involves the equities of multiple agencies can only be achieved with direct leadership emanating from the White House at the most senior level. Over the last 40 years, we have seen only one White House-led attempt at classification reform and that was in the 1990's during the Clinton administration. Having been involved in the process during that period, I can assure you that the bureaucracy's response to these attempts at reform were typical. Specifically, delay and foot-drag because agency officials know that sooner or later every administration eventually goes

away, a reality that will provide new opportunities to rollback attempts at reform. I know of this because I was a part of the bureaucracy at that time and was involved in the subsequent classification reform rollbacks that occurred during the Bush administration. As a DoD official I participated in this pushback effort. There were a number of classification reform issues that were problematic for the department, especially from a budgetary perspective. Other agencies, such as the CIA, had different issues that were troublesome for them. Thus, absent White House leadership, the interagency process is reduced to mere consensus and the process becomes one of horse-trading and logrolling. The outcome is thus inevitably reduced to the lowest common denominator among multiple agencies with differing imperatives. When I became ISOO Director and in my new role attempted to resist further rollback efforts, my effectiveness in doing so was likewise hampered absent strong White House support.

With respect to the executive branch's unwillingness to implement real classification reform, I believe it is unreasonable to expect it to do so, primarily since the unconstrained ability to classify information is such an attractive tool for any administration in order facilitate implementation of its national security agenda. In this regard, especially in the years since 9-11, we have seen successive administrations lay claim to new and novel authorities, and to often wrap these claims in classification. This can amount to unchecked executive power. I acknowledge that it has long been recognized that the president must have the ability to interpret and define the constitutional authority of the office and, at times, to act unilaterally. However, the limits of the president's authority to act unilaterally are defined by the willingness and ability of Congress and the courts to constrain it. Of course, before the Congress or the courts can act to constrain presidential claims to inherent unilateral powers, they must first be aware of those claims. Yet, a long recognized power of the president is to classify and thus restrict the dissemination of information in the interest of national security – to include access to certain information by Congress or the courts. The combination of these two powers of the president – that is, when the president lays claim to inherent powers to act unilaterally, but does so in secret – can equate to the very open-ended, non-circumscribed, executive authority that the Constitution's framers sought to avoid in constructing a system of checks and balances.

Thus, absent ongoing congressional oversight or judicial review of executive assertions of the need to restrict the dissemination of information in the interest of national security, no one should ever be surprised that the authority to classify information ends up being routinely abused, either deliberately or not, in matters both big and small. For example, over the years I have seen agencies improperly deny information in response to access demands under the auspices of either the Freedom of Information Act (FOIA) or the executive order governing the declassification of information. Even more disturbing is when agencies abuse the classification system in order to attain unfair advantage against a fellow citizen.

In the years since my retirement from public service, I have personally been involved as a pro bono expert for the defense in three criminal cases in which the prosecution ultimately did not prevail in large part due to government-overreach in its claims that certain information was classified. In these instances I made it clear to defense counsel that I would become involved in their case not as an advocate for the defendant but rather as an advocate for the integrity of the classification system, which I saw being undermined by the government's own actions. In each of these cases – *U.S. v. Rosen, U.S. v. Drake*, and the special court-martial of a former Marine

Captain who faced charges arising out of an operation in Afghanistan during which four Marines were videoed urinating on enemy corpses – the government abused the classification system and used it not for its intended purpose of denying sensitive information to our nation's enemies but rather as leverage to carry out an entirely different agenda. The opaque nature of the classification system can give the government a unilateral and almost insurmountable advantage when it is engaged in an adversary encounter with one of its own citizens, an advantage that is just too tempting for many government officials to resist.

I have attached to this statement a number of documents that provide greater detail for each of the above cases. Included as attachment 2b is a copy of the actual email from the Drake case that the government asserted had been properly classified and, in fact, served as the first count of its felony indictment and for which the government was prepared to send Mr. Drake to prison for up to 35 years. There was no doubt in my mind that had this matter gone to trial, I would have been able to convince a jury of Mr. Drake's peers that they could use their own common sense and judgment in coming to the conclusion that the information contained therein did not meet the government's own standards for classification.

In the face of this long history of failure by the executive branch to effectively deal with the issue of overclassification I believe there are steps that the Congress can and should take in order to address this matter, an issue that this committee aptly points out impacts both transparency and security. This morning I'd like to focus on two such steps.

The first is the issue of accountability. Over the past several decades, tens of millions of individuals have been afforded access to classified information. Although comparably small, the number of individuals during this same period who have been rightly held accountable for improperly handling, possessing or disclosing classified information is nonetheless significant. Many have been subject to criminal sanctions, countless others to administrative sanctions. During this same period, the number of individuals who have been held accountable for improperly classifying information or otherwise abusing the classification system is likewise countless. However, in the latter instance, the number is countless because to my knowledge no one has ever been held accountable and subjected to sanctions for abusing the classification system or for improperly classifying information. This is despite the fact that the president's executive order governing the classification of information treats unauthorized disclosures of classified information and inappropriate classification of information, whether knowing, willful, or negligent, as equal violations of the order subjecting perpetrators to comparable sanctions, to include "reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation."[1]

---

[1] Sec. 5.5, E.O. 13526, "Classified National Security Information Memorandum."
[2] "Audit Report – Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes," April 26, 2006. See: https://fas.org/sgp/isoo/audit042606.pdf
[3] Sec. 5.3, E.O. 13526, op. cit.
[4] Ibid, Sec. 3.5.
[5] ISOO "2015 Report to the President," p. 28. See: https://fas.org/sgp/isoo/2015rpt.pdf
[6] Ibid.
[7] Section 311 of the Intelligence Authorization Act for Fiscal Year 2014, Section 365 of the Intelligence Authorization Act for Fiscal Year 2010, Section 2 of the Public Interest Declassification Board Reauthorization Act of 2012, Section 602 of the Implementing

Thus, although intended as a safeguard against overclassification and abuse of the classification system, this provision of the current and prior president's orders governing classification has proven over the decades to be utterly feckless. As such, it is no surprise that overclassification occurs with impunity. From the perspective of the typical individual with a clearance, such an outcome is understandable. Everyone with a clearance knows that if he or she improperly discloses or otherwise mishandles information that should be classified, even inadvertently, he or she will be subject to sanction, perhaps even to criminal penalties. However, cleared individuals likewise know if they overclassify information, whether willfully or negligently, there will most likely be no personal consequences. Given this disparity, its no wonder that the attitude "when in doubt, classify" prevails, not withstanding any admonition to the contrary. The proven lack of accountability in this regard within the executive branch is one area worthy of legislative attention.

Another area worthy of possible legislative attention is that of providing a mechanism for independent expert review of agency classification decisions; especially as a potential tool to be made available to the executive's two coequal branches of government when exercising congressional oversight and judicial action. Both Congress and the courts are frequently overly deferential to assertions of classification by the executive branch. This is understandable since there is often an unwillingness to override the judgment of executive branch subject matter experts. Furthermore, since the order governing classification is permissive and not prescriptive, the decision to originally classify information is ultimately one of discretion – the order clearly states what **can** be classified, not what **must** be classified. Nonetheless, it is also important to note that when deciding to apply the controls of the classification system to information, government officials are in-turn obligated to follow the standards set forth by the president and not exceed the governing order's prohibitions and limitations. Thus, it is not only possible but also entirely appropriate to conduct a standards-based review of classification decisions, one that does not necessarily second-guess the discretion of an original classification authority. I have attached to this statement (Attachment 4) an updated methodology for such a review that I had originally developed when I was the ISOO director. This standards-based methodology can be employed to evaluate the appropriateness of classification decisions, both original and derivative. A fundamental point of this methodology is that agencies cannot simply assert classification; they must be able to demonstrate that they have adhered to the governing order's standards. Most notable is the need to be able to identify or describe the damage to national security that could be expected in the event of unauthorized disclosure, a standard that the government failed meet in the Drake case as evidenced by the government's own declarations included at Attachment 2.

It is worthy of note that when independent review of agency classification decisions does occur, the results clearly highlight the extent of rampant overclassification within the executive branch. For example, when I was at ISOO, I oversaw the audit[2] of all re-review efforts undertaken by a number of agencies in their belief that certain records at the National Archives and Records Administration (NARA) had not been properly reviewed for declassification, but had been made available to the public. The audit found that these agency efforts resulted in the withdrawal of at

[2] "Audit Report – Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes," April 26, 2006. See: https://fas.org/sgp/isoo/audit042606.pdf

least 25,315 publicly available records. In reviewing a sample of the withdrawn records, the audit concluded that nearly one third of the sampled records did not, in fact, contain information that clearly met the standards for continued classification. What this meant is that even trained classifiers, with ready access to the latest classification and declassification guides, and trained in their use, got it clearly right only two thirds of the time in making determinations as to the appropriateness of continued classification. This is emblematic of the challenge confronting the millions of cleared individuals who are confronted daily with the ability to label information as being classified.

Equally revealing are the actions of the president's own Interagency Security Classification Appeals Panel (ISCAP). The President created the ISCAP by executive order in 1995 in order to, among other functions, decide on appeals by persons who have filed classification challenges under the governing order. It is also responsible to decide on appeals of agency decisions by persons or entities such as researchers, the media and other members of the public who have filed requests for mandatory declassification review (MDR) under the governing order[3]. The permanent membership is comprised of senior-level representatives appointed by the Secretaries of State and Defense, the Attorney General, the Director of National Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs. The President selects the Chairperson. I served as both the DoD member of this panel in the early 2000's and as its Executive Secretary from 2002-2007.

Under the governing order, the MDR process requires a review of specific classified national security information in response to a request seeking its declassification[4]. The public must make MDR requests in writing and each request must contain sufficient specificity describing the record to allow an agency to locate the record with a reasonable amount of effort. Agencies must also provide a means for administratively appealing a denial of a mandatory review request. MDR remains popular with some researchers as a less litigious alternative to requests under FOIA. It is also used to seek the declassification of Presidential papers or records not subject to FOIA.

After being denied both the initial request and an appeal to the agency itself, requestors have the further ability to appeal to the ISCAP. Particularly noteworthy is that in FY 2015 (the most recent year for which data is available) agency decisions to retain the classified status of requested information were overridden by the panel, either entirely or in part, 92% of the time[5]. Since the ISCAP's initial decision in 1996 through the end of FY15, agency decisions to retain the classified status of requested information has been overridden by the panel, either in whole or in part, 75% of the time[6]. I believe these numbers speak for themselves. In essence, even when specifically asked to review information in order to ascertain if it still meets the standards for continued classification, agency officials specifically trained for this task get it wrong far more often than not. Based upon personal experience, I can attest that even as effective as the ISCAP is, the typical interagency horse-trading and logrolling occurs there as well and even more

[3] Sec. 5.3, E.O. 13526, op. cit.
[4] Ibid, Sec. 3.5.
[5] ISOO "2015 Report to the President," p. 28. See: https://fas.org/sgp/isoo/2015rpt.pdf
[6] Ibid.

information would be determined not to meet the standards for continued classification if the information had been subject to a truly independent review.

With respect to the mechanics and effectiveness of an independent panel of experts to review classification decisions of the executive, I believe that Congress can look to entities such as the already existing Public Interest Declassification Board[7], which has members appointed by both the president and congressional leadership. Potential enhancements to this Board's role and authority are one place to start.

There is one final point I would like to make. I have been an ardent supporter of agency Inspectors General (IGs) becoming more involved in auditing the appropriateness of agency classification decisions as one means to address the critical issue of overclassification. IGs, of course, have dual reporting responsibility to both the executive and legislative branches. In the "Reducing Overclassification Act" of 2010 (Public Law 111-258), IGs were assigned specific responsibilities in this area. I believe with the proper training and direction, they can accomplish much more and prove to be an effective tool in the exercise of congressional oversight in this area. Potential enhancements to the role and responsibilities of agency IGs in combatting overclassification are another area worthy of congressional attention.

I applaud this committee for focusing on this critical topic to our nation's well-being and I again thank you for inviting me here today, Mr. Chairman. I would be happy to answer any questions that you or other committee members might have.

[7] Section 311 of the Intelligence Authorization Act for Fiscal Year 2014, Section 365 of the Intelligence Authorization Act for Fiscal Year 2010, Section 2 of the Public Interest Declassification Board Reauthorization Act of 2012, Section 602 of the Implementing Recommendations of the 9/11 Commission Act of 2007, and Section 1102 of the Intelligence Reform and Terrorism Prevention Act of 2004 extended and modified the PIDB as established by the Public Interest Declassification Act of 2000 (P.L. 106-567, title VII, Dec. 27, 2000, 114 Stat. 2856).

Secrecy News

AIPAC Case: New Ruling May Lead to Acquittal

Posted on Feb.19, 2009 in Secrecy by Steven Aftergood

A federal court this week ruled that J. William Leonard, the former director of the Information Security Oversight Office, may testify for the defense in the long-running prosecution of two former officials of the American Israel Public Affairs Committee (AIPAC) who are charged with illicitly receiving and transmitting classified information that prosecutors say is protected from disclosure.

Prosecutors had sought to prevent Mr. Leonard, a preeminent expert on classification policy, from testifying for the defendants, on grounds that he had briefly discussed the case with prosecutors while he was still in government. They even suggested that he could be liable to a year in jail himself if he did testify. To protect himself against such pressures, Mr. Leonard (represented by attorney Mark S. Zaid) moved to challenge the subpoena in the expectation that the court would order him to testify, thereby shielding him from any potential vulnerability. ("To Evade Penalty, Key AIPAC Witness Seeks to Quash Subpoena," Secrecy News, September 2, 2008). The court has now done so.

In a February 17, 2009 memorandum opinion (pdf), Judge T.S. Ellis, III affirmed the subpoena and directed Mr. Leonard to testify for the defendants.

The ruling's consequences for the AIPAC case are likely to be momentous, because government secrecy policy has become a central focus of the proceeding and because Mr. Leonard is the strongest witness on that subject on either side.

More than almost any other litigation in memory, the AIPAC case has placed the secrecy system itself on trial. In Freedom of Information Act lawsuits and other legal disputes, courts routinely defer to executive branch officials on matters of classification. If an agency head says that certain information is classified, courts will almost never overturn such a determination, no matter how dubious or illogical it may appear to a third party.

But in this case, it is a jury that will decide whether or not the information in question "might potentially damage the United States or aid an enemy of the United States." Far from granting automatic deference on this question, Judge Ellis wrote that "the government's classification decision is inadmissible hearsay"!

The dispute over whether or not the classified information that was obtained by defendants Steven J. Rosen and Keith Weissman qualifies for protection under the Espionage Act will be "a major battleground at trial," Judge Ellis observed, and it will be addressed at trial "largely through the testimony of competing experts."

While the prosecutors naturally have their own classification experts, including former CIA Information Review Officer William McNair, none of those experts have Mr. Leonard's breadth of experience and none of them reported to the President of the United States on classification matters as he did.

Judge Ellis wrote with perhaps a hint of admiration that the defense "understandably characteriz[es] Leonard's experience and expertise as 'unsurpassed'."

As noted in the new opinion, Mr. Leonard will testify for the defense on the "pervasive practice of over-classification of information," "the practice of high level officials of disclosing classified information to unauthorized persons (e.g. journalists and lobbyists)," whether the classified information in this case qualifies for protection under the Espionage Act, and "whether... the defendants reasonably could have believed that their conduct was lawful."

In other words, the prosecution probably just lost this case.

The new memorandum opinion has not been posted on the court web site for some reason, but a copy was obtained by Secrecy News. Other significant AIPAC case files may be found here.

A nominal trial date has been set for April 21, 2009 but that date is likely to slip as a pre-trial appeal by the prosecution remains pending at the Court of Appeals. (Update: The trial has been rescheduled for June 2, 2009.)

https://fas.org/blogs/secrecy/2009/02/aipac_case-2/

P.O. Box 2355
Leonardtown, MD 20650

July 30, 2011

Mr. John P. Fitzpatrick
Director
Information Security Oversight Office
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

Dear Mr. Fitzpatrick:

I am writing to you pursuant to Section 5.2(b)(6) of Executive Order 13526, "Classified National Security Information" (the Order) which assigns to you the responsibility to "consider and take action on complaints ... from persons within or outside the Government with respect to the administration of the program established under this order." Specifically, in the matter of United States v. Thomas Andrews Drake (Case No. 10 CR 00181 RDB) I am requesting you to ascertain if employees of the United States Government, to include the National Security Agency (NSA) and the Department of Justice (DoJ), have willfully classified or continued the classification of information in violation of the Order and its implementing directive and thus should be subject to appropriate sanctions in accordance with Section 5.5(b)(2) of the Order.

In count one of an indictment dated April 14, 2010, the United States Government charged that Mr. Drake, "having unauthorized possession of a document relating to the national defense, namely, a classified e-mail (attachment 1) entitled 'What a Success', did willfully retain the document and fail to deliver the document to the officer and employee of the United States entitled to receive it." In a letter dated November 29, 2010, (attachment 2) the Department of Justice informed Mr. Drake's counsel that this document is classified overall as SECRET because the information contained therein reveals classified technical details of NSA capabilities. As a plain text reading of the "What a Success" document reveals, this explanation is factually incorrect -- it contains absolutely no technical details whatsoever. The aforementioned DoJ letter went on to state that the document also revealed a specific level of effort and commitment by NSA Notwithstanding that as a basis for classification this notion is exceedingly vague, it is also factually incorrect in view of the fact the the document is absolutely devoid of any specificity. All that is revealed in this otherwise innocuous "rally the workforce" missive is multiple unclassified nicknames with absolutely no reference to the classified purposes, capabilities, or methods associated with the programs or other events or initiatives represented by the unclassified nicknames.

In a letter dated March 7, 2011, (attachment 3) the DoJ provided supplemental information to Mr. Drake's counsel. In this letter, the Government belatedly informed counsel that the "What a Success" document "no longer required the protection of classification," ostensibly because the classification guide for this information was

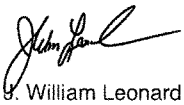
updated on July 30, 2010. This letter went on to state that one of the unclassified nicknames revealed in the document related to a malicious attack on a U.S. government computer system. The letter goes on to rightfully state the reasons why specific information associated with a malicious attack attack on a U.S. government computer system could be classified; however, as supported by a plain text reading of the document, no such information is contained therein. Obviously, if it did contain such information, it should rightfully continue to be classified to this day and its difficult to understand how the update of a classification guide would change this.

Various government officials affiliated with this case have publicly stated that cleared individuals do not get to choose whether classified information they access should be classified, the government does. Nonetheless, when deciding to apply the controls of the classification system to information, government officials are in-turn obligated to follow the standards set forth by the President in the governing executive order and not exceed it's prohibitions and limitations. Failure to do so undermines the very integrity of the classification system and can be just as harmful, if not more so, than unauthorized disclosures of appropriately classified information. It is for that reason that Section 5.5 of the Order treats unauthorized disclosures of classified information and inappropriate classification of information as equal violations of the Order subjecting perpetrators to comparable sanctions, to include "reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation."

I have devoted over 34 years to Federal service in the national security arena, to include the last 5 years of my service being responsible for Executive branch-wide oversight of the classification system. During that time, I have seen many equally egregious examples of the inappropriate assignment of classification controls to information that does not meet the standards for classification; however, I have never seen a more willful example. Failure to subject the responsible officials at both the NSA and DoJ involved in the inappropriate classification and continuation of classification of the "What a Success" document to appropriate sanctions in accordance with Section 5.5(b)(2) of the Order will render this provision of the Order utterly feckless.

I look forward being informed of the results of your inquiry into this matter and any action you take in response to this formal complaint.

Sincerely,



J. William Leonard

cc:

Honorable Tom Donilon
Assistant to the President for National Security Affairs

Honorable Eric H. Holder, Jr.
Attorney General of the United States

General Keith B. Alexander, USA
Director, National Security Agency

U//FOUO

SECRET//REL TO USA, FVEY

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

WHAT A WONDERFUL SUCCESS!

You should all be extremely proud of the part you played in our Spin 1 efforts to demonstrate TURBULENCE. The Director of NSA saw first-hand what you've accomplished, and everyone in the room associated with TURBULENCE was just BEAMING with pride (especially me!)...

U//FOUO

John McHenry did an outstanding job representing us, explaining how TURBULENCE worked and explaining what was happening during the actual demo. The Director was extremely engaged, and knew all about TURBULENCE and the projects associated with it. He asked lots of questions and your teammates around the room provided the detailed information that the Director needed. Thanks to all of you who did - Bill Cocks, Larry Johnson, Jeff Undercoffer, Linda Shields, Jim Bieda, Bill Christian – forgive me if I left anyone out.

UNCLASS

SECRET//REL TO USA, FVEY

approp. Classification at time of signature

During the briefing/demo portion of the meeting, the Director suggested that an application for TURBULENCE might be the Byzantine Hades effort (in conjunction with work being done in TAO). (As an aside, TUTELAGE is mentioned in Byzantine Hades briefings as being part of the solution.) When TRAFFICTHIEF was introduced as being part of the TURBULENCE effort, he interjected, "Clearly the best thing we've done at this Agency up to this point is TRAFFICTHIEF." He asked a lot of questions about how TRAFFICTHIEF and XKEYSCORE interact. In reference to how TURBULENCE follows the quick spin philosophy, the Director mentioned that just this morning, in his discussions with Congress, it was mentioned that rapid spins need to be more widely used, because change in technology is so rapid. He wants to get those congressmen here and show them how we're demonstrating TURBULENCE using spins.

Classified per TURBULENCE and TUTELAGE classification guide

U//FOU

(has been declassified UNCLASS) per Tutelage Class Guide 10-12 dtd 30 Jul 2010

The Director wants you to know that there's "nothing more important in this Agency" than what you're doing. He wants us to have "unfettered access" to him (and mentioned that Pat Dowd is probably the person he deals with the most). Pat, in turn, pointed out that when the Director pings him, the way TURBULENCE is structured, he goes directly to the tech leads and the people working TURBULENCE, so there's a direct line of communication.

The Director emphasized that his goal is that "we are moving out as quickly as possible and as smartly as we can." No pressure! Once the system is stabilized, he "wants us to get it out to the field, be pragmatic, but deliver it." The environment is "changing so quickly we have to use it as soon as possible."

U//FOUO

His primary concerns are twofold: 1) The Global War on Terrorism, and 2) Net Warfare. And the work you've done to MAKE TURBULENCE HAPPEN will have a profound impact on those two concerns. He "wants to make sure you are getting all the support you need" and he wants to "help you deal with the multiple layers of bureaucracy" that may hinder progress. (At that point, almost jumped out of my seat and cheered!)

He then reiterated TURBULENCE is "really, really important to this Agency, to this Nation and we have to overcome the risks" associated with making it work. He talked about the "fight on the network" and used the analogy of the Wright Brothers – they did not build a plane thinking that it would give us such a strategic advantage in WWII. "In the Information Age, we have to win by getting there first."

CM

The Director talked about how "our Agency has tremendous talent across the board" (and Pat chimed in that the TURBULENCE team represents the best). As "we get into this Net Warfare front," we will have to increase the number of folks who have skills in EE, and CompSci and High Performance Computing (we already have the best talent in Math).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SECRET//REL TO USA, FVEY

U//FOUO

 CM

u//FOUO

SECRET//REL TO USA, FVEY

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

He predicted that "the fight on the network is going to come on in the near-term." We need to GET THERE FIRST! We need to be the "fastest with the most." He talked about how important this demo was to him, apologized for the delay in his coming to see the demo, and thanked us for jumping through hoops to provide today's demo on such short notice. He complimented John on his excellent briefing, and noted that the slides were great and wanted to get a copy.

He ended the meeting by saying again: "What you're doing is extremely important. Pat gets more attention than anyone else in the Agency." He made a joke of what we could deliver out to the field by Spin 4, looked at my shocked expression, and suggested that Spin 3 might be a better goal. My response was "please." ☺ He said "you are leading the path, are the advanced scouts" and are key in how we get there.

~~SECRET//REL TO USA, FVEY~~

UNCLASS

He left the conference room, but before he left the building, he greeted the entire test team in the lab (who worked behind the scenes to make sure the demo was successful). Kurt Dawson did an excellent job briefing him on the Stage 1 TURMOIL rack. Thanks, Kurt!

Classified per TURBULENCE and TUTELAGE classification guide

THANKS to all of you. What a GREAT team we have.

Based on today's success and the Director's comments, we have appended our vision:

approp. Class. at time of origination. Has been declassified per Tutelage Class Guide 10-12 dtd 30 jul. 2010

MAKE TURBULENCE HAPPEN

AND

GET THERE FIRST!

u//FOUO

SECRET//REL TO USA, FVEY

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

NSA(u)000688

Cm

U.S. Department of Justice
Criminal Division

Washington, D.C. 20530

UNCLASSIFIED//FOR OFFICIAL USE ONLY

November 29, 2010

James Wyda, Esq.
Deborah Boardman, Esq.
Office of the Federal Public Defender
100 South Charles Street
BankAmerica Tower II, Ninth Floor
Baltimore, MD 21201

Re: United States v. Thomas Andrews Drake
Case No. 10 CR 001811-RDB

Rule 16(a)(1)(G) Expert Summary Disclosure

Dear Counsel:

(U) Pursuant to your request for expert disclosures, the written discovery agreement, and our obligation under Rule 16(a)(1)(G), this letter is a written summary of the testimony of Catherine A. Murray, an Original Classification Authority (hereinafter "OCA") for the National Security Agency (hereinafter "NSA"). This letter does not set forth each and every fact about which Ms. Murray will testify, but rather sets forth her qualifications and a written summary of her testimony, including the bases and reasons for her opinions.

(U) We hereby request production of any and all discovery relating to your experts pursuant to Rule 16(b).

Qualifications

(U) Ms. Murray has been employed at NSA for approximately 28 years in a variety of positions primarily within the signals intelligence mission. While assigned as the Chief S02 (SID Policy), she was also a designated Agency OCA. Ms. Murray's OCA-specific duties and responsibilities include mandatory annual training in the basis of classification in accordance with Executive Order 13526; reviewing and determining the proper level of classification for NSA documents and information; reviewing the work of other NSA classification advisory officers; and serving as an expert in federal court.

Summary of Testimony

(U) Ms. Murray will testify that the authority of an OCA generally derives from Executive Order 13526 and its predecessors. The purposes of the Executive Order are to prescribe a uniform system for classifying, safeguarding and declassifying national security information, and to protect information critical to national security while also balancing an interest in an open government. Ms. Murray will define some of the terms and phrases important in understanding original classification, including, but not limited to, "national security information," "information," and other terms and phrases necessary and helpful to the jury's understanding of the process of original classification. Ms. Murray also will testify that the original classification authority is non-delegable, and that the uniform system of classification would fail if others could make their own independent determination of the proper classification of information.

(U) Ms. Murray also will testify regarding what conditions must be met in order for information to be classified. By way of example only, these conditions include that: the information must be classified by an OCA, the information must be owned by, produced by or for, or under the control of the U.S. Government, the information must relate to intelligence activities, and the unauthorized disclosure of information reasonably could be expected to cause damage, and the OCA can identify or describe that damage.

(U) Ms. Murray will testify about the different levels of classification. She will define and discuss what is "Confidential," "Secret," and "Top Secret" information, as well as "Sensitive Compartmented Information ("SCI") information. "Confidential" information is information that, if subject to unauthorized disclosure, can reasonably be expected to cause damage to the national security of the United States. "Secret" information is information that, if subject to unauthorized disclosure, can reasonably be expected to cause grave damage to the national security of the United States. "Top Secret" information is information that, if subject to unauthorized disclosure, can reasonably be expected to cause exceptionally grave damage to the national security of the United States.

Ms. Murray will describe some of the factors that go into a classification decision. These factors can include, but are not limited to, foreign government information, intelligence activities to include sources, methods, and means, resource commitment or investment, compromise, safety, equity considerations of partners, and foreign relations. Ms. Murray will explain how

documents containing classified information are marked, including header and footer markings, portion markings, and the methods required to disseminate classified information.

(U) In addition, she will define and discuss markings and acronyms that may appear on certain documents, such as "COMINT," "FOUO," and other similar types of markings. Ms. Murray also will testify about other aspects of the Executive Order, such as what to do if there is significant doubt about the need to classify information (i.e. not classify) or the appropriate level of classification (i.e. adopt the lower level of classification), or inappropriate reasons for classification (e.g. concealment of violations of law, prevention of agency embarrassment, etc.). In addition, Ms. Murray will testify about the procedures to review classification decisions to determine if classifications need to be modified.

(U) Ms. Murray will testify about the general restrictions on access to classified information, including the requirements of appropriate security clearances, non-disclosure agreements, and the "need to know." She will testify about how NSA is a closed system, and each NSA employee's responsibility to safeguard classified information, including the tools and guides available to each and every employee to assist them in making an initial classification when creating a document. She will testify that no NSA employee may remove classified information from NSA without proper authorization.

(U) Based upon her training and experience, as a twenty-eight year NSA employee and as an OCA, and consistent with the classification guide(s) relevant to the documents and information at issue in this case, Ms. Murray will testify as follows:

1. "Collections Sites" Document

(U//FOUO) This document is classified overall as "Top Secret," because the information contained therein reveals physical locations of collection activity, including undeclared and potentially single source collection activity; the forward deployment of employees; and classified technical details of NSA capabilities to a degree that adversaries could design or employ countermeasures. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

2. "Trial and Testing" Document

(U//FOUO) This document is classified overall as "Top Secret," because the information contained therein reveals classified technical details of NSA capabilities to a degree that adversaries could design or employ countermeasures. In addition, the document contains "Secret" information, because the information contained therein reveals classified technical details of NSA capabilities, but not to a degree that adversaries could design or employ countermeasures. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

3. "Volume is our Friend" Document

(U//FOUO) This document is classified overall as "Top Secret," because the information contained therein reveals classified technical details of NSA capabilities to a degree that adversaries could design or employ countermeasures. In addition, the document contains "Secret" information, because the information contained therein reveals classified technical details of NSA capabilities, but not to a degree that adversaries could design or employ countermeasures, and classified budget information that demonstrates a specific level of effort and commitment by NSA. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

4. "What a Success" Document

(U//FOUO) This document is classified overall as "Secret," because the information contained therein reveals classified technical details of NSA capabilities and a specific level of effort and commitment by NSA, but not to a degree that adversaries could design or employ countermeasures. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

5. "Regular Meetings" Document

(U//FOUO) This document is classified overall as "Secret," because the information contained therein reveals covered operations and sources and methods, but not to a degree that adversaries could design or employ countermeasures. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

6. "Shoestring Budget" Document

(U//FOUO) This document is classified overall as "Top Secret," because the information contained therein reveals classified technical details of NSA capabilities to a degree that adversaries could design or employ countermeasures. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

7. "BAG" Document

(U//FOUO) This document is classified overall as "Confidential," because the information contained therein reveals a connection between classified technical details of NSA and a specific program. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

8. "Buy vs. Make" Document

(U//FOUO) This document is classified overall as "Top Secret," because the information contained therein reveals classified technical details of NSA capabilities to a degree that adversaries could design or employ countermeasures. In addition, the document contains "Secret" information, because the information contained therein reveals classified technical

details of NSA capabilities, but not to a degree that adversaries could design or employ countermeasures, and classified budget information that demonstrates a specific level of effort and commitment by NSA. Finally, the document contains "Confidential" information, because the information contained therein reveals personnel strength and a specific level of effort and commitment by NSA. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

9. "9-11 Commission" Document

(U//FOUO) This document is classified overall as "Confidential," because the information contained therein reveals personnel strength and a specific level of effort and commitment by NSA. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

10. "TT Notes" Document

(U//FOUO) This document is classified overall as "Secret," because the information contained therein reveals classified budget information that demonstrates a specific level of effort and commitment by NSA. Finally, the document contains "Confidential" information, because the information contained therein demonstrates personnel strength and a specific level of effort and commitment by NSA. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

11. "Terrorism Threat" Document

(U//FOUO) This document is classified overall as "Secret," because the information contained therein reveals classified technical details of NSA capabilities, but not to a degree that adversaries could design or employ countermeasures, and classified budget information that reveals a specific level of effort and commitment by NSA. Finally, the document contains "Confidential" information, because the information contained therein reveals sources and methods associated with a specific program of NSA. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

12. "Note Card 1" Document

(U//FOUO) This document is classified overall as "Secret," because the information contained therein reveals classified budget information that demonstrates a specific level of effort and commitment by NSA. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

13. "Note Card 2" Document

(U//FOUO) This document is classified overall as "Secret," because the information contained therein reveals classified budget information that demonstrates a specific

level of effort and commitment by NSA. In addition, the classified information in this document appears in other "source" documents, and these documents are classified at a similar level.

(U//FOUO) The United States reserves the right to supplement this expert summary. You may schedule an appointment at the NSA to review Ms. Murray's classification review of the aforementioned documents.

Very truly yours,

By: _____
WILLIAM M. WELCH II
Senior Litigation Counsel
Criminal Division
United States Department of Justice

U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

March 7, 2011

VIA EMAIL

James Wyda, Esq.
Federal Public Defender
Deborah Boardman, Esq.
Assistant Federal Public Defender
100 South Charles Street
BankAmerica Tower II, Ninth Floor
Baltimore, Maryland 21201

Re: United States v. Thomas Andrews Drake
Case No. 10 CR 00181 RDB

Dear Attorneys Wyda and Boardman:

This letter shall supplement the previous unclassified Rule 16(g) expert summary of Catherine Murray.

4. "What a Success" Document

(U//FOUO) This document is classified overall as "SECRET," because the information contained therein reveals classified technical details of NSA capabilities and a specific level of effort and commitment by NSA, but not to a degree that adversaries could design or employ countermeasures. More specifically, the combination of the cover terms for this network architecture implied a level of effort, scale, and scope by NSA, and a level of activity and commitment by NSA, to this network architecture such that the information was classified as "SECRET."

(U//FOUO) On July 30, 2010, the classification guide for this information was updated by NSA in accordance with the Executive Order, and NSA determined that this information no longer required the protection of classification. The information, however, was appropriately classified as "SECRET" through the time of the defendant's possession, which ended on November 28, 2007, and through the date of the indictment, April 14, 2010.

(U//FOUO) In addition, this document also discussed NSA efforts related to a malicious computer attack by an external actor or third party on a U.S. government computer system. This fact was classified as "SECRET//REL TO USA, FVEY." Additionally, the document included a specific cover term that had been assigned to this instrusion in order to protect the sensitive nature of the discovery and vulnerability to U.S. government computer networks. The fact that a

specific malicious computer activity had been found on a U.S. government computer system or network, and the U.S.'s identification of and/or response to the malicious activity, was classified as "SECRET." Unauthorized disclosure of exposure of the success or failure of a malicious computer activity against a U.S. government computer system would provide a determined adversary insight into the strengths and/or vulnerabilities of U.S. government computer systems or networks and allow a more focused intrusion.

(U//FOUO) On July 30, 2010, the classification guide for this information was updated by NSA in accordance with the Executive Order, and NSA determined that this information no longer required the protection of classification. The information, however, was appropriately classified as "SECRET" through the time of the defendant's possession, which ended on November 28, 2007, and through the date of the indictment, April 14, 2010.

Very truly yours,

/s/

William M. Welch II
Senior Litigation Counsel
John P. Pearson
Trial Attorney
Public Integrity Section
United States Department of Justice

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

December 26, 2012

J. William Leonard
P.O. Box 2355
Leonardtown, MD 20650

VIA E-MAIL

Dear Mr. Leonard,

I am responding to your letter of July 30, 2011, in which you asked that I, in accordance with my assigned duties under Executive Order 13526, "Classified National Security Information" ("the Order"), consider and take action with regard to what you viewed as a violation of the Order. Specifically, you requested I "ascertain if employees of the United States Government, to include the National Security Agency (NSA) and the Department of Justice (DOJ), have willfully classified or continued the classification of information in violation of the Order" in the matter of *United States v. Thomas A. Drake*. I have concluded my inquiries into this matter, having consulted with the above-mentioned agencies, drawn upon the Order, its implementing Directive, and examined relevant portions of each agency's security regulations, and now share with you my findings and observations.

With regard to your complaint, I conclude that neither employees of the Department of Justice nor of the National Security Agency willfully classified or continued the classification of the "What a Wonderful Success" document in violation of the Order. I wish to note that your complaint suggests this was done "in the matter of *United States v. Thomas A. Drake.*" I think it is important to point out that my process in addressing your complaint examined (and distinguished between) the classification of the document in its first instance and any continuation of its classification "in the matter of *United States v. Thomas A. Drake*." I find no violation in either case. In fact, as materials you provided with your complaint make clear, NSA discontinued the classification of the document in question and represented the same to the court "in the matter of *United States v. Thomas A. Drake*."

In examining the "What a Wonderful Success" document, I find that the NSA did not violate the Order's requirements for appropriately applying classification at document creation, nor did the agency violate the Order's expectation that information shall be declassified when it no longer meets the standards for classification. While my examination of the matter has led to my conclusion that the content and processing of the document fall within the standards and authority for classification under the Order and NSA regulations, that does not make them immune to opinions about how substantial the document's content may or may not be. I find, simply, that those opinions do not rise to the level of willful acts in violation of the Order. That said, such commentary on the culture of classification fits well in discussions of policy reform. In such fora, including the work of the Public Interest Declassification Board, your experience and observations would continue to be welcome.

Separate and apart from the specifics of the Drake matter, there are important aspects of the classification system worth noting in this larger discussion of the scope of classification guidance. As you are aware, section 1.1 of the Order grants both responsibility and latitude to Executive branch officials with original classification authority. These officials are the chief subject matter experts in government concerning information that could be damaging to national security if compromised or released in an unauthorized manner.

In light of this, section 2.2 of the Order directs officials with original classification authority to prepare classification guides to facilitate the proper and uniform classification of information. A well-constructed classification guide can foster consistency and accuracy throughout a very large agency, can impart direction concerning the duration of classification, and ensure that information is properly identified and afforded necessary

protections. Throughout the Executive branch, officials strive to impart proper classification guidance that is accurate, consistent, and easy to adopt in workforces that operates under tight time constraints. It seems quite clear, however, that the system would benefit from greater attention of senior officials in ensuring that their guidance applies classification only to information that clearly meets all classification standards in section 1.1 of the Order. For emphasis, I draw specific attention to language in Section 1.1 (a)(4) "... that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security..." and, 1.1 (b) "If there is significant doubt about the need to classify information, is shall not be classified."

I have a few observations about these matters in the context in which you raised them, namely, the matter of the *United States v Thomas A. Drake*. I have no basis to comment about the disposition of the case in the courts; that is not my purview. The conduct of the case did, however, bring to light actions and behaviors I will comment on briefly, for emphasis. The Order does not grant any individual the authority to safeguard classified information in a manner that is contrary to what the Order, its implementing directive, or an agency's security regulations require. The Order does not grant authorized holders of classified information the authority to make their own decisions concerning the classification status of that information. Furthermore, individuals are provided the means to challenge classification either formally or informally. Section 1.8 of the Order provides all authorized holders of classified information with the authority to issue challenges to classification actions. It explicitly states that individuals are "encouraged and expected" to challenge the classification status of the information through appropriate channels, and every agency is required to implement procedures whereby any authorized holder may issue a challenge without fear of retribution. I know, through the work of this Office, that the National Security Agency is well practiced in the Order's requirements concerning classification challenges. It is my understanding that Mr. Drake made no attempts to challenge the classification status of the information in question.

I note that neither version of the Order in force during the Drake case's time frame [Executive Order 13526 (29 December 2009) and its predecessor Executive Order 12958 (17 April 1995)] provides much in the way of guidance or direction, on its own, to influence the use of classified information in building prosecutions such as this. In general, the Department of Justice defers to the judgment of the "victim" agency as to what constitutes classified information. In building a case, victim agencies, for their part, tend to provide evidence that they deem sufficient to obtain a conviction with the hopes of protecting their most sensitive information and activities from release during court proceedings. The Directive (32 CFR 2001.48) requires only that agency heads "use established procedures to ensure coordination with" the Department of Justice and other counsel. All of this assumes that other influences will be at work to pursue only worthwhile prosecutions, but one interpretation of the Drake case outcome might suggest that this "coordination" was not sufficient. I would welcome your thoughts on whether there is role for policy to provide clearer, more effective guidance in the manner in which such cases are built.

I thank you for your diligent, care-filled observations and comments concerning classification matters. You continue to serve the public well by remaining engaged in the dialogue around the use of secrecy by the government. I can assure you that we take these viewpoints to heart.

Sincerely,

<Signed>

JOHN P. FITZPATRICK
Director, Information Security Oversight Office

From: Bill Leonard
Date: December 31, 2012, 4:10:23 PM EST
To: John Fitzpatrick
Subject: Re: Complaint

John:

Thanks very much for your reply. While I appreciate the time, effort and consideration you put into this matter, I am nonetheless disappointed in the substance of your reply. Some of my final thoughts on this matter include:

1. It took almost one and a half years to respond to a rather straightforward yet serious request. I recognize the need for coordination; nonetheless, irrespective of the nature of the reply, responsiveness is essential for a system to be able to be self-correcting.

2. As we discussed when we met in August 2011, I have never taken real issue with the classification of the "What a Success" document in the first instance, which although improper was, by all appearances, a reflexive rather than willful act. Nor did I take issue with its eventual "declassification," which I regarded as NSA simply coming to the proper conclusion, albeit belatedly. What I did and continue to take issue with is that in between those events, senior officials of both the NSA and DoJ made a number of deliberate decisions to use the supposed classified nature of that document as the basis for a criminal investigation of Thomas Drake as well as the basis for a subsequent felony indictment and criminal prosecution. Even after NSA recognized that the document did not meet the standards for continued classification and made the unprecedented decision to declassify an evidentiary document while an Espionage Act criminal prosecution was still pending, senior officials of both the NSA and DoJ still willfully persisted and made yet another deliberate decision to stand by the document's original classification status. I cannot imagine a clearer indication of willfulness on the part of senior government officials to "continue the classification of information in violation" of the governing order through numerous deliberate and collaborative decisions made over the course of years. Based upon my extensive experience, I find the provenance of this document's classification status to be unparalleled in the history of criminal prosecutions under the Espionage Act.

3. You ascribe the merits of my complaint as constituting a mere honest difference in opinion. However, this complaint is more than a question of the document failing to pass what I call the "guffaw test" (i.e. common sense). Rather, as I pointed out in my original complaint and yet you did not address, at the heart of this issue are matters of fact. In justifying the deliberate decision to represent during the Drake prosecution that the "What a Success" email was a legitimately classified document, NSA and DoJ officials did not cite some amorphous classification standard or classification guide - rather they made factual representations which simply were not true and, in one instance, inherently contradictory (i.e. "information contained therein **reveals ... a specific level** (emphasis

added) of effort ..." and that the same information **"implied a level** (emphasis added) of effort ..."). Keep in mind that these determinations were not made on the fly by NSA and DoJ but were in fact deliberate representations made over a period of time and subsequently further qualified but never disavowed. They were intended to demonstrate that the document met the standards of classification that require the original classification authority to identify or describe the damage to national security that could reasonably be expected to result from the unauthorized disclosure. A familiarity with classification standards is not required to determine that these official representations were on their face factually incorrect when compared with a plain text reading of the "What a Success" email. All too often, representatives of the Executive branch believe all they need to do is simply assert classification rather than adhere to the president's own standards, as apparently was the situation in the Drake case. That attitude must change and I will continue to do all I can to help make it foster change.

4. You comment on the fact that the Order does not grant any individual the authority to handle classified information in a manner contrary to the Order and other pertinent regulations. While reference to alleged actions taken or not taken by Mr. Drake are gratuitous and have no bearing on the merits of my complaint, I nonetheless agree with your sentiment. However, allow me to add my own observations, not only as one of your predecessors but also as the only individual who has played an integral role for both defense teams in the only two Espionage Act prosecutions (Drake and AIPAC) not to result in either a conviction or a plea of guilty. In both instances (in which I provided my services pro bono) my decision to get involved was not to defend the actions of the accused but rather to defend the integrity of the classification system, a highly critical national security tool. I have long held that when government agencies fail to adhere to their responsibilities under the governing order and implementing directive, they in turn compromise their ability to hold cleared individuals accountable for their actions. Accountability is crucial to any system of controls and the fact that your determination in this case preserves an unbroken record in which no government official has ever been held accountable for abusing the classification system does not bode well for the prospect of real reform of the system. This phenomenon, the readily apparent inclusion in the Order of a feckless provision which infers that accountability cuts both ways has once again been proven to be a major source of why most informed observers both inside and outside the government recognize that the classification system remains dysfunctional due to rampant and unchecked over-classification. It is disappointing to note that a genuine opportunity to instill an authentic balance to the system has been forfeited in this instance.

As to your request for my recommendations as to the potential for clearer guidance when the classification status of information is integral to a criminal prosecution, I would recommend requiring coordination with an independent body such as the Interagency Security Classification Appeals Panel. In the two cases I referenced above, the fact that the government did not obtain a criminal conviction under the Espionage Act actually bode well for the integrity of the classification system -- otherwise, the perceived wisdom in the reflexive over-classification of information would have been codified in case law.

Finally, I stand ready to share my experiences and observations with the Public Interest Declassification Board and other fora as seen fit.

Thanks again for the reply, John. While I admire the job you do and the challenges you face, I obviously disagree with the content of your reply. Nonetheless, I am appreciative of the courtesy.

Best wishes for the New Year.

jwl

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,	*	
v.	*	Criminal Action No. RDB 10-00181
THOMAS ANDREWS DRAKE,	*	
Defendant.	*	

* * * * * * * * * * * * *

MEMORANDUM ORDER

Presently pending before this Court is Defendant Thomas Andrews Drake's Motion for Relief from Protective Order (ECF No. 180). This motion requests that permission be given to the defense's expert witness, J. William Leonard, the former Director of the Information Security Oversight Office (ISOO), to disclose and discuss three unclassified documents which are subject to this Court's Protective Order (ECF No. 13) governing unclassified discovery. The three unclassified documents at issue are (a) the document charged in Count One of the Indictment, entitled "What a Success," (b) the government's November 29, 2010 expert witness disclosure, and (c) the government's March 7, 2011 expert witness disclosure. Mr. Leonard has indicated that he seeks to use these documents to have an open discussion about the government's actions in this case as they pertain to the Executive Branch's national security information classification system.

The government has opposed this motion on the grounds that both Defendant Drake and Mr. Leonard lack standing to bring this motion. Additionally, the government contends that Mr. Leonard should elect to obtain these documents by filing a Freedom of Information Act ("FOIA") request with the National Security Agency ("NSA"). Moreover,

on July 26, 2012, the government notified this Court that similar FOIA requests had been approved for six other individuals, that Mr. Leonard's request, once filed, would be immediately approved and that he would be able to "use the documents as he pleases." Notice to the Court at 2, ECF No. 193. Despite the government's willingness to provide these documents to Mr. Leonard, it continues to request that this Court deny Defendant's Motion for Relief from Protective Order (ECF No. 180).

Nevertheless, the government's arguments in this case are inapposite. As is aptly stated in the Defendant's Reply (ECF No. 192), Mr. Leonard is bound by the terms of the Protective Order and is therefore required to seek relief from the order to discuss unclassified information. The explicit language of the Order provides that it applies to "experts or consultants assisting in the preparation, trial and appeal of this matter" and that "[t]he contents of the Protected Material . . . *shall not be disclosed to any other individual or entity* in any manner except to a photocopy service as agreed by the parties or *by further order of this Court*." Protective Order, ECF No. 13 (emphasis added). Moreover, the government has repeatedly insisted that this Protective Order remains in force despite the resolution of this case. Additionally, a FOIA request would not have been sufficient to permit Mr. Leonard's public use of these documents. In fact, while a FOIA request would have permitted him to receive the documents in question, he would not have been permitted to discuss them as he would remain bound by this Court's Protective Order.

In light of the foregoing and adopting the Defendant's reasoning in its Reply (ECF No. 192), it is this 10th day of September 2012, ORDERED that Defendant Thomas Andrews Drake's Motion for Relief from Protective Order (ECF No. 180) is GRANTED.

Specifically, Defense expert witness, J. William Leonard, may disclose and discuss with the public the following unclassified documents: (a) the document charged in Count One of the Indictment, entitled "What a Success," except for NSA employees' names identified in the document, which shall be redacted and shall not be disclosed; (b) the government's November 29, 2010, expert witness disclosure; and (c) the government's March 7, 2011 expert witness disclosure. Additionally, Mr. Leonard is permitted to discuss his July 30, 2011 letter complaint to John P. Fitzgerald, Director of ISOO.

The Clerk of the Court transmit copies of this Memorandum Order to Counsel.

/s/ Richard D. Bennett

Richard D. Bennett
United States District Judge

How Classification Abuse Leads to Manipulation of UCMJ Process
(Unpublished Op-ed, August 2014)

When used properly, the system to classify national security information can protect service members from harm by denying information to the enemy on the battlefield. In the hands of calculating superiors willing to undermine the system's integrity, classification can be used to manipulate the military justice process and deny service members the due process to which they are entitled. Such was the case in a special court-martial of former Marine Captain James Clement who faced charges, which were subsequently dismissed, arising out of a July 2011 operation in Helmand Province, Afghanistan during which four Marines were videoed urinating on enemy corpses.

The use of classification in this case was problematic from the very beginning. With legal counsel for the Commandant of the Marine Corps taking the lead, unofficial images depicting mistreatment of corpses and other violations of the law of armed conflict were classified notwithstanding President Obama's governing executive order which clearly prohibits the use of the classification system to conceal illegal or embarrassing conduct. Additionally, use of classification in this instance was contrary to the clear precedent that was established in the wake of the Abu Ghraib torture and prisoner abuse scandal. In that instance, as director of the Information Security Oversight Office, I was instrumental in getting the Department of Defense to acknowledge that classification of the Article 15-6 Investigation into the abuse was inappropriate and that corrective action was required to ensure that similar misuse of the classification system did not occur in the future. Furthermore, as recently as five years ago, all three branches of our Federal government evidently believed that the use of classification to conceal similar images was inappropriate. Specifically, facing a court order under the Freedom of Information Act directing the release of a trove of undisclosed images of abuse at Abu Ghraib and elsewhere, Congress felt compelled to pass legislation in October 2009 giving the Pentagon special authority to ban the release of these or similar images without the use of classification.

After a lengthy internal debate within the Marine Corps, the preponderance of the images as well as most of the attendant command and criminal investigations into the circumstances surrounding the urination video, were declassified. Not declassified were a number of critical exculpatory sworn interviews which Captain Clement's defense team sought to use in his Article 32 hearing. However, the prosecution objected claiming unavailability under the military's rules for the use of classified information in UCMJ proceedings, thus denying Captain Clement the benefit of critical testimony. His counsel was further advised that critical portions of the testimony at another Marine's Article 32 hearing were classified and unavailable for Captain Clement's defense despite the fact that the hearing itself was public. Notwithstanding having the requisite security clearances and official access to the actual statements, Captain Clement's defense counsel was never advised as to why the statements were classified; a clear violation of President Obama's order that information must be uniformly and conspicuously marked so as to leave no doubt about the classified status. Thus, exculpatory sworn statements could not be used, not even as the basis for interviews of other witnesses. I was thus brought on as a pro-bono expert consultant for the defense in order to assist in compelling the government to adhere to its own responsibilities under the classification system. Shortly thereafter, the criminal charges against Captain Clement were dismissed and instead he was subjected to an administrative proceeding.

While I was never provided access to the purportedly classified statements critical to Captain Clement's defense, due to the Marine Corps' ineptitude in applying classification and declassification decisions, it readily became apparent to me the specific information the government was claiming to be classified. Specifically, a section of the unclassified version of the command investigation report details what another Marine back at the combat operations center was able to observe of the ill-fated operation in real-time. The investigative report then goes on to state in the very next paragraph "that (original statement is classified technology SECRET//NOFORN) can provide persistent video surveillance of an area." Thus, exculpatory sworn statements which contained references to how the combat operations center was able to maintain real-time video surveillance on events in the field were placed beyond defense counsel's use based upon the bogus claim by the government that reference to such surveillance platforms was classified.

Evidence of the falsity of claims to legitimate classification in the interest of national security is contained in the unclassified version of the command investigation report itself which includes a number of references to the surveillance platforms by name (i.e. "Aerostat" and "ScanEagle"). For example, while the name of the platform was redacted from the body of the report, the enclosure referenced when discussing the unnamed platform was not removed from the report. This enclosure is a fact sheet prepared by the defense contractor Raytheon and approved by the Department of Defense for public release. It provides details of the "Rapid Aerostat Initial Deployment (RAID) system and it sensor suites (EO/IF sensor, radar, flash and acoustic detectors) (that) provide unprecedented elevated persistent surveillance (EPS)". It goes on describe the Aerostat's capabilities and how it is deployed in-theater in far greater detail than any of the information contained in the purportedly classified statements. Furthermore, unclassified statements included in the command investigation report include references, for example, as to how the Aerostat is used to counter indirect fire and how ScanEagle (which is actually an unclassified commercial drone) is used to conduct battle damage assessments. In addition, the classification guide eventually cited by the government as justification for classification does not specifically address these surveillance platforms. Finally, by simply Googling "Aerostat" or "ScanEagle" and "Afghanistan" anyone, to include the enemy, can access numerous articles, photographs and videos released by Department of Defense elements as to how these two surveillance platforms are employed in-theater.

Clearly, ineptitude permeated almost every classification and declassification decision associated with this investigation. For example, an official in the office of the Marine's Deputy Commandant for Plans, Policies and Operations (DC, PP&O) stated in an email that the DC, PP&O never even reviewed the video which was cited more than any other video in the command investigation report and which contained evidence of multiple unlawful acts to include mistreatment of enemy corpses; thus the video with the most inflammatory images second to urination video was never "considered in his classification decision." This despite the fact that the purported rationale for classifying the images and videos in the first place was that their dissemination could encourage attacks against service members in-theater.

However, more than ineptitude was entailed when classification was invoked in this matter. For example, the legal advisor to the Consolidated Disposition Authority in Captain Clement's case indicated in an email that direction was given to trial counsel "to let those DC's (defense counsel) know who have been extended the NJP (non-judicial punishment) deal pre-preferral that if they allow this investigation to go unclass (i.e. wait until the investigation is declassified), their clients will probably be looking at preferred

charges. This needs to be moving and right now the only way to move this is through the pre-preferral NJP deals. That will no longer be the case once the investigation becomes unclassified." Clearly, Marines were being pressured to accept plea deals before an investigation that contained exculpatory information and which never should have been classified in the first place became declassified.

Finally, the Commandant of the Marine Corps himself gave very clear insight into the real intent for the classification of these images and the attendant investigation when he addressed fellow Marines in June 2012 at the Marine Barracks in Washington, DC during his "Heritage Tour." When specifically addressing the issues of images associated with the urination video, the Commandant does not bother to mention even in passing the ostensible reasons why the Marine Corps initially classified these images. He did not, for example, say that the Marine's conduct and the public dissemination of related images jeopardized the lives of fellow Marines by potentially inciting violence. He did not say that the dissemination of the images undermined the military objectives of the war or potentially damaged foreign relations. Rather, in talking about all the various images of the inevitable consequences of war that the American public is exposed to, he states: "But we are right smack in the middle of it. We're lumped right in there with everybody. I don't want to be lumped in with anybody else. We are United States Marines. We're different. Our DNA is different. I don't want to be lumped in with anyone else. We've got issues; we'll solve it. We'll take care of it ourselves. And we will police ourselves..." Thus, from the Commandant's perspective, the ability to hold others accountable ends with him. The Congress and the public, for example, have no right to the images and other information necessary to assess not only his accountability but the accountability of society as a whole in acknowledging responsibility for some of the inevitable consequences of repeatedly sending the same men and women off to war for more than a decade.

Classification is a critical tool that is intended to be used for the benefit, not detriment, of service members. Yet, the experience of Captain Clement where the classification system is deliberately abused in order to manipulate the UCMJ process is not unique. While military rules governing the use of classified information in UCMJ procedures require trial counsel to first ensure that purportedly classified information relevant to the case is properly classified in the first place, the mechanisms to ensure this is done properly are woefully inadequate and lacking the impartiality required in the interest of justice. Thus, Congress must step in and act. For example, the UCMJ could be revised in order to provide avenues for the independent and impartial review of purported classified information integral to an UCMJ action, exercised perhaps by an entity such as the already existing Public Interest Declassification Board which has members appointed by both the president and congressional leadership. Such a reform is essential if the classification system is to continue to serve as the critical national security tool it is intended to be rather than a trump action exercised at the whim military superiors.

J. William Leonard was Director of the Information Security Oversight Office from 2002-2008 and prior to that served as the Deputy Assistant Secretary of Defense (Security & Information Operations) in the Clinton and Bush administrations.

The New York Times

Official Backs Marines' Move to Classify Photos of Forces With Taliban Bodies

By CHARLIE SAVAGE JUNE 10, 2014

WASHINGTON — In an apparent expansion of the government's secrecy powers, the top official in charge of the classification system has decided that it was legitimate for the Marines to classify photographs that showed American forces posing with corpses of Taliban fighters in Afghanistan.

President Obama's executive order governing secrecy bars use of the classification system to cover up illegal or embarrassing conduct. But the official, John P. Fitzpatrick, the director of the Information Security Oversight Office, accepted the Marines' rationale for classifying the photographs: that their dissemination could encourage attacks against troops.

Mr. Fitzpatrick laid out his conclusion in a May 30 letter to a Marine lawyer who had filed a whistle-blower complaint saying that the secrecy violated the executive order. It could be an important precedent for allowing the military to keep future war-zone photographs depicting abuses by American soldiers hidden from the public.

The decision stands in contrast to the government's position in a legal fight over hundreds of photographs depicting the abuse of detainees in Iraq, which the American Civil Liberties Union sought in a long-running Freedom of Information Act lawsuit.

In that case, military officials raised similar concerns that disseminating the photographs could cause significant harm, provoking attacks on forces in the war zone. But neither the Bush nor the Obama administration claimed they were classified. Instead, Congress passed a special law in 2009 allowing the secretary of defense to block the photographs' release.

J. William Leonard, a former director of the information office, called the move "a significant and disturbing shift" in the government's secrecy policy.

"As recently as five years ago, all three branches of government agreed that the executive did not have power to classify such images," Mr. Leonard said.

Mr. Fitzpatrick said in an email that his decision did not amount to a broad new

executive branch policy, and that questions about classifying war-zone photographs showing wrongdoing by American troops had to be evaluated on a case-by-case basis.

"Because a decision was found to be permissible in one instance does not require it to apply in all, or even in any other instance(s)," he wrote. "In the U.S.M.C. matter, the temporal nature of the decision as relates to a specific set of circumstances in that threat environment at that point in time is key."

The White House declined to comment on whether it agreed with Mr. Fitzpatrick's interpretation of Mr. Obama's executive order.

The dispute traces back to January 2012, when a video was posted online showing four Marines urinating on three dead Taliban fighters. A military investigator obtained several dozen other so-called trophy images, which were not made public, showing troops posing with corpses.

The Marines decided to classify the photographs, along with other materials gathered in the investigation. But several military officers argued that there was no legal basis for doing so. Among them was Maj. James Weirick, a Marine lawyer who was advising the general overseeing the investigation.
Major Weirick later filed whistle-blower complaints about the case, making several allegations, among them that the classification decision was illegal. Mr. Fitzpatrick handled that question and concluded that the Marines' rationale for classifying the photographs fell within the rules.

While Mr. Obama's executive order explicitly bars the use of classification to prevent the public from learning about a criminal or embarrassing act, Mr. Fitzpatrick pointed in his email to another section that allows information related to military operations to be classified, saying that it implicitly encompassed "force protection" concerns.

"That reaction to the material would make coalition forces vulnerable, perhaps even to actions by Afghan forces fighting with the coalition, was an immediate concern," he wrote, calling the classification of the photographs "a tactically oriented decision meant to prevent immediate backlash/harm."

The Marines later asked for a second opinion from the United States Central Command, and the photos were declassified, although they have not been published.

Major Weirick said he was disappointed with Mr. Fitzpatrick's decision, which was first reported on Tuesday on the Secrecy News blog. "That would allow every bad thing to be covered up," he said.

In a related twist, the dispute brought to light a Central Command regulation that says information about past operations is to be kept unclassified if it meets

several criteria, including that it "does not embarrass any coalition members."

Asked on Tuesday how that regulation squared with the executive order's prohibition on classifying information because it is embarrassing, a military spokesman said he was researching the question and had no immediate answer.

METHODOLOGY FOR DETERMINING APPROPRIATENESS OF AN ORIGINAL CLASSIFICATION DECISION

- Who made the decision?
  - Was the individual an original classification authority (OCA)? (§1.1 (a) (1), Order*)
  - Was the individual properly delegated the authority?
    - By the President (§1.3 (a), Order); or
    - If Top Secret, by an official designated by the President (§1.3 (a) (2), Order)
    - If Secret or Confidential by an official designated by the President pursuant to §1.3 (a) (2), Order or by a Top Secret OCA designated pursuant to §1.3 (c) (2), Order (§1.3 (a) (3), Order)
    - Was the delegation in writing; did it identify the official by name or title? (§1.3 (c) (4), Order)

- Is the information owned by, produced by or for, or is under the control of the US Government? (§1.1 (2), Order)

- Does the information fall within one of more of prescribed categories of § 1.4, Order?
  - military plans, weapons systems, or operations
  - foreign government information
  - intelligence activities (including covert action), intelligence sources or methods, or cryptology
  - foreign relations or foreign activities of the United States, including confidential sources
  - scientific, technological, or economic matters relating to the national security
  - United States Government programs for safeguarding nuclear materials or facilities
  - vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
  - the development, production, or use weapons of mass destruction

- Can the OCA identify or describe damage to national security that could be expected in the event of unauthorized disclosure? (§1.1 (4), Order)
  - If Top Secret, can its unauthorized disclosure be reasonably expected to cause exceptionally grave damage to the national security?
  - If Secret, can its unauthorized disclosure be reasonably expected to cause serious damage to the national security?
  - If Confidential, can its unauthorized disclosure be reasonably expected to cause damage to the national security?

---

* Executive Order 13526, "Classified National Security Information"

- Is the information subject to prohibitions or limitations with respect to classification? (§1.7, Order)
  - Is the information classified in order to conceal violations of law, inefficiency or administrative error?
  - Is the information classified in order to prevent embarrassment to a person, organization, or agency?
  - Is the information classified in order to restrain competition?
  - Is the information classified in order to prevent or delay the release of information that does not require protection in the interest of national security?
  - Does the information relate to basic scientific research not clearly related to national security?
  - If the information had been declassified, released to the public under proper authority, and then reclassified:
    - Was the reclassification action taken under the personal authority of the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security?
    - Was that official's determination in writing?
    - Was the information reasonably recoverable without bringing undo attention to the information?
    - Was the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office notified of the reclassification action?
  - If the information had not previously been disclosed to the public under proper authority but was classified or reclassified after receipt of an access request:
    - Does the classification meet the requirements of this order (to include the other elements of this methodology)?
    - Was it accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official?
  - If the classification decision addresses items of information that are individually unclassified but have been classified by compilation or aggregation:
    - Does the compilation reveal an additional association or relationship that meets the standards for classification under this order?
    - Was such a determination made by an OCA in accordance with the other elements of this methodology?
    - Is the additional association or relationship not otherwise revealed in the individual items of information?

METHODOLOGY FOR DETERMINING APPROPRIATENESS OF A DERIVATIVE CLASSIFICATION DECISION

- Who made the decision?
  - Does the decision relate to the reproduction, extract or summation of classified information, either from a source document or as directed by a classification guide? (§2.1 (a), Order*)
  - Is the person who applied the derivative classification markings identified in a manner apparent for each derivative classification action? (§2.1 (b) (1), Order)
  - Is the decision directly attributable to and does it ***accurately*** reflect an appropriate original classification decision by an OCA, to include the level and duration of classification? (§2.1 (b) (2), Order)

- Is the information owned by, produced by or for, or is under the control of the US Government? (§1.1 (2), Order)

- Does the information fall within one of more of prescribed categories of § 1.4, Order?
  - military plans, weapons systems, or operations
  - foreign government information
  - intelligence activities (including covert action), intelligence sources or methods, or cryptology
  - foreign relations or foreign activities of the United States, including confidential sources
  - scientific, technological, or economic matters relating to the national security
  - United States Government programs for safeguarding nuclear materials or facilities
  - vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
    the development, production, or use weapons of mass destruction

- Can damage to national security be expected in the event of unauthorized disclosure? (§1.1 (4), Order)
  - If Top Secret, can its unauthorized disclosure be reasonably expected to cause exceptionally grave damage to the national security?
  - If Secret, can its unauthorized disclosure be reasonably expected to cause serious damage to the national security?
  - If Confidential, can its unauthorized disclosure be reasonably expected to cause damage to the national security?

- Is the information subject to prohibitions or limitations with respect to classification? (§1.7, Order)
  - Is the information classified in order to conceal violations of law, inefficiency or administrative error?

---

* Executive Order 13526, "Classified National Security Information"

- Is the information classified in order to prevent embarrassment to a person, organization, or agency?
- Is the information classified in order to restrain competition?
- Is the information classified in order to prevent or delay the release of information that does not require protection in the interest of national security?
- Does the information relate to basic scientific research not clearly related to national security?
- If the information had been declassified, released to the public under proper authority, and then reclassified:
    - Was the reclassification action taken under the personal authority of the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security?
    - Was that official's determination in writing?
    - Was the information reasonably recoverable without bringing undo attention to the information?
    - Was the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office notified of the reclassification action?
- If the information had not previously been disclosed to the public under proper authority but was classified or reclassified after receipt of an access request:
    - Does the classification meet the requirements of this order (to include the other elements of this methodology)?
    - Was it accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official?
- If the classification decision addresses items of information that are individually unclassified but have been classified by compilation or aggregation:
    - Does the compilation reveal an additional association or relationship that meets the standards for classification under this order?
    - Was such a determination made by an OCA in accordance with the other elements of this methodology?
    - Is the additional association or relationship not otherwise revealed in the individual items of information?

Chairman CHAFFETZ. Thank you.

Now there is a model for ending right at the 5-minute mark.

Mr. Aftergood, I challenge you to come within 1 second of that mark as well, but you are now recognized for 5 minutes.

STATEMENT OF STEVEN AFTERGOOD

Mr. AFTERGOOD. Thank you, Mr. Chairman and Ranking Member Cummings.

As you know and as you really expressed very well, overclassification presents many kinds of problems. It makes your oversight job more difficult. It incurs substantial financial and operational costs, and it often leaves the public in the dark about national security matters of urgent importance that they should be aware of.

Why do we even have overclassification? I think there are many reasons. For one thing, it is easier for officials to restrict access to information without carefully weighing the pros and cons of what should be disclosed. Overclassification many times is simply the path of least resistance. Unchecked classification can also serve the political interests of the classifiers. It is a way to manage public perceptions, to advance an agenda, to limit oversight, or simply to gain a form of political advantage.

So what is the solution to overclassification? I don't think there is a single solution. I discuss several partial solutions in my written statement. Many of those solutions depend on Congress to assert itself and to affirm its own institutional interests. Congress is not a spectator, and it should not be a victim when it comes to overclassification. It is a coequal branch of government.

In the executive branch, there are lots of fine and conscientious people who are involved in classification policy, fortunately, but we should not have to rely on their integrity. We rely instead on Congress to exercise checks and balances in performing its routine oversight duties.

Finally, I would like to say that we are in a peculiar moment in our history that makes this issue particularly urgent. Everything I have just said about overclassification could have been said 10 years ago or 20 years ago. This is a stubborn and persistent problem, but there is something different today. We are living in a period of unusual political instability that I believe requires even greater transparency. Almost every day, we see increased expressions of hostility against religious and ethnic minorities. So-called fake news has lately resulted in actual acts of violence here in Washington, D.C., in the past week. And it seems that our political institutions are under a subtle form of attack by foreign actors, as the ranking member discussed. This is not a normal situation, and it is not the way that things have always been.

What complicates things further is that the incoming administration, at least during the election cycle, has indicated policy preferences that depart significantly from existing law and policy in areas such as foreign policy, questions of whether or not to engage in torture, questions involving freedom of religion. In some cases, these raise basic constitutional issues. So the bottom line is that we are entering a turbulent time. Reducing overclassification and increasing transparency will not solve our problems. But if we fail to reduce overclassification, we are going to make those problems

worse and harder to solve. Thank you again for holding this hearing and for the essential work of oversight that you do. I would be glad to answer any questions you may have.

[Prepared statement of Mr. Aftergood follows:]

Testimony of Steven Aftergood
Director, Project on Government Secrecy
Federation of American Scientists

Before the
Committee on Oversight and Government Reform
U.S. House of Representatives
Hearing on

Overclassification and Other Failures of the Classification System

December 7, 2016

Thank you Chairman Chaffetz and Ranking Member Cummings for holding this hearing. My name is Steven Aftergood. I direct the project on government secrecy at the Federation of American Scientists, a non-profit policy research and advocacy organization. My project studies the operation of the national security secrecy system and advocates reductions in the scope of secrecy.

What Problem(s) Are We Trying to Solve?

Dissatisfaction with the government's system of classifying national security information is widespread. The President of the United States, senior intelligence officials, members of Congress, frustrated FOIA requesters and others have all criticized secrecy policy at one time or another.

But they are not all talking about the same problem. Some of the various objections to current classification policy that have been raised include these:

- Classification restricts desired information sharing
- Classification impedes congressional oversight
- Classification undermines government accountability
- Classification limits public awareness of national security threats
- Classification clouds the historical record of U.S. government operations
- Classification is inefficient and increases financial costs
- Classification is susceptible to massive single-point failures through unauthorized disclosures

All of these criticisms have some merit, I believe, but they are also distinct problems that are likely to require distinct solutions.

Even the term "overclassification" that is the subject of this hearing has a double meaning that may be a source of confusion.

Overclassification as used within the government usually means that information is classified at a higher level than it ought to be (e.g. Top Secret instead of Secret). This kind of overclassification limits information sharing to those who hold the higher clearance, and increases associated security costs. It can be resolved by reclassifying the information at a lower classification level.

But the word overclassification is also used, often by outside critics, to refer to controls on information that is classified when it shouldn't be. The concern is not about the level of classification, but rather about the fact that the information is classified at all. The only way to fix this kind of overclassification is through declassification and disclosure.

When Congress enacted the Reducing Over-Classification Act of 2010 (P.L. 111-258) requiring agency Inspectors General to investigate the problem, legislators did not include a definition of what they meant by "over-classification," nor did they indicate how to identify it. In the absence of such a definition, the Inspectors General assumed that information was overclassified whenever it did not meet the criteria set forth in the President's executive order on classification, but that it was properly classified if it did meet them. This understandable assumption totally missed the key problem of information that is overclassified yet still within the framework of the executive order.

So selecting the problem that is to be solved, and defining it precisely, is an important step towards devising a solution.

I will propose a particular version of the problem that I think deserves priority attention below. But first I would like to take note of two "all-purpose," general solutions that would improve classification policy across the board.

1. Shrink the Size of the Problem

All of the adverse effects of classifying information can be diminished by reducing the scope and volume of classification activity.

Even if we can't figure out exactly how to get classification "right," classifying less information means that the consequences of getting it "wrong" will be less severe. Obstacles to oversight and accountability will be reduced, financial costs will be diminished, barriers to information sharing will be lowered, and so on.

Remarkably, some progress has been made in recent years towards "shrinking the problem" in this way:

- The number of "original classification decisions" – or new national security secrets – has dropped to historically low levels in recent years,

according to estimates gathered and reported by the Information Security Oversight Office.[1]

- The number of "original classification authorities" – or individuals who are authorized to designate new classified information – hit an all time reported low (2,199 officials) in FY2015, also according to the Information Security Office.

- The national security clearance system for granting eligibility for access to classified information has undergone significant contraction. According to the Office of the Director of National Intelligence, the number of security-cleared personnel dropped from a recent high of 5.1 million clearances in 2013 down to 4.25 million in 2015.[2]

These are positive developments that can collectively help to make the problems of the classification system more tractable and more amenable to possible solutions. (And to bring the persistent remaining problems into sharper relief.) They should be encouraged.

2. Appoint Government Officials Who Value Open Government

"Personnel is policy" according to the Reagan-era slogan. In other words, the selection of agency leadership is likely to have a decisive impact on the execution of national policy. This is also true in the area of classification policy: choosing conscientious officials who favor open government is a highly effective way to correct many weaknesses of the classification system.

This is all the more true since there is an unavoidable element of personal judgment in the classification of information. Classifiers need to make certain assumptions about: the requirements of national security, the sensitivity of specific items of information, the unintended impacts of secrecy in a particular case, and other factors. Based on how they weigh such factors, they then decide whether or not to classify.

---

[1] Annual Report to the President for FY 2015, Information Security Oversight Office, July 15, 2016; available at https://www.archives.gov/files/isoo/reports/2015-annual-report.pdf ; and "Number of New Secrets in 2015 Near Historic Low," *Secrecy News*, July 29, 2016; available at https://fas.org/blogs/secrecy/2016/07/new-secrets-2015/

[2] "Security-Cleared Population Continues to Shrink," *Secrecy News*, June 30, 2016; available at https://fas.org/blogs/secrecy/2016/06/clearances-2015/

Those officials who are predisposed to open government and democratic values will conduct their official business accordingly, sometimes even when it seems contrary to their near-term interests. Those who are not so predisposed will favor secrecy, and may even take advantage of classification authority to advance their own policy agenda.

In a sense, the selection of national security officials may the single most consequential step in the proper implementation of secrecy policy. That is because it is hard to formulate a comprehensive secrecy policy that will fit every conceivable circumstance. But a wise official will act properly despite an inadequate written policy. On the other hand, an imprudent official will not be constrained by even the most carefully crafted statement of principles and procedures.

This is a particular concern at this historical moment, when some of our elected officials and their designated appointees have engaged in reckless and irresponsible speech.[3]

Next, Define a Performance Goal

To move beyond general reductions in unnecessary secrecy ("shrinking the problem") and the good faith exercise of classification authority -- both of which are desirable under any circumstances -- it is necessary to set a performance goal and then to pursue it.

But just as there are numerous facets to the problem of secrecy, there are multiple potential goals that could be pursued: Should we seek to reduce the cost of the classification system? Expedite declassification of historical records? Enhance congressional oversight of classified programs? Expand sharing of classified information? Increase protections against unauthorized disclosures?

These are not necessarily incompatible objectives, but they involve different areas of emphasis that are likely to require different approaches.

Speaking for myself – as an individual citizen and advocate – I would say that the most important task is to modify secrecy policy so as to increase government accountability to the public. That means that special efforts should be made to reduce secrecy concerning military conflict, intelligence policy, foreign relations, defense spending, and other major areas of national security policy.

---

[3] See, e.g., "The Disruptive Career of Michael Flynn, Trump's National-Security Adviser," by Dana Priest, The New Yorker, November 23, 2016; available at: http://www.newyorker.com/news/news-desk/the-disruptive-career-of-trumps-national-security-adviser

Although those categories may seem very broad, adopting government accountability as the guiding principle for secrecy reform would actually simplify the problem and focus efforts to mitigate it. That's because not all classified information is relevant to questions of accountability; there is a great deal of secret information that is of little or no value for that purpose. So, for example, in most cases it would be of no concern to the public if some specific component of a military platform or weapon system were classified, overclassified, or altogether unclassified. There may or may not be valid reasons to protect such information, but if enhancing government accountability is the priority, then the classification status of some detail of military hardware will usually be of little or no interest.

By contrast, prioritizing government accountability would dictate reduced secrecy and heightened disclosure concerning the justifications for U.S. military action, the consequences of such action, and the parameters of U.S. military and intelligence policies.

The Role of Congress / Legislative Options

What can Congress do to encourage improvements in national security classification policy? There are lots of possibilities.

- *First, do no harm*

Of course, Congress should take no action that would aggravate the existing problems of secrecy. As noted above, significant progress has recently been made in slowing the pace of classification activity, reducing the number of classifiers, and shrinking the security clearance system. These are wholesome trends that should be encouraged, not reversed. Recent breakthroughs in disclosure such as declassifying the size of the U.S. nuclear stockpile, disclosing the annual intelligence budget appropriation and request, and declassification of historical editions of the President's Daily Brief should also be preserved and built upon, not reversed.

Regrettably, however, there has been a notable erosion of transparency standards this year with the refusal of President-elect Trump to release his tax returns prior to the election (or since). This is not a matter of national security secrecy *per se*, but the President's finances could easily have national security implications if they create conflicts of interest. In any event, such disclosure had been a routine practice among presidential candidates of both parties for four decades. Today it can no longer be taken for granted.

- *Conduct regular oversight of the secrecy system*

Congress should signal its interest in classification policy by conducting regular oversight of the secrecy system. Each year, the Information Security Oversight Office

produces an annual report to the President concerning government-wide classification and declassification activity. Release of this report would be a fitting occasion for legislators to review the latest trends in national security secrecy, and to examine what is working and what is not. Likewise, the ongoing production by the U.S. State Department of the *Foreign Relations of the United States* series -- which incorporates declassified historical records to produce a "thorough, accurate and reliable" account of U.S. foreign policy – would also benefit from periodic congressional oversight, but practically never receives it. Throughout the budget cycle and in the course of oversight, Members should also routinely ask government officials to explain and to justify their national security classification practices.

- *Provide adequate funding for declassification and internal oversight*

Declassification – whether of historical records or of current policy and program information – cannot proceed without the requisite funding. Without adequate funding, a backlog of materials awaiting declassification quickly builds up, agency responsiveness to declassification requirements slows down, and dysfunction ensues. Congress should provide stable, predictable funding to ensure this does not occur.

Because declassification is part of the "life cycle" of classified information (at least in the case of those records that are deemed to be permanently valuable), it would be reasonable to allocate funding for declassification as a normal part of the budget for managing classified information.

In order to maintain viable internal oversight of executive branch classification activity, Congress should also provide robust funding for the Information Security Oversight Office (housed at the National Archives), and for agency Inspectors General.

- *Prioritize topics of special interest for declassification*

It is well within Congress's power to select and to mandate declassification of topical areas that are of particular public or congressional interest.

This was notably accomplished in the case of the John F. Kennedy Assassination Records Collection Act of 1992, which established an Assassination Records Review Board. The Board led a highly productive declassification effort that yielded millions of pages of records.

This example could profitably be replicated, even if on a smaller scale, to address declassification of other issues of current interest.

- *Legislate a secrecy system?*

It is also within Congress's power to legislate a statutory foundation for the national security classification system, as it has in fact done for control of atomic energy information in the Atomic Energy Act.

The case for such a statutory classification system was presented in the 1997 report of the Commission on Protecting and Reducing Government Secrecy (the Moynihan Commission). A bill to that effect was actually introduced in the 105th Congress (S. 712) and was the subject of hearings before the Senate Governmental Affairs Committee.[4] But the fact that the bill never made it out of committee is an indication that this is a politically difficult undertaking that may not be worth the effort. Congress can assert its interests in classification policy effectively in other ways.

- *Repeal the "Kyl-Lott Amendment"*

Congress could expedite the declassification of historically valuable records by repealing a measure known as the Kyl-Lott Amendment that was enacted in the FY1999 Defense Authorization Act (Public Law 105-261, section 3161).

That measure was adopted in response to inadvertent disclosures of classified atomic energy information that occurred occasionally in the 1990s in the course of declassification of historical records. It required a dedicated audit or review of entire record collections to screen them for protected atomic energy records before declassification could proceed.

While this cumbersome approach may have made sense at the time, the improved quality and professionalism of current declassification activities at National Declassification Center render it an unnecessary obstacle to declassification today. Its repeal would help to streamline and improve the efficiency of declassification.

- *Address the legacy of congressional secrecy*

For more than half a century, congressional committees have periodically held closed hearings on sensitive or classified topics. Defense and intelligence committees routinely enact classified annexes to the annual authorization bills they mark up. Much of this material is likely to be of profound historical and even contemporary public interest. But there is no mechanism for bringing it to light. As you know, the Freedom of Information Act does not apply to Congress.

The Office of the Historian of the House of Representatives could be asked to formulate a plan, in cooperation with the relevant committees, for curating these

---

[4] Prepared testimony from that March 25, 1998 hearing is available here: http://www.fas.org/sgp/congress/hr032598/index.html

secret archives, identifying those collections that have enduring value, and initiating their orderly declassification and disclosure.

- *Task GAO to identify best practices and new options*

While the overall framework of the government-wide classification system is set by executive order, actual classification practices differ from agency to agency. Government agencies naturally vary in their commitment and competence with respect to information security and disclosure. Also, the secrecy required for military operations, for example, is qualitatively different from the secrecy needed for intelligence sources, and both differ from diplomatic secrecy.

This Committee could task the Government Accountability Office to identify those best practices in national security classification and declassification that could be broadly adopted by multiple agencies. GAO could also be asked to survey options for enhancing the performance of the classification system.[5]

*

In short, there are many constructive steps that Congress could take to help improve the functioning of the national security classification system, and to make it more responsive to the broad public interest.

---

[5] The FY 2017 Intelligence Authorization Act (H.R. 6393), adopted by the House on November 30, 2016, included a provision (Section 708) to require the Director of National Intelligence "to review the system by which the Government classifies and declassifies information" and to develop recommendations to improve it.

Chairman CHAFFETZ. Thank you.

Mr. Blanton, you are now recognized for 5 minutes.

STATEMENT OF TOM BLANTON

Mr. BLANTON. I am certainly not going to match those timings. He did 5 minutes. He did 4 minutes. It was outstanding.

Thank you, Mr. Chairman, and thank you, Ranking Member Cummings, and thank you other distinguished members of this committee for having me here today.

I am here to make three points: One of them is a thank you for the Freedom of Information Act amendments that you all mentioned, because it is a model for what you can do here on classification.

Second is to reinforce the message of that Moynihan Commission report. It was actually Moynihan, Combest, Jesse Helms, John Podesta commission. So you can tell when it is a unanimous bipartisan, it is something to pay attention to. And the number one recommendation was to pass a law to govern and fix this system.

The third thing I am here to tell you is that, when a security official—officials—tell you something is classified, don't believe them. Most of the time they are wrong. Fifty to 90 percent of the time, as the chairman commented, they are wrong. So don't believe them. I am going to back that up with a few examples.

But, first, the Freedom of Information Act amendments and why that is a model. You have already had an impact. You all, this committee was the leaders in this House of Representatives to get those amendments passed, and already the Central Intelligence Agency has released its Bay of Pigs draft history that they locked up for 30 years. On what grounds? Well, when you read it, you find out the grounds. The historian who wrote it and drafted it said: "After more than 20 years, it appears that fear of exposing the Agency's dirty linen, rather than any significant security information, is what prompts continued denial of request for release of these records." That is the norm in the bureaucracy. Your amendments broke this loose. The CIA historian wrote on the back: Well, shucks, recent 2016 changes in the Freedom of Information Act require us to release some drafts that are responsive to FOIA requests.

You did it by statute. That is the Congress' role. You can do it to the classification system. And I recommend the detailed list of recommendations in the back of this extraordinary report, the Moynihan-Combest report, for how you can do that. You can build in cost-benefit into the originating classification decision. You can build in assessments of, what is the real risk? What is the real vulnerability? What is the stream of cost to the public and to efficient government operations from classifying? You can do that on the front end. You can build in a declassification board with power to release so you get a rational declassification on the back end so the system doesn't get completely gummed up with unnecessary secrets. You can move those 50 to 90 percent of what shouldn't be secret out to the public. You can do that, but you have got to do it by statute. As Bill Leonard says, the government is not going to fix itself. You have got to do it.

My third point is just don't believe them on classification. Last month, we got a nice, you know, letter from the Joint Chiefs of Staff in answer to a Freedom of Information request. That is the document they gave us. It is all blacked out because releasing it would damage our national security, seriously damage it. This is at the secret level, right? It was fascinating because our staff person took a look and said: Oh, that is the Joint Chief's advice on a Presidential policy directive back in July of 1986. That looks kind of familiar.

And he flipped back in the files. Turns out we got it in 2010 in full. That made us go look at the cover letter. You know what the cover letter says? It says: We have coordinated your Freedom of Information review in consultation with the Joint Staff and the National Security Council. This is from the Office of the Secretary of Defense. It says OSD and NSC have no objection to declassification in full. However, Mr. Mark Patrick of the Joint Staff thinks it ought to be classified, and thus you got the black blotches. Classic case. One office doesn't agree with another office. One says it has been released for 6 years. Another says it is going to damage our national security.

Attached to my testimony, I got a half dozen other examples where it is not even one office and another office. It's the same reviewer one week apart had diametrically opposed views of what would damage our national security from release. So, bottom line, Mr. Chairman, Ranking Member: Don't believe them. Thank you very much for your time. I welcome your questions.

[Prepared statement of Mr. Blanton follows:]

Testimony of Thomas Blanton, Director, National Security Archive, George Washington University, www.nsarchive.org

To the Committee on Oversight and Government Reform, U.S. House of Representatives

Hearing: Examining the Costs of Over-classification on Transparency and Security
Wednesday, December 7, 2016
Rayburn House Office Building, Room 2154, 9 a.m.

Chairman Chaffetz, Ranking Member Cummings, distinguished members of the Committee, it is an honor to be invited to testify today before this Committee, which provided so much leadership for the passage this year of the Freedom of Information Act amendments, signed into law by President Obama on June 30.

Already your far-sighted reforms have driven real change in the bureaucracy. For example, the CIA finally had to release their internal draft history of the Bay of Pigs disaster, revealing – horrors! – that the Agency suffered a nasty internal power struggle afterwards – hardly a national security secret, just bureaucratic "dirty linen," as the suppressed history remarked. The 25-year sunset you imposed on bureaucratic drafts, on agency deliberative process, the 5th exemption to the FOIA, really works. Thank you!

That success, the 25-year rule, and your whole legislative approach to reforming FOIA, needs to be applied here today, to the classification system. It's time for Congress to step up to its Constitutional Article I responsibilities and write a law to govern an out-of-control, dysfunctional, counter-productive classification system. Until now, you've pretty much left it to the Article II folks, who claimed as much power as they could get away with in the name of the Commander-in-Chief.

A law to govern classification – that was the number one recommendation of the Moynihan Commission 20 years ago. They asked me to testify back then, and I'm sorry to report today that most of what they recommended never happened. It is worth looking back in order to look forward.

That Moynihan Commission was quite an effort. The formal title was "The Commission on Protecting and Reducing Government Secrecy" – some people saw that as contradictory, protecting and reducing, but I believe this is just the common sense notion that the only way you can truly protect the real secrets is by releasing the non-secrets. The Commission report quoted Justice Potter Stewart in the Pentagon Papers case, saying "when everything is classified, then nothing is classified." My own metaphor at the time was: We have low fences around vast prairies of classified information, when what we need is high fences around small graveyards of what could really hurt us.

I'm here today to tell you, we're still stringing two strands of barbed wire around the prairies. To compound the problem, we're deploying our armored cars to go round up unclassified emails like Hillary's, instead of focusing on the real hazards, like the millions of hacked security clearance files at the Office of Personnel Management. I'll come back to that point, about priorities, about whether you can believe anything a securocrat tells you about what's classified (you can tell from the outset that I'm a skeptic). But let's start with the lessons from the Moynihan Commission.

The Moynihan Commission came up with unanimous bipartisan recommendations – and not just the usual suspects – not only Pat Moynihan, Democrat of New York, but also Jesse Helms, Republican of North Carolina, John Podesta of Washington D.C., and Larry Combest of Lubbock, Texas, then the Republican chair of the House Intelligence Committee. Among others.

The Moynihan Commission reported a range of findings about how much over-classification there was. From insiders administering the classification system, they received testimony that the problem was only a 5-to-10-per-cent overage. But the final report treated with far more credence the estimate from President Reagan's top National Security Council staffer, Rodney B. McDaniel, that only 10 per cent of classification was for "legitimate protection of secrets." (Commission report, p. 36). That is, 90% over-classification.

My own experience at the National Security Archive, with more than 50,000 Freedom of Information Act requests over 30 years, and millions of pages of declassified documents, tells me that McDaniel is especially on target with his 90% when it comes to historical records. For more current information,

you can't get a more informed and independent view than from the head of the 9/11 Commission, Republican Governor Tom Kean. Kean was looking at all the intelligence on the 9/11 attacks, all the signals intercepts and CIA assessments of Al Qaeda, and commented publicly that too much secrecy had been part of the problem that left our country vulnerable: "Three quarters of what I read that was classified should not have been." (Cox News Service, July 21, 2004) So 75% over-classification on very current national security information.

The Moynihan Commission was greatly impressed with the costs of secrecy – not so much the dollar costs, however substantial, but the detriment to open research that would keep the United States ahead of the rest of the world technologically. A central theme of the Moynihan report concerns the ways classification retards scientific and technical progress by compartmenting information and stifling the scientific method. One 1970 study organized by scientists and cited by the Commission even suggested that "more might be gained than lost" if the U.S. unilaterally adopted "a policy of complete openness in all areas of information," but given existing realities, recommended a 5-year sunset on scientific and technical classification. In effect, the Moynihan Commission attributed the American national security advantage to our society's open flow of information, rather than the potential development of thicker vaults to rival the Kremlin's.

That finding is still true today. No less an authority than former Los Alamos Laboratory director Siegfried Hecker describes in his latest book, *Doomed to Cooperate* (p. 402), how excessive secrecy and compartmentalization actually produces a "negative impact on nuclear weapons stewardship." Hecker criticizes government "overreaction" to allegations of security breaches, ramping up security at the expense of the research environment in ways that have "undermined the effectiveness of the labs."

After extensive hearings, the Moynihan Commission concluded that our secrecy system was broken and needed a statute to fix it. That law would mandate changes to the thought process around making the initial classification decision. The classifiers should have to consider the public interest in release, the cost-benefit ratio, the actual vulnerability of the information, the long-term cost of keeping the secret, and not just whether it might damage national security, but all the other factors including the benefit from disclosure.

Key to the new statute would be a new concept of a "life cycle" for secrets. Restrain the decision on the front end so you have fewer to start with. Continuously push the unneeded secrets out of the system so they don't stack up and gum up the information flows you need in any efficient decision-making process. Minimize the amount you keep for the long haul, by using sunsets like the 25-year-rule and automated processes for release.

I have to say, this was especially prescient. The World Wide Web was only a couple of years old at the time of the Moynihan Commission report (1997). Google was still a year away from even launching. But already electronic systems were proliferating documents at a rate the old carbon-copy secretaries would never have imagined. What we now know is no matter how far you reduce the number of "original classification authorities" and no matter how far you bring down the number of "original classification" decisions, the capacity of computer systems to produce infinite copies means that the classified universe is expanding faster than the Big Bang. That means the costs keep going up – $16 billion plus in the last fiscal year – and even more of a problem, the declassifiers will never catch up. That's why we need a statute that puts some automatic sunsets into the mix: no more page-by-page reviews, if a document is in a certain category, it's public after 10 years or 25 years.

The bureaucracy will object. They'll say every document has to be reviewed in case there's a Social Security number in there, or a phone number, or other data protected by the Privacy Act. But this is a formula for perpetual backlogs, a system that chokes on its old secrets, and of course, full employment for retirees doing the reviews. Instead, we need to apply computing power to search and sort and protect privacy – standard formats like SSNs and phone numbers should be the easiest for automation to deal with.

The Moynihan Commission also recommended creating a central office to run classification policy. They found all kinds of confusion and bureaucratic tussling between the Security Policy Board and the Information Security Oversight Office. Frankly, as an outsider, I didn't see this issue nearly as interesting as the bureaucrats found it. But what we ended up with, as a combination of the Commission's attention to this problem, and the 1995 Executive Order that set up an appeals process for mandatory declassification review requests, was an interagency panel that has been a rousing success – not least as a result of its staffing from the ISOO.

This is the Interagency Security Classification Appeals Panel – or Icecap as we call it. The Panel has overruled the agencies in favor of requesters more than 70% of the time – yet another hard data point about over-classification. Turns out that simply moving the decision about declassification out of the hands of the original agency makes a huge difference, even when the originators still have a say. Yet, as useful as the Panel's decisions have been, we've seen little evidence that the bureaucracy has learned anything from them. We have to keep going back to the Panel, and the backlog there keeps growing, with some cases dating back a whole decade.

In my Moynihan testimony 20 years ago, I highlighted the huge successes in declassification that Congressional statutes had accomplished in creating the Nazi War Crimes board and the Kennedy Assassination Records Board – those two reviews combined to compel the release of tens of millions of pages of historically valuable records that would have otherwise remained secret indefinitely. Without these statutes, we would never have seen the CIA's file on Adolf Eichmann, or on Eichmann's deputy whom the CIA recruited after the war and installed as a well-paid vice president at Proctor&Gamble in Cincinnati. These records were technically still classified, but the Congress made a finding in law that the public and historical interest outweighed the bureaucratic factors. We need such a finding across the board on classification, in statute, with an oversight board that can order openness and re-balance the secrecy teeter-totter.

But instead of a government-wide Declassification Board that could break the logjam on whole series of historical files, we got the limited ISCAP handling only mandatory review appeals (and only a few hundred of them, usually for individual documents), authorized by Executive Order rather than statute.

Congress did legislate an advisory function in this arena, the Public Interest Declassification Board. The Pidib (as we call it) has become a helpful and responsive sounding board, producing useful recommendations, and even weighing in on some priority declassifications; but it is not the kind of drag-the-quarry-back-to-the-cave operation we need, or that the JFK and Nazi war crimes boards provided.

The statute you write needs to combine the ISCAP and the PIDB, by adding outside blue-ribbon nominees to an inter-agency panel of insiders, and

giving the new body the power to overrule agencies and order the release of batches of documents. The new body should turn its decisions into binding guidance on the agencies. Such guidance is desperately needed.

The Moynihan Commission recommended that the CIA Director produce a new directive that would only withhold sources-and-methods information if there was a demonstrable harm from release, not just any and every method. Such a directive has never happened, and there's hardly a CIA Director born who would ever give away power so cavalierly. So Congress has to do it, put this recommendation into the statute, there has to be demonstrable harm from the release of the source/method or else it can't be withheld.

Instead of a rational cost-benefit approach, however, the last 20 years have only demonstrated the CIA's burka approach to redaction. Look at the President's Daily Briefs that the CIA produced for Presidents Kennedy and Johnson and finally declassified (partly) last year. We had gone to court to get the Briefs released for their historical value, but the CIA opposed us on the grounds that the very document itself was an intelligence method. After the courts finished laughing at this, they allowed the CIA to withhold the two Briefs we had asked for (from Lyndon Johnson's presidency), but denied the CIA's claim for a "per se" exemption for all the Briefs.

With some pushing from the CIA's own historical advisory group, the CIA finally started releasing the Briefs last year, even though many looked like Swiss cheese from the redactions. One white blotch seemed familiar – the claim was "sources and methods" – but we already had a copy we had used in the lawsuit, found at the LBJ Library before the CIA began its absolutist claim. That censored paragraph? Our other copy showed the redacted source was our United Nations mission quoting foreign officials in New York.

What's the secret? My guess is that the CIA doesn't want us to know that sometimes somebody in the State Department can actually come up with useful information.

Another major Moynihan Commission recommendation focused on centralizing declassification in a National Declassification Center. This took about 10 years to see the light of day (that's one measure of bureaucratic resistance).

The NDC does exist, and cranks out the low-hanging fruit from the classified trees, but it has little power over the agencies, and continues to pursue a hugely wasteful approach where one classified word can keep a document denied from release, and send it into the pile that has to be re-reviewed down the road. That pile has taken on Jack-and-the-Beanstalk proportions. Here the Moynihan Commission apparently bowed to the wishes of CIA director John Deutch and said the NDC "would not supersede agency control" over declassification decisions. A decade of real experience shows that if NDC keeps avoiding any superseding, the backlog of historical classified records will overwhelm the system, especially with the tsunami of electronic records already in the pipeline.

We need to draw a line at least on the historical records – after 25 years, agencies have to turn over to the NDC the authority to declassify, and if the agencies want to keep a hand in, they have to put in real funding and real detailees into the NDC process. Even so, the NDC should make the decision, not the cold dead hands of the bureaucracy.

This is especially true at the Presidential Libraries, where the process to open records is excruciatingly slow. My organization obtained Mikhail Gorbachev's transcript of his Malta summit with President George H.W. Bush two decades before the Bush Library was able to declassify the American version. Now, 25 years after the end of the Soviet Union, we're finally able to publish all the summit conversations between Gorbachev, Reagan, and Bush – and the American side, not the Russian side, was responsible for almost all the delay. At the Presidential Libraries, a researcher has to file a Freedom of Information request just to get a group of files "accessioned," which can take years, and then come back to the library, go through the boxes full of withdrawal sheets listing still-classified documents, and file individual Mandatory Declassification Review requests for those, which takes more years. The National Declassification Center should be a geyser of Presidential records, centralizing the review, saving time and money. A new statute on classification could make it so.

As for the other Moynihan Commission recommendations on areas like standardizing security clearance procedures, I can't speak to those. Not my expertise. I've never had a clearance, and I don't want one. I remember the late 18-term Congressman George Brown, who saw the commercial potential in spy satellites (we take it for granted today in our traffic apps and Google maps), but the securocrats prohibited him even from talking about

the possibility, so he resigned from the House intelligence committee so he wouldn't be bound and gagged.

Well, that's what a single securocrat can do today. Bind and gag by claiming classification. Other officials with equal or more seniority and expertise may well disagree, but all it takes is one securocrat and the whole system grinds to a halt.

Let me show you our latest example. At the National Security Archive, we're hardly even surprised any more. We've been publishing these compilations called "Dubious Secrets" on our Web site for more than a decade now – side-by-side examples of different versions of the very same document, one section blacked-out here, but left in full over there. Sometimes the documents have almost mirror image redactions, so when you slide them together you get the whole text.

In other words, I'm about to show you some documents that senior government authorities with the power to say so insist are classified. Yet at the same time, these very same documents have been declassified by senior government authorities also with the power to say so. All of which is to say, don't believe them until you see for yourself. Always ask, where's the damage?

Here's a document still classified, you can see all the black blotches, this was a decision just a month ago, in November. The Joint Staff at the Pentagon deemed this document very sensitive, even though it dated all the way back to 1986, 30 years ago, and it was about the Soviet Union, a country that no longer exists. But the document looked familiar. Our expert on the topic, Dr. Bill Burr, thought he'd seen that headline and title before, and he poked around in our files. Sure enough, back in 2010, the Headquarters staff at the Pentagon had declassified this document from a copy in another file. In full.

So now we can read from six years ago the text that the Joint Staff thinks, right now today, is really sensitive, classified, worth spending taxpayers' dollars on protecting, can't be looked at by you or us in any public setting. And what's in there? Just the Joint Chiefs' comments on a draft presidential directive for our mid-1980s strategy against the Soviet Union. No weapons systems design. No intelligence assets. It's a waste of the Committee's time even to read this out loud.

That made us go back to the cover letter on this document, this November. In there, the Pentagon tells us that neither OSD (Office of the Secretary of Defense) nor NSC (National Security Council) had any objection to declassification in full, but a single securocrat, Mr. Mark Patrick of the Joint Staff Information Management Division, decided to exercise his Sharpie, or his computerized black-out system. What a travesty of national security.

It gets worse. At least with the Joint Staff example, it's one office against another. But consider this piece of White House e-mail, originally sent to Colin Powell because he had missed the meeting. The declassification review, going through several thousand White House e-mails, looked at the version from Powell's user area first, and blacked out chunks from the top and bottom sections. A little over a week later, the review dealt with the sender's copy, as written by the meeting note taker. This time, the middle section was whacked. We found out the punch line once both versions arrived and we put them together. The same person did the review both times – a highly experienced reviewer with TS/SCI clearances. He told me later there must've been something in the *Washington Post* the first time around that made Egypt and military aid seem sensitive, and the second time around he had forgotten the document and the only news stories were on the Iran-contra arms deals, so he blacked that out.

Fast forward from this piece of Colin Powell e-mail from the 1980s to February of this year, when somebody in the inspector-general line of work grabbed two of Colin Powell's e-mails from the account he had on the State Department unclassified system (his main account was with AOL.com) and deemed them classified. When reporters called Powell for comment, the former 4-star general, Presidential national security adviser, chairman of the Joint Chiefs, and secretary of state described the messages as "fairly minor" notes from ambassadors, and remarked, "I do not see what makes them classified." Later, Powell told NBC News (February 4, 2016), "I wish they would release them, so that a normal, air-breathing mammal would look at them and say, 'What's the issue?'"

That's what we'll ask when the purportedly classified Hillary e-mails ever see the light of day. When we actually get to read the declassified versions of those 110 or so messages in 52 chains, my bet is we'll find that those 8 chains supposedly containing TOP SECRET information started with newspaper stories, like the one in the *New York Times* about drone strikes in

Waziristan in 2011 while the then-chair of the Senate Foreign Relations Committee was visiting Pakistan – and neither he nor the ambassador Cameron Munter apparently were informed ahead of time. So millions of Americans can read the newspaper story and talk about it over the breakfast table or around the office water cooler, but not the Secretary of State. The CIA has effectively extended its capriciously high classification level covering the drone program, which was anything but secret even in 2011, to constrain the most basic diplomatic discussion of what's in the newspaper that day.

Already, one of the Hillary e-mails now classified at the SECRET level has emerged with enough metadata (the date and the To/From/Subject lines) to check with the author, Dennis Ross, a veteran of three decades at State and the National Security Council in highest-level negotiations and highest-level security clearances. Ross had emailed the Secretary of State in September 2012 with unclassified thoughts about the back-channel talks between the Israelis and the Palestinians. Ross told the *New York Times* (February 13, 2016) that nothing about the discussion should be classified, "It shows the arbitrariness of what is now being classified."

That's the problem: an arbitrary and capricious classification system that lacks internal and external credibility and contains too many secrets. This system shields government misconduct, obstructs Congressional and public oversight, retards scientific progress, and cedes enormous power to its enforcers, the securocrats. It's time to write a law that reduces government secrecy. Thank you for your attention and I look forward to your questions.

Attachments:

CIA President's Daily Brief, 8 June 1967, two versions, one released in 2015, one released in 1993.

Joint Chiefs of Staff, "Memorandum for the National Security Advisor to the President," 14 July 1986, two versions, one released in October 2016, one released in August 2010. Plus cover letter from Department of Defense, Washington Headquarters Services, to the Archive, 3 November 2016.

White House e-mail to Colin L. Powell from William A. Cockell, 21 January 1987, released in two versions less than two weeks apart in 1994.

Chairman CHAFFETZ. Well, thank you. We love your passion for it. It is good.

Mr. Amey, you are now recognized for 5 minute.

STATEMENT OF SCOTT AMEY

Mr. AMEY. That is a tough act to follow. Good morning, Chairman Chaffetz, Ranking Member Cummings, and members of the committee. POGO has always recognized the tension between openness and protecting legitimate government secrets, but the executive branch frequently overclassifies more information than is necessary and has developed new ways to conceal government information. Such obstructions create barriers to public deliberations on policy and government spending, impede sharing, and harm efforts to identify and remedy waste, fraud, and abuse. The 9/11 Commission said it simply: "Secrecy, while necessary, can also harm oversight." Sometimes the result of classification is not for the legitimate need of secrecy but the concealment of embarrassing information, which creates public distrust.

There are five main points that I want to briefly discuss today: overclassification, retroactive classification, controlled unclassified information, treatment in handling cases, and, finally, executive branch use of secret laws.

In overclassification, overclassification might be a form of either excessive redactions or improper markings. Reports by the National Security Archive and ISOO show that the classification process is mostly heading in the right direction, and we have seen some improvement over the last few years, especially considering the amount of electronic documents that have to be reviewed. But one number is a concern. In 2015, classification decisions were overturned in whole or in part in over 50 percent of the challenges. That was 411 cases overturned out of 814 decisions that were made. Additionally, we have heard stories about the lack of clarity and authority in standards leading different agencies to come to different conclusions, as Mr. Blanton just discussed.

POGO is also concerned about the lack of clarity about what constitutes intelligence sources and methods, which also can lead to overclassification.

And, finally, classifications aren't free. As the chairman mentioned, total security classification costs exceeded $16 billion back in 2015.

The Moynihan Commission had an excellent recommendation to improve the system: classification decisions, including the establishment of special access programs, no longer be based on damage to national security. Additional factors, such as cost of protection, vulnerability, threat, risk, value of the information, and public benefit from release, could also be considered when making classification decisions. POGO is in agreement that such factors should be considered to reduce executive branch secrecy.

On the issue of retroactive classification, for years, POGO has expressed concerns about questionable activities to retroactively classify government information. POGO has firsthand experience because we were involved in instances involving Area 51 and unclassified briefings to Members of Congress in a whistleblower retaliation case. POGO believes that any reviews of the classification

process should include a comprehensive look at issues affecting retroactive classification, including failures in the system to classify the information appropriately, how frequently it occurs, what considerations were given to the information, if it is publicly available, and what constitutes constitutional issues related to prior restraints.

On the issue of controlled unclassified information, there has been a proliferation of CUI, and by 2010, there were over 100 different CUI markings within government agencies. We have even witnessed examples of misuse, and POGO hopes that the committee will consider providing oversight of the implementation of the recently released CUI regulations. We have also even recently heard an example—and it was something that we had complained about during the process—that employees at DHS, when they were given FOIA training, were also instructed that, if they have a FOIA that comes in and the information is marked "CUI," it should not be released. And so that is opposite to the executive order that the President issued as well as the language that is in the final regulation from there and ISOO.

Unequal treatment in handling cases. In the past few years, we have witnessed numerous instances of mishandling of classified or protected information. I go into more detail in my written testimony, but POGO thinks that, if an intent is considered in high-profile cases involving senior officials, it should also be considered, as well as other factors, in whistleblower cases.

Secret law. POGO has voiced many concerns about the executive branch use of secret law. How we come to conclusions and striking the right balance between our security and our rights is imperative, and the legal interpretations cannot be cloaked in secrecy. Secret law poses a serious harm to our democracy.

POGO's written recommendations are in our written testimony, but I think there is one issue and point that the 9/11 Commission made that is important about nurturing—that the current system nurtures overclassification. There are no punishments for not sharing information. Agencies uphold a need-to-know culture of information, protecting rather than promoting a need-to-share culture of integration.

Thank you for inviting me to testify. I look forward to working with the committee and further exploring how to legitimately protect classified information and reducing government secrecy and cost. Thank you.

[Prepared statement of Mr. Amey follows:]

Testimony of Scott Amey, General Counsel
Project On Government Oversight (POGO)
before the
House Committee on Oversight and Government Reform

"Examining the Costs of Overclassification on Transparency and Security"

December 7, 2016

Good morning Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee.

Thank you for inviting me to testify today about the state of the federal government's classification system. I am Scott Amey, General Counsel with the Project On Government Oversight (POGO), a nonpartisan public interest group. Founded in 1981, POGO investigates and exposes corruption and other misconduct in order to achieve a more effective, accountable, open, and ethical federal government. I am pleased to testify before you on how best to reduce overclassification and to improve openness.

Throughout its thirty-five-year history, POGO has always recognized the tension between openness and protecting legitimate government secrets. But the executive branch frequently overclassifies information and more recently has created a pseudo-classification, Controlled Unclassified Information (CUI), which unnecessarily hinders Congressional and public access to government information. Such obstructions create barriers to legitimate public deliberation on domestic and foreign policies and government spending. Furthermore, secrecy harms efforts to identify and remedy waste, fraud, and abuse. The 9/11 Commission said it simply: "Secrecy, while necessary, can also harm oversight." The Commission further added that even Congressional oversight is often "spurred into action by the work of investigative journalists and watchdog organizations."[1]

Sometimes the reason for classification is not the legitimate need for secrecy, but the concealment of embarrassing information. Unfortunately, unjustified secrecy creates public distrust in government, impedes the sharing of information within the government, and raises questions about the protection of legitimate secrets.

[1] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, July 22, 2004, Report p. 103, PDF p. 120. https://9-11commission.gov/report/911Report.pdf (Hereinafter 9/11 Commission Report)

Overclassification

According to the *2015 Report to the President* by the National Archives and Records Administration's (NARA) Information Security Oversight Office (ISOO), original classification authorities are down,[2] derivative classification decisions are down,[3] and page reviews and declassifications are up.[4] On a less positive note, original classifications are up.[5] Certainly a mixed bag, but the trends are mostly heading in the right direction and we have seen a substantial improvement over the last few years, especially considering the amount of electronic documents that must be reviewed.

One number, however, highlights a major problem in the classification system. According to ISOO, of the 814 decided classification challenges that agencies closed in fiscal year 2015, the classification determination was overturned in whole or in part in over 50 percent of those cases (411 cases overturned out of 814 decided cases).[6] We understand that classifying information can be subjective. That said, that 50 percent of the challenged classifications were overturned shows that when agencies are asked to consider disclosing information to public review, they often make the wrong decision and choose unnecessary secrecy. Secrecy might come in the form of excessive redactions or improper marking. Either way, good government groups have been concerned that the executive branch classifies more information and records than it should.

Additionally, we have heard stories about the lack of clear authority and standards leading agencies to make different classification determinations. It's not uncommon for different agencies to have disagreements about whether to classify information or not. This issue was recently highlighted in the Hillary Clinton email controversy, with the State Department and the intelligence community holding differing opinions about the classification status of some of her emails.[7]

As noted above, classifying information isn't an exact science. For example, in the intelligence community there is a lack of clarity about what constitutes intelligence sources and methods, which can result in overclassification. A broadly worded provision in the National Security Act of 1947 to protect "intelligence sources and methods from unauthorized disclosure" has essentially required that nearly every piece of information in the intelligence community be concealed.[8] In 1997, the Moynihan Commission released its comprehensive report *Secrecy*, which included a recommendation to clarify the term source and methods to better explain the

---

[2] National Archives and Records Administration, Information Security Oversight Office, *2015 Report to the President*, July 15, 2016, Report p. 2, PDF p. 10. https://archivesaotus.files.wordpress.com/2016/07/isoo-2015-annual-report.pdf (Hereinafter ISOO Report)
[3] ISOO Report, Report p. 6, PDF p. 14.
[4] ISOO Report, Report p. 11, PDF p. 19.
[5] ISOO Report, Report p. 5, PDF p. 13.
[6] ISOO Report, Report p. 8, PDF p. 16.
[7] Lauren Carroll, Politifact, *FBI findings tear holes in Hillary Clinton's email defense*, July 6, 2016. http://www.politifact.com/truth-o-meter/statements/2016/jul/06/hillary-clinton/fbi-findings-tear-holes-hillary-clintons-email-def/
[8] Public Law 80-253, National Security Act of 1947, Section 102(d)(3), July 26, 1947. http://legisworks.org/congress/80/publaw-253.pdf

appropriateness of that protection.[9] Almost 20 years has passed, yet this common-sense recommendation has not been implemented. Instead there have been legislative efforts to expand the intelligence community's interpretation of sources and methods—efforts that were fought off by civil society groups as being ill-advised and unnecessary.[10]

And classification efforts aren't free. The government's total security classification cost for fiscal year 2015 was $16.2 billion, and contractors and other nongovernmental entities spent an additional $1.3 billion according to ISOO's report.[11] Overclassification adds to those costs and no doubt adds to other budget line items that cost agencies additional time and resources. If the 50 percent of overturned classifications statistics provides a rough estimate of the level of the problem throughout the process, then there are potentially billions to be saved by solving our overclassification problem.

Finally, even at current levels, declassification procedures cannot possibly keep pace, especially given the many obstacles to declassification that exist. Declassification efforts are improving, but more needs to be done. The House appears to agree, as last week it passed the Intelligence Authorization Act for Fiscal Year 2017, which includes Section 708 calling on the Director of National Intelligence to "review the system by which the Government classifies and declassifies information" and develop recommendations to make the system more effective, to improve information sharing, and to support the appropriate declassification of information.[12]

The Moynihan Commission had an excellent suggestion for how to make the system more effective when it recommended that:

> classification decisions, including the establishment of special access programs, no longer be based solely on damage to the national security. Additional factors, such as the cost of protection, vulnerability, threat, risk, value of the information, and public benefit from release, could also be considered when making classification decisions.[13]

POGO is in agreement that such factors should be considered to reduce executive branch secrecy.

Retroactive Classification

For years, POGO has also expressed concerns about the questionable activity of retroactively classifying government information. POGO has first-hand experience, having been involved in instances where an unmarked employment manual from Area 51 and a series of unclassified briefings to Members of Congress in a whistleblower retaliation case were retroactively

---

[9] The Commission on Protecting and Reducing Government Secrecy, *Secrecy*, March 3, 1997, pp. 70-71. https://www.gpo.gov/fdsys/pkg/GPO-CDOC-105sdoc2/content-detail.html (Hereinafter Moynihan Commission Report)
[10] The "FOIA Oversight and Implementation Act of 2016," H.R. 653, Section 2(b)(2)(A). https://www.congress.gov/114/bills/hr653/BILLS-114hr653rfs.pdf
[11] ISOO Report, Report pp. 32-34, PDF pp. 40-42.
[12] Intelligence Authorization Act for Fiscal Year 2017 (H. R. 6393, 114th Congress, 2015-2016), Section 708. https://www.congress.gov/bill/114th-congress/house-bill/6393/
[13] Moynihan Commission Report, p. 38.

classified.[14] POGO is concerned that in many instances, retroactive classification is more about clawing back embarrassing information or silencing whistleblowers than protecting legitimate national security concerns.

POGO believes that any reviews of the classification process should include a comprehensive look at the information at issue, the frequency of retroactive classifications, failures in the system to classify the information appropriately at the beginning, what considerations were given if the information was publicly available, and constitutional issues related to prior restraints that could violate the First Amendment.

Controlled Unclassified Information

The proliferation of controlled unclassified information (CUI),[15] formerly known as sensitive but unclassified (SBU) information,[16] has also been a problem for years. While we have all heard of classified information and realize the need to protect legitimately sensitive information, CUI fits into a very gray area. The use of the CUI markings rose dramatically after 9/11 as a way to manage all unclassified information that the executive branch believed required safeguarding or dissemination controls. By 2010, there were more than 100 different CUI markings. President Obama and NARA have tackled the problem through Executive Order 13556 and the overdue regulation to standardize and simplify the government-wide CUI program; however that program will not be fully implemented for several years.[17]

As is the case with overclassification, the confusing patchwork of CUI markings is wrongly restricting public access to information, failing to safeguard legitimately sensitive information, hampering information sharing within the government, and potentially concealing embarrassing information.

The Transportation Security Administration (TSA), in particular, is on the hot seat for its use of the "sensitive security information" (SSI) designation. A Department of Homeland Security (DHS) Inspector General (IG) report sharply criticized the way the TSA screened a draft IG report.[18] The IG wrote to TSA Administrator John Pistole questioning the decision to mark

---

[14] *POGO v. John Ashcroft*, Declaration of Danielle Brian in Support of the Plaintiffs' Motion for Summary Judgment and Opposition to Defendants' Motion to Dismiss, September 30, 2004. http://www.pogoarchives.org/m/gp/a/Brian%20Declaration.pdf

[15] President George W. Bush, Memorandum for the Heads of Executive Departments and Agencies, *Designation and Sharing of Controlled Unclassified Information (CUI)*, May 7, 2008. https://www.archives.gov/files/cui/documents/2008-WH-memo-on-designation-and-sharing-of-cui.pdf; Executive Order 13556, November 4, 2010. https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf

[16] Library of Congress, *Laws and Regulations Governing The Protection Of Sensitive But Unclassified Information*, September 2004. https://www.loc.gov/rr/frd/pdf-files/sbu.pdf President George W. Bush, Memorandum for the Heads of Executive Departments and Agencies, *Guidelines and Requirements in Support of the Information Sharing Environment,* December 16, 2005. https://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051216-10.html

[17] Controlled Unclassified Information, 81 Federal Register 63324, PDF p. 2, September 14, 2016. https://www.gpo.gov/fdsys/pkg/FR-2016-09-14/pdf/2016-21665.pdf

[18] Department of Homeland Security, Office of the Inspector General, *Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised)*, OIG-15-18, January 16, 2015 (Revised). https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-18_Jan14.pdf (Hereinafter DHS Report OIG-15-18)

several items in the report as SSI, and noted the conflict that the "very same office that initially and improperly marked the information as SSI" was the office that affirmed the original redactions to the report. The DHS IG also wrote:

> I believe that this report should be released in its entirety in the public domain. I challenged TSA's determination because this type of information has been disclosed in other reports without objection from TSA, and because the language marked SSI reveals generic, non-specific vulnerabilities that are common to virtually all systems and would not be detrimental to transportation security. My auditors, who are experts in computer security, have assured me that the redacted information would not compromise transportation security. Our ability to issue reports that are transparent, without unduly restricting information, is key to accomplishing our mission. Congress, when it passed the Reducing Over-Classification Act in 2010, found that over-classification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information."[19]

The report was redacted for public release and an unredacted version was sent to Congress.

That criticism follows the bizarre case involving Robert MacLean, a TSA whistleblower who was subject to retroactive labeling of information as CUI. In 2003, MacLean received a text message over an unsecured network to his unsecured phone announcing cuts to air-marshal coverage. The text wasn't marked with warnings, restrictions, or any other indicators that are used when messages, briefings, or other information contain classified or CUI (then called SBU). Concerned that the TSA was pulling air marshals off high-risk flights at a time when there was a heightened intelligence warning of potential hijackings, MacLean reported those concerns to his superiors and the Inspector General. Only after being told that "nothing could be done" and to "just walk away," MacLean decided to warn the public by contacting a reporter. His intent was to keep the flight cancelation plan from taking effect. His efforts paid off and after some media scrutiny and Congressional inquiries, the government admitted that the plan to remove the air marshals was a "mistake."

Three years later, in April 2006, the TSA fired MacLean for "Unauthorized Disclosure" of what they claimed to be SSI—despite the fact that the text message was sent over an unsecured network to unsecured phones and not designated in any way as sensitive. The Office of SSI did not actually label the message as SSI until August 31, 2006, four months after MacLean was fired. MacLean recently won his case before the Supreme Court.[20]

There are likely other instances, and therefore the open government community pushed hard to ensure that NARA's final CUI rule and related training materials included provisions that clearly state that CUI markings do not prohibit the release under FOIA and other public-release authorities or protected disclosures under whistleblower protection laws. Without a formal

---

[19] DHS Report OIG-15-18, Report pp. 2-3, PDF pp. 3-4.
[20] *Department of Homeland Security v. MacLean*, 574 U.S. __, 135 S. Ct. 913, January 21, 2015. https://www.supremecourt.gov/opinions/14pdf/13-894_e2qg.pdf

process, CUI dissemination controls are prone to abuse and will cause any employee to err on the side of secrecy—secrecy even in instances where the information might be publicly available or releasable under FOIA. Proving the point, POGO was recently informed that the Department of Homeland Security held a FOIA training session and there was a mention that if records are marked CUI they should not be publicly released. So while we might have won the battle to get openness protections into the CUI rule, more clearly needs to be done to win the war to overcome the perception that CUI markings prevent all disclosure.

On a positive note, POGO is deeply appreciative of NARA's efforts to engage in extensive consultations with open government advocates and stakeholders regarding a draft CUI directive and the final CUI regulation and guidance. Despite a lot of foot-dragging by federal agencies, NARA's openness was a great example of the government and civil society working together to get the system right.

Unequal Treatment in Handling Cases

In the past few years we have witnessed numerous instances of mishandled classified information, from Secretary of State Hillary Clinton to CIA Directors David Petraeus and Leon Panetta. In those instances, the handlers have suffered little or no serious consequences for the same infractions that have destroyed the lives of whistleblowers.

Robert MacLean spent more than a decade fighting to get back his job as a US air marshal after blowing the whistle on cutbacks that would have removed air marshals from certain flights during a time when the government was aware of a looming terrorist plot. DHS retroactively determined the information MacLean disclosed was CUI.

Thomas Drake, a decorated US Air Force and Navy veteran, was relentlessly prosecuted under the Espionage Act for his revelations of illegal domestic surveillance activities by the NSA.

It's worth noting that neither MacLean nor Drake ever released classified information; yet, their lives were turned completely upside down.

POGO isn't proposing harsher penalties against Clinton, Petraeus, Panetta, or others in high positions of power. Rather, we feel it necessary to highlight the double standard and demand better from our government. If the government is willing to consider the intent behind, and consequences of, infractions for high-level officials, it should do so for whistleblowers working in the public interest by exposing wrongdoing.

Hopefully today's hearing will lead to a balancing test that will be used when considering what repercussions individuals should face after having released CUI or classified information.

Recommendations

Overclassification remains a problem and has its costs, and for decades, many entities have worked to improve executive branch openness. The Moynihan Commission opened the door to

reducing overclassification.[21] The 9/11 Commission report also discussed concerns with secrecy.[22] The Public Interest Declassification Board (PIDB) is developing recommendations for a "more fundamental transformation" of the classification system.[23] Finally, some pieces of legislation to prevent overclassification have become law.[24] Despite all of those efforts, more should be done.

POGO offers the Committee the following recommendations:

1. The federal government should protect only legitimate national security and privacy concerns, and it should penalize agencies that violate that principle.
2. Congress should pass legislation clarifying the term "use of sources and methods."
3. Congress should pass legislation adding factors like cost, value of the information, and the public benefit from release to the criteria used when making decisions regarding classification and whether individuals who released CUI or classified information should face repercussions.
4. Congress should push for clear standards and authorities for resolving instances in which agencies make differing classification decisions.
5. Any future studies of the classification system should not merely look at check-the-box procedures, but also at what was classified and why, at retroactive classifications, and at CUI in order to determine whether the systems are effective and to identify abuses. Identifying the abuses can help reduce overclassification and improve training.
6. The government should adopt a presumption of disclosure which allows the public full access to all unclassified and uncontrolled information.
7. NARA should speed up the full implementation of the CUI Executive Order and regulation.

The 9/11 Commission made a point that is still valid today:

> But the security concerns need to be weighed against the costs. Current security requirements nurture overclassification and excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs—even in literal financial terms—are substantial. There are no punishments for *not* sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.[25] (Emphasis in the original)

---

[21] Moynihan Commission Report.
[22] 9/11 Commission Report, p. 417.
[23] National Archives and Records Administration, Public Interest Declassification Board, *About the PIDB*. https://www.archives.gov/declassification/pidb#about (PIDB)
[24] Public 111–258, Reducing Over-Classification Act, October 7, 2010. https://www.gpo.gov/fdsys/pkg/PLAW-111publ258/pdf/PLAW-111publ258.pdf; Clearance and Over-Classification Reform and Reduction Act (H.R. 5240, 113th Congress, July 29, 2014. https://www.congress.gov/113/bills/hr5240/BILLS-113hr5240ih.pdf
[25] 9/11 Commission Report, p. 417.

POGO recognizes that the tension between openness and secrecy in government continues to be extremely high. Abuse of FOIA, overclassification, retroactive classification, quasi-classification, and suppression of whistleblowers are all-too common. Even with some of the post-9/11 improvements to promote information sharing and reduce overclassification it might be time for a comprehensive review to ensure we are on the right path.

Thank you for inviting me to testify today. I look forward to working with the Committee to further explore how we can protect legitimate classified information and reduce government secrecy.

Chairman CHAFFETZ. Thank you. I appreciate all of the opening statements.

We will now recognize the gentleman from Michigan, Mr. Walberg, for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman, and thank you for holding this hearing. It is something that probably many of us have surmised was going on. It certainly goes to a frustrating level, and I appreciate the fact that, in this report that you pointed out, Mr. Chairman, "Pentagon buries evidence of $125 billion in bureaucratic waste," done by two reporters, one of which certainly has established credentials for doing investigative reporting, and we ought to take this seriously. But I think when I read this, the frustrating thing was the number of assertions that lawmakers don't want to do anything about this because of the impact in their districts. And certainly there is evidence to show that, but I think this committee has lawmakers better than that. I hope this is a real start.

Mr. Amey, according to that article in the Washington Post, the Department of Defense first commissioned and then hid—hid—the unflattering results, and did it aggressively, hid that, with retribution, offered threats, you name it, of the waste and efficiencies. Are you familiar with the report?

Mr. AMEY. Yes.

Mr. WALBERG. I would expect so. In your view, what reasons could the DOD have had to keep the results of the report from the public?

Mr. AMEY. Oh, boy, you are putting me on the spot. I'm trying to predict what the Department of Defense was thinking. I don't know. It is very difficult because the report is actually on the Internet. We found it yesterday when the story came out. It has been on the Internet since that time. The Defense Business commission actually had a slide presentation, a summary of the report, on its Web site, and so we are trying to actually figure out, and we actually reached out to the reporters to try to figure out where the secrecy was coming in and what was taking place. But I would imagine it is public embarrassment. I mean, at the end of the day, we are talking about the Department of Defense trying to protect $125 billion and the fact that they can't pass an audit and there is other scrutiny on top of them, that I think this was just an issue of "we didn't want this to get out and so let's try to keep it under wraps."

Mr. WALBERG. And I am sure $125 billion doesn't sound unreasonable to you?

Mr. AMEY. Oh, no, sir. I mean, we have been saying it for years that, between when you look at goods and services—most of my work is on contract oversight, and when you look at Department of Defense goods and services, we factored that, yeah, we are probably in the tens to hundreds of billions of dollars' worth of waste.

Mr. WALBERG. As I read that, it just goes back to simple truth that a bureaucracy will protect itself. And a bureaucracy does not want to be downsized in any way, shape, or form. But in a time of sequestration, at a time when our warfighters and their families, et cetera, are suffering reductions, for this type of dollar amount to be held over and attempted at least to be hid from us is unconscionable. To think that this could, as I have read, cover the cost,

the operational costs, of 50 Army brigades—that is pretty significant—or 3,000 F–35 strike forces or 10 strike forces of carriers, that is just unconscionable that this would have been disregarded and hidden.

What can Congress do to ensure that agencies engage in this type of self-analysis but then also use results to improve existing operations?

Mr. AMEY. It is a wonderful question because that is exactly what the point is, is, at the end of the-day, we have asked for inventories of contracts, of inventories of what we are buying, how many services are being provided. Unfortunately, there was actually a chart out a few years ago that said that the government doesn't often know how much the government is spending and what it is being used for, and so that is where we need to get to the audits, but specific audits—just not check the box, did people do X, Y, and Z?— we need specific audits of specific spending. GAO does a fairly good job. DCAA is involved in the process. But that is where I think we need to go a lot deeper into these specific programs and then get to the heart of why we see so many overruns on some of these programs. I mean, there is a lot of waste out there, and we just have to identify and then come to the solution on how to remedy it from the beginning. I mean, let's stop trying to put the milk back in the bottle after the fact. Let's do it at the start of the process before billions is wasted.

Mr. WALBERG. Well, I trust that, because of this hearing and others, I would assume that we can do that, plus starting new, afresh on January 20 as well, that this lesson will not be lost because, frankly, this is the number one responsibility of our Federal Government, to make sure that we have the resources available to do what is necessary to protect and defend our positions and not just protect a bureaucracy.

And I yield back.

Mr. HICE. [presiding.] I thank the gentleman.

The chair now recognizes the ranking member, Mr. Cummings, for 5 minutes.

Mr. CUMMINGS. Thank you, Mr. Chair.

Mr. Aftergood, I and many other Americans have serious concerns with reports of hacking and other actions by the Russian Government to interfere with the 2016 Presidential election. The intelligence community has confirmed that the Russian Government or its associated entities hacked the email accounts of individuals and political organizations before the Presidential election. The Director of the National Security Agency, Admiral Michael Rogers, said, and I quote: "There shouldn't be any doubt in anybody's minds. This was not something that was done casually. This was not something that was done by chance. This was not a target that was selected purely arbitrarily. This was a conscious effort by a nation-state to attempt to achieve a specific effect," end of quote.

Do you believe this is an important issue for our country? And I notice that, in your testimony, you talked about classification, and you talked about the state that we find ourselves in overall today, and I am just curious.

Mr. AFTERGOOD. Yeah. It is a crucial issue. The integrity of the electoral process is absolutely fundamental. If we don't have cred-

ible, authoritative elections, the foundation of our political system is washed away. So, yes, it is an extremely serious question. I think the blanket of classification that has been spread over it needs to be reevaluated. Even before that happens, Congress needs to understand exactly what did happen. There are actually several questions here. What kind of attack occurred? What are our vulnerabilities? And what steps can be taken to prevent future attacks of this kind? And I think all of those questions are wide open.

I would also say, though, that it is important that this not be construed as a sort of left-handed attack or attempt to undermine the incoming administration because that would only aggravate whatever damage has already been done, at least in my opinion. So I would hope that this be undertaken, as you said, on a bipartisan basis to say: Look, we have got a problem. We need to deal with it.

Mr. CUMMINGS. I agree with you. I think it is definitely a bipartisan issue. The FBI has refused to disclose any information about its investigation of these hacks. This is the opposite approach from the one the FBI took in the Clinton email investigation. I wrote to our chairman on November 17, 2016, to request that our committee conduct a bipartisan investigation into Russia's role in interfering with and influencing the Presidential election, again, not to take anything away from President-elect Trump, but just the idea of it, just should bother every single American. Even Republican Lindsey Graham, Senator Graham, called for an investigation into it. Outside experts have also called for Congress to act. A group of 158 scholars from colleges and universities around the country sent Congress a letter calling for a congressional investigation. A group of experts on cybersecurity defense and fair elections wrote, and I quote: "This evidence made available in an investigation might show that foreign powers have played an important role. It might show that such a role was negligible. At this juncture, we can only say that existing reports are plausible enough and publicly expressed enough to warrant Congress' full attention and swift action," end of quote.

Mr. Blanton, do you believe there is a role for Congress in investigating these allegations?

Mr. BLANTON. Yes, sir. To me, one of the great headlines of the whole election season appeared in the Washington Post on November 1 when the FBI was trying to explain why it didn't sign on to that statement from the Director of National Intelligence and the Homeland Security. And the headline read: "Comey was concerned publicly blaming Russia for hacks of Democrats could appear too political in runup to elections." That is the Washington Post headline. It is an interesting reticence as you point out. Congress should get your classified briefing, Congress should understand the hacking. There is a huge problem. We are constructing at the National Security Archive Web site at George Washington University a whole cyber vault, trying to get declassified much of the cybersecurity policy documents because, as former National Security Agency Director Michael Hayden said, one of the problems of cybersecurity is it was born classified. It grew up in this hothouse where it was all shielded by compartments, but what we really need in our society is a robust debate that involves academics, civil

libertarians, the tech companies, and this committee and this Congress. We have got to open it up. That cyber vault is beginning to get populated, but it needs more. It needs this Congress to get into this. It needs to press the intelligence community and Homeland Security to release the basis of their attributions. How do they figure that? That is the hardest part, as you well know, Mr. Cummings.

Mr. CUMMINGS. One last thing, Mr. Chairman. I have said it, and I guess, at 65, I look back and I am not so much worried about my life. I am worried about future generations. The idea, I mean, I just see, I am very concerned about our democracy. Mr. Aftergood, I appreciate your comments because it seems as if you can just chop away and chip away, and the next thing you know, you won't have a democracy. Do you all have similar concerns, any of you?

Mr. Leonard?

Mr. LEONARD. Yes, Mr. Cummings. You know, I think, obviously, my insights are only based upon what I have seen in open-source material and whatever, but I do know from being, based on my past experiences, this is something straight out of the Russian playbook. We have seen it repeatedly happen in Europe, especially in Eastern Europe and things along those lines. In fact, it is straight out of the KGB playbook during the cold war. It was known as special measures back then and the use of disinformation and things along those lines. So, clearly, it does go at the very fabric. And, again, this is an example of what I made reference to in my opening comment in terms of the impact that denying information to the Congress can have in terms of the Congress' own ability then to carry out its Article I constitutional authorities, which essentially is oversight.

Mr. BLANTON. If I could just make one more comment on that issue, I think we have got to look at this question of hacking and attribution and roles with an eye to, what is the long-term fix? If you look at what the Obama administration achieved with China, the price of a state visit for the head of state of China was that China had to stop its hacking. And that whole arm of the People's Liberation Army kind of went on hold. And the question—one of the first documents we published in the cyber vault was the directive that authorized our National Security Agency to do offensive cyber operations, and that was in 1997. That was in 1997. I think one of the things that Congress has got to look at when it is trying to figure out who is hacking us and why and what is the damage is, what is the fix? I think we are going to have to end up with new international norms governing cyber war because our country is the most vulnerable in the cybersphere. It is in our national security interest to impose rules on other folks and to cut the deals, like President Obama did with President Xi, to restrain us. To restrain them, it will also restrain us, but that is in our interest.

Mr. CUMMINGS. Thank you.

Mr. HICE. I thank the ranking member, and I would ask our panelists to help us keep within our 5 minutes. We have got a number of people who want to ask questions, so if we can work both ways.

The chair now recognizes Mr. Farenthold for 5 minutes.

Mr. FARENTHOLD. Thank you, Mr. Chairman.

Mr. Amey, you mentioned that there is no penalty for overclassification. What would you suggest that we do? Obviously, you would want some penalty for self-serving classification. What other areas, what would you suggest as a potential punishment, or do you just make it illegal with no punishment?

Mr. AMEY. Oh, I think there has to be some punishment. We can debate what the punishment will be, but there has to be some kind of civil, criminal, or administrative punishment that happens. I mean, currently, you know, things are marked, and at least with classification, there is at least a better process. A lot of what we have also been concerned with is this—in the old days, it was the FOUO—with the Controlled Unclassified Information, the CUI out there, is that anybody that thinks something can stamped "CUI," they put a stamp on it. And then, all of a sudden, that has a dissemination control on it. It can't be shared, and then there's questions on, well, wait a second, if people can't learn about it, how can we FOIA it? But I think you are absolutely right. We have to figure out what the punishment will be, and it may be something purely administrative. And I am sure the other panelists have some ideas on it as well, but I think there has to be something.

Mr. FARENTHOLD. All right. So let's talk a little bit. This committee has had pretty good success with the IG community where, within each agency, there is an independent inspector general that does investigations. We have had success with the chief information and chief technology officers under FITARA. Is there a model in which we create within all agencies a classification office? Or are we better off setting up something outside the agency, certainly on longer term, you know, move something within in the National Archives, where there is a method for declassification?

We will start with you, Mr. Blanton, and let anybody else weigh in.

Mr. BLANTON. Excellent question. All I can do is point back to some of the lessons of history, which are the times when we have had real success in forcing unneeded secrets out of the system was when Congress took action with the Nazi War Crimes records bill, with the JFK Assassination Records bill. It set up blue-ribbon panels outside and inside——

Mr. FARENTHOLD. Well, part of our problem here in Congress is we can do a lot of things. We need your suggestions on what specifically to do. I understand that that is probably more indepth we can get into in the 2–1/2 minutes that I have left. Let me let anybody else.

Mr. Leonard, do you want to weigh in?

Mr. LEONARD. Yes, sir. I am a big advocate of the IG's involvement in these types of issues. Having been external to agencies when I was at ISOO—I was part of the Federal Government but yet an outsider—I was very much limited to what I could do when dealing with CIA or even the Department of Defense or what have you. IGs don't experience those limitations to the same extent. Plus they also have the dual reporting responsibilities in both the executive and legislative branch.

Mr. FARENTHOLD. So your suggestion might be expand the responsibility of the IGs?

Mr. LEONARD. Absolutely. There was the 2010 Reducing Overclassification Act, which assigned specific responsibilities to the IG. I believe those types of things can be greatly expanded, and given the proper training, IGs can very effective in this area.

Mr. FARENTHOLD. Yes, Mr. Aftergood.

Mr. AFTERGOOD. One hopeful sign in current classification policy is the growth in classification challenges from within the system. The current executive order allows people who have access to classified information to challenge its classification status and to say: Wait a minute; this shouldn't be classified.

In the most recent year, the number of internal classification challenges reached a record high of more than 900. And of those challenges, more than 40 percent were granted. That is a trend that I think could be built on. If the system can be made more and more self-correcting where people inside the system themselves are finding errors and helping to adjust them——

Mr. FARENTHOLD. One final question before I am completely out of time. This committee and other committees often get classified information in response to our requests for information as part of our oversight responsibilities. Do you think it would be appropriate to create a mechanism for Congress once we have read that and said, "This is crazy, this doesn't need to be classified," do you think Congress should have the ability to declassify material? Does anybody think we shouldn't?

Mr. LEONARD. I believe Congress should. In fact, some committees by virtue of rules have empowered themselves with that option yet, to my knowledge, have never been acknowledged. It is a dicey issue, but two coequal branches of government and each have the——

Mr. FARENTHOLD. Mr. Amey, you look like you wanted to weigh in.

Mr. AMEY. Well, in the final CUI rule that is one of the things that we fought for. Originally, there was only allowed to be a challenge internally, and we fought that it could beinternally or externally. So, yeah, I would think that the same process should be applied to classified information as well.

Mr. FARENTHOLD. Thank you. I see my time is expired.

Mr. HICE. I thank the gentleman.

The chair now recognizes Mrs. Watson Coleman for 5 minutes.

Mrs. WATSON COLEMAN. Thank you very much, Mr. Chairman.

And thank you to each of you for raising what I think is a very important, complex list of issues, actually. And I recognize that we need to be talking about security first. We need balance. We need accountability. And we need fairness. And so this is a huge area with so many people interacting. In many cases, there is a disagreement among agencies and within agencies. And a lot has to be done here.

I wanted to ask a series of questions, and so I hope that you will answer them as sort of succinctly as possible, recognizing that you are only going to give me sort of the top lines.

I want to start with you, Mr. Blanton, because you testified about the recommendations of the Moynihan Commission more than 20 years ago, and I just want to have a reaction from you as

to why you think Congress has not moved to fix this classification system.

Mr. BLANTON. I am no expert on Congress, and I assume that you could give a far more sophisticated answer to that than I could. I think Steve Aftergood, I think, testified at one of the congressional hearings back in 1998, and that was when Senator Moynihan was alive and Senator Helms was alive. They were in powerful positions, and even they didn't push through their recommendations. My own sense is there wasn't enough of a notion of crisis, and we have got a crisis today I think in the classification system.

Mrs. WATSON COLEMAN. I think that you are quite accurate on that, that we may be in a situation right now where we are in an unprecedented environment.

Mr. Aftergood, would you like to comment to that?

Mr. AFTERGOOD. You know, the Moynihan Commission report itself included an appendix of previous studies from previous decades that had also not solved the problem, and here we are 20 years later looking back at the Moynihan Commission. I think it may be that the recommendation didn't quite capture the issue properly, and it seems to me that a law on secrecy is a means to an end. It is not the end. I would think about what is the end that you really want and then go for that. And the end that you really want is greater congressional control over what is or is not classified. Focus on that. Go for that. If there are particular areas, particular topical areas that need classification, declassification, mandate their declassification.

Mrs. WATSON COLEMAN. So probably the end result should be the kinds of things that I sort of mentioned when I opened up, the issue of security and balance and fairness and accountability, and how we get there.

Mr. Blanton, again, you talked about a possible reform that could be made by statute. One of those would be to implement a life cycle of secrets. Would you talk to me a little bit about what that is?

Mr. BLANTON. In the most straightforward version, it was in the Freedom of Information amendment, like a 25-year sunset for deliberative process. The reality of our classification system, one of the reasons it is entering crisis is we have got a tsunami of electronic records. The volume is—we are talking petabytes of information. We are not going to be able to do page-by-page review, which is what our declass system currently consists of. We are going to have to build in automatic releases for entire categories of records without review.

Mr. BLANTON. And that, I think, is going to be the only way to deal with those electronic records. So life cycle is just a kind of summary term to say you've got to put sunsets on the secrets, you've got to have better decisions on the front end that build in the sunsets, and then automatic release. Otherwise we're sunk.

Mrs. WATSON COLEMAN. I believe it was your testimony that I read where you said within this age of technology we can take care of those things that are sensitive in nature, personal information that could be deleted automatically if it's programmed to do so.

Mr. BLANTON. Yes, ma'am. That's the big holdup right now in releasing the State Department cables. They say they've got to look at every single cable to make sure there's no Social Security num-

ber or personal phone number in there. Well, I can't think of something that is more easily automated than searching and removing a Social Security number.

Mrs. WATSON COLEMAN. So help me to understand this, because I am a relatively new member. And I want to ask two questions here.

Number one is, is it currently a situation where each agency is responsible for classifying its information even though that information might be shared with other agencies and involve other agencies?

And, lastly, and anybody can respond to this, is there a proposal where this sort of classification consideration would go into a sort of multidisciplined entity where those things could be vetted under standards and circumstances and then sort of move in a way that agencies can sort of agree on the ground levels and would reduce the amount of classification?

Mr. BLANTON. That entity exists. It was recommended by Moynihan. The Congress and the Presidents put it—it's called the National Declassification Center. But the reality is it doesn't have the power, maybe the will, to override those agencies. So you get a constant equity referral where the agencies all get a bite at the apple. And one of the recommendations in my testimony is empower that center. Make the decisions. Do a sunset. If something's older than 25 years, that center should be able to review it.

Mrs. WATSON COLEMAN. So does that empowerment require our legislative—my last—I'm sorry—does that require our legislative action to reconfigure this and empower in a different way?

Mr. BLANTON. Yes, ma'am.

Mr. LEONARD. Absolutely.

Mrs. WATSON COLEMAN. Thank you.

Thank you, Mr. Chairman.

Mr. HICE. I thank the gentlelady.

The chair now recognizes Mr. DeSantis for 5 minutes.

Mr. DESANTIS. Thank you, Mr. Chairman.

I appreciate the testimony and the invitation for Congress to be involved in this. But I want to just start at the beginning and just ask everybody, does everyone agree that at some level the executive does have inherent authority under Article II as part of the executive power to maintain secrecy of information related to the national security?

Mr. Leonard.

Mr. LEONARD. Absolutely.

Mr. AFTERGOOD. Yes.

Mr. BLANTON. Yes, but. Because there's an Article I that says Congress makes the rules to govern the military, Armed Forces, and national security. So it's both.

Mr. DESANTIS. Well, it's both, but I think Hamilton when he talked—because there was a debate whether you should even have a single executive. They had revolted against George III. Some proposed a council. And one of Hamilton's main arguments for why you needed a single executive was for secrecy, particularly with regards to national security.

So there's got to be—I mean, is there anyplace, I guess, that Congress can't go into that? Or could Congress basically legislate as far as it wants, in your judgment?

Mr. BLANTON. It can legislate as far as it wants. Congress has the power of the purse. That is the key. And I think the Founders said separate the power of the purse from the power of the sword. That's key. Takes money to run a——

Mr. DESANTIS. Well, I think that's—I think—absolutely. So the Congress could abolish the CIA if they wanted to. There's no requirement you have that. But we do have intelligence agencies. We do that. Could Congress just pass a statue saying declassify as much sensitive stuff as we want? Would there be any constitutional concern with doing that?

Mr. BLANTON. None. And Congress has already done so with the Nazi war crimes, which exposed the files of Nazis that the CIA recruited and brought to the United States. So Congress has already done that.

Mr. DESANTIS. But when did they do that, though?

Mr. BLANTON. In 1998 and 1999.

Mr. DESANTIS. Yeah, well, but I guess my point is, if Congress wanted to start declassifying things that were germane and ripe right now with how our government's conducting sensitive operations, you say that would still be okay even though it could jeopardize lives?

Mr. BLANTON. It would still be okay because my bet is that this Congress and this committee would act pretty judiciously on that. You're not going to willy-nilly, you're not Julian Assange.

Mr. DESANTIS. No, I get it. But what I'm trying to figure out is if there's a——

Mr. BLANTON. I have a lot of confidence in your judgment.

Mr. DESANTIS. Well, but there's certain constitutional prerogatives. We obviously have the power to legislate, of course the purse. The executive has certain—or, I mean, the executive power means something. I mean, there's certain things.

And so what I'm trying to figure out is are there certain places—because I think we all agree some of this stuff is ridiculous. And there's an incentive to just simply take on more—some of this stuff isn't even classified that's being protected.

But at the same time I just think it's important to recognize that there is a legitimate reason to do it, because I think when you overclassify, I think that actually undermines the core reason of why you want to do it.

But let me just get you, Mr. Amey, down on the end.

Mr. AMEY. I totally agree. I do believe that there's a constitutional protection for secrecy. But at the same time, as Tom said in his statement, I think you have to get to his point number three, and that is don't trust it. I mean, eventually we're going to have to get down to a point where, whether it's through the challenge process or through briefings that Congress gets, on questioning what the executive branch is doing.

Mr. DESANTIS. So you look at some of these things, some of these agencies, the Antitrust Division at the Department of Justice, the Bureau of Prisons has somebody who's an original classification authority.

Mr. Leonard, how did it get to be that point? Is that really necessary in those instances?

Mr. LEONARD. It's an example, perhaps, of—when I was in my position at ISOO one of the things I had to do was to deal with requests for agencies to get original classification authority. And, quite frankly, one of the issues that I had to contend with is it was one of convenience more than anything else.

And there were a number of instances where there were agencies or even small activities looking for original classification authority that had to push back because they were looking to really accomplish something that probably could have and should have been accomplished through legislation if there was really a legitimate reason to withhold information from public disclosure.

Mr. DESANTIS. How do you analyze? Because some of this stuff, it's just the agencies are embarrassed, they don't want to do it, and it's clearly just—it's not credible. But sometimes when you're trying to get information from FOIA or Congress, I mean, you are diverting the executive from kind of their core mission, actually do good. I mean, we're the first ones to criticize the government when they screw up or when they're not competent.

And so how do you do this in a way that's not going to impose too many costs? I mean, for example, if we're going to always review every 10 years some of this stuff, that is going to create some costs. So how would you recommend we strike that balance? Is that a valid concern?

Mr. LEONARD. It very much so is. And one way would be to, as Mr. Blanton referred to, was to consolidate authority and responsibility and not spread it so far and wide within the government.

I'll give you a perfect example. When I was in the Department of Defense, I could write a memo and use CIA information. The CIA trusted me to properly classify the information. They didn't want to look at it and whatever.

If I came back 20 years later and wanted to work at the National Declassification Center and looked at my same memo, they wouldn't allow me to declassify it because I didn't get a paycheck from CIA.

That type of redundancy can be beaten out of the system and it would result in significant cost savings.

Mr. DESANTIS. Great. I yield back.

Mr. HICE. I thank the gentleman.

The chair now recognizes Ms. Kelly for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair. And thank you for holding today's hearing on this important topic.

I believe that secrecy is a serious problem that is widespread in the Federal Government and that it goes beyond classified information. For instance, there's a category of pseudoclassification that has exploded over the last 15 years called controlled unclassified information. I understand there may be as many as 100 different designations in use, but the label "sensitive but unclassified" is one of the worst of offenders.

First, I want to get a sense of the extent of this problem. The Information Security Oversight Office annually reports how many classification decisions agencies make. However, there is not a cor-

responding section on how many decisions were made to designate materials as controlled unclassified information.

Mr. Leonard, you previously served as the director of ISOO. Are agencies required to track how many materials they designate as controlled unclassified information?

Mr. LEONARD. Quite frankly, I'll defer to one of my copanelists because I've been away from ISOO since they assumed that responsibility and have not followed it that closely.

Mr. AFTERGOOD. I would say that there has been significant progress compared to where we were 10 years ago. It used to be that anybody could mark any document anything. You could say this is for official use only and that would restrict its access.

Now, under the executive order on controlled unclassified information, there is what's called a CUI registry, and only those markings that have been approved and validated can be used. And there are many things, of course, we want to protect. We want to protect tax returns. We want to protect privacy information. All those kinds of things have been validated, and only those markings that are on the CUI registry are supposed to be used.

Now, is that system working perfectly? Are people bending the rules? I don't know the answer to that question. It just went into force very recently, and we're still waiting to see how it's working. But I think the policy has improved substantially over the past decade.

Ms. KELLY. Would you estimate that more information is designated as CUI than is classified?

Mr. AFTERGOOD. I don't know the answer to that.

Mr. AMEY. I don't think we know the answer to it. Agencies are going to be required to report how much information is marked. They did boil the over 100 categories down to 20. However, there are 80 subcategories. And so at that point you still end up with a real patchwork of designations and markings that can be placed on documentation.

The big thing with it also is there's going to be better training. ISOO is doing a very good job, and I have to applaud them, because they actually reached out to our community and worked with us on the rules. As it went through the process, they really did work with the agencies to try to get it. But they didn't—I don't think they realized how big that this had expanded within agencies. And there was a lot of foot dragging by Federal agencies as well.

So as Mr. Aftergood said, it was only in effect, I think, as of mid-November, something like that. And so at that point we're going to have to wait and see. And full implementation of the CUI regulation isn't expected to be completed until 2017, '18, '19. So at that point it's going to take a very long time to probably get some answers on it. But it needs the proper oversight from this committee.

Ms. KELLY. I know you called it a gray area, because I was going to ask you what do you think the potential for abuse is.

Mr. AMEY. We've already seen some abuses. In my written testimony I provide two examples, and one was even an IG report in which there were examples involving the TSA. Also, the bizarre case of Robert MacLean in which something was marked SBU. It was actually the original CUI. And so at that point something was

marked SBU I think 4 years after he released it, even though it didn't have any marking or designation, but they retroactively marked that information as SBU. So there are problems in the system and it is prone to abuse and so we do have to watch it.

Now, the nice thing with the CUI rule is that there is a misuse provision, and so that may be something that can be borrowed upon for the classification system that we should look at since it's already in regulation. And also the challenge procedure. But, again, challenges go back to the agency, and then I think you have a right to dispute resolution. So it's a little murky due to the fact that you're, in essence, going back to the fox guarding the henhouse that may have originally marked it. So there are some concerns with that.

Ms. KELLY. Mr. Blanton, you keep shaking your head. So I want to give you opportunity for comment.

Mr. BLANTON. I agree.

Ms. KELLY. Okay. I yield back the balance of my time.

Mr. HICE. I thank the gentlelady.

The chair is now going to recognize himself for 5 minutes.

I want to go back to something that came up a little while ago, and that is the number of classifications. Over the last 5 years some 400 million, and yet only a little over 2,300 in the same 5-year period have been challenged. And those numbers can be debated a little bit here and there. But whatever it is, 2,300 out of 400 million is virtually no challenges whatsoever.

Just real quickly, just a sentence or two, why so few challenges? Mr. Leonard, I'll start with you.

Mr. LEONARD. Mostly one of culture. When I was in the Pentagon, when I had reports in my inbox, if I had an unclassified report and a top secret report, which one would I read first? The top secret one, even though the unclassified one may be more substantive. So sometimes it's just as simple as just sheer culture, People get inured to it and just expect nothing else.

Mr. HICE. Mr. Aftergood.

Mr. AFTERGOOD. In many cases, employees are not aware of the challenge provision that enables them to make this challenge. And that's one simple step that can be taken to say, look, as soon as you sign your nondisclosure agreement, you also sign, "I'm aware that I can challenge a classification marking that I believe is improper."

I would also mention that I think your hundreds of millions figure is including original and derivative classifications. The number of original classifications or entirely new secrets has been on a steady downward trajectory.

Mr. HICE. I don't want to get into a number right now.

Mr. Blanton, why so few challenges?

Mr. BLANTON. It's easier just to classify. And much classification just occurs reflexively. And most of those derivative classifications it's just keep it going. Because there's not a thought process on the front end of the first decision. What's the cost benefit? What's the real risk? What's the vulnerability? What's that? And you've got to educate them at the nondisclosure agreement point, but I would argue you've got to put it in a statute.

Mr. HICE. All right.

Mr. Amey.

Mr. AMEY. And just quickly, it could be career suicide. I mean, at this point we have insider threat investigations that could take place, and also whistleblower retaliation. So a lot of the times, as Mr. Blanton just said, it's a lot easier just to go along with the process than to question it.

Mr. HICE. Okay. So it's not a matter of red tape. Perhaps poor advertisement, people don't know, perhaps a culture, or whatever. But red tape is not the problem, is that correct, all of you would agree with that?

Mr. LEONARD. Oh, absolutely. And, again, a lack of accountability is key too.

Mr. HICE. Okay.

Now, when it comes to—obviously we know there's been a lot of threats to our country, and I'm concerned about the lack of information sharing within our Federal Government.

A scale of 1 to 10, how serious of a problem is this, to each of you?

Mr. AFTERGOOD. I think it was 10 around the time of 9/11. It's 5 now. In other words, there has been significant progress.

Mr. HICE. Okay. The rest of you?

Mr. Leonard.

Mr. LEONARD. I would tend to agree, but my sense is that there's also been a rollback with respect to some of the recent rather significant wholesale compromises that have occurred as well too.

Mr. HICE. All right. Mr. Aftergood, how serious of a problem?

Mr. AFTERGOOD. It's a serious challenge. When you classify, you restrict dissemination. And so they're the flip side of each other. It's an ongoing problem.

Mr. HICE. Mr. Amey.

Mr. AMEY. Agreed.

Mr. HICE. All right. So across the board we still have a serious problem. There may be some improvements. But we still have a serious problem with sharing information, even when potential threats are hanging in the balance of our country. And in the mix of all of that, also came up earlier is the ability of Congress to do our job.

How serious is the issue or is it at all an issue where agencies are overclassifying to either complicate or obstruct congressional oversight? I'd like to hear from each of you quickly.

Mr. AFTERGOOD. Honestly, you're probably in a better position to answer that. I think it's the exception, not the rule.

Mr. BLANTON. I think it varies by agency. And I think the intelligence community has the, in a sense, the worst cultural problem. You've got to go into that SCIF. You can't bring out notes. You can't have staff. How are you going to have a serious consideration of real oversight over some of the most important and sensitive and deadly operations of our entire government?

Mr. HICE. All right. Real quickly.

Mr. LEONARD. It inevitably occurs, whether intention or not. And, again, the lack of accountability makes it ripe for abuse.

Mr. AMEY. And it's why in any oversight or any new commission that is going to be paneled here to take a look at classification and the status and secrecy issues, is why you have to get out of just

the check-the-box kind of audit on are people following procedures, but take a look at some specifics where challenges have been raised and why those things were allowed to be overclassified.

Mr. HICE. And when we do get stuff, it's so redacted it's virtually worthless much of the time. So a serious problem.

I again want to thank the panelists. My time has expired.

The chair will now recognize Mrs. Maloney for 5 minutes.

Mrs. MALONEY. Thank you, Mr. Chairman and Ranking Member.

Mr. Blanton, earlier you mentioned the Nazi War Crimes Disclosure Act. That happened to have been a bill that I authored. It took about 4 years to pass it because the CIA was objecting. It opened up the files of Nazi Germany and Japan 50 years after the war.

Now, every other country had opened their files, but we were refusing to, and it took Congress to pass a bill to open up these files. It's been turned into books. It's been turned into all kinds of helpful information that's helped our defense strategies and how to operate in an environment as they did.

But I want to ask you about another way of classifying, which is retroactively classifying. And I join you in saying there was no reason why we shouldn't have declassified that information. But on September 8 of this year, State Department Under Secretary for Management Patrick Kennedy, testified before this committee about a unique process in the State Department used to retroactively classify 2,000 of Secretary Clinton's emails that she turned over to the State Department.

In other words, they were not classified at the time they were sent or received by her, but then they were reclassified after the fact by staff in the Department of the FOIA office. And Patrick Kennedy testified that 1,400 of these documents, or 70 percent, were retroactively classified because they contained what is known as foreign government information.

So my question is, it seems to me that this is a confusing process. Foreign government information is not treated like classified information until it's reviewed for public release, and then all of a sudden it's classified. It seems to me we should have one standard. Why have one retroactively? It makes no sense. And how are State Department employees supposed to know when to treat information as classified and when not to if the designation might change without warning?

Mr. BLANTON. I read Mr. Kennedy's testimony with great interest because he asked this committee to create an exemption under the Freedom of Information Act for foreign government information, which I think is a terrible idea, for three reasons. One, it puts Tajikistan standards into our freedom of information law. No, thank you. The lowest secrecy abroad.

I think second reason is if there's harm from release of that foreign government information, it's protected already under our executive order. You can classify it.

And I think the third reason is that's the easy way out. Instead of our diplomats actually thinking about how you protect stuff that actually would get us into trouble, they don't want to think about it.

And I'd just remind you of the Weatherhead case went all the way to the Supreme Court over foreign government information.

Finally it got booted out. It turned out the document at issue had already been handed over to the plaintiff and the government had no idea. And it wasn't going to damage our relationship with Great Britain, which is where the document came from. So skepticism is in order.

Mrs. MALONEY. Well, I agree with you, and I truly understand the need to protect truly sensitive diplomatic discussions from public release. But using the classification label to do that makes the classification system even more confusing and, I would argue, less effective. And we need to find a better solution.

So with that statement, I'd just like to ask all of the panelists in my remaining time, do you have any recommendations of how to improve this process? And we could start with you, Mr. Leonard, and just go right down the line.

Mr. LEONARD. The consistent theme this morning, and I agree with it wholeheartedly, is providing legislative backing to the very system in order to ensure uniformity, consistency, and most of all accountability. And also to facilitate the Congress to be able to fulfill their Article I constitutional authorities as well.

Mr. AFTERGOOD. The government requires a degree of flexibility, and so I would be cautious about strict provisions that remove such flexibility. Information that is provided in confidence needs to be protected somehow if one wants to maintain that working relationship. Classification seems like a heavy-handed way to do it, but if the alternative is a blanket FOIA exemption, then that might not be better. So I don't have a good solution for you offhand.

Mr. AMEY. When it comes to retroactive classification, I think we need a study. I'm not aware of anything in depth or comprehensive in taking a look at the issue on the whos, whys, wheres, whens. And so I think that would be in order.

Mr. BLANTON. The fundamental phenomenon on retroactive is being driven by agencies like what Mr. Leonard said, CIA asserting control and no longer allowing the Defense Department or State to declassify their own information.

Mrs. MALONEY. Okay. Thank you very much.

Mr. HICE. I thank the gentlelady.

The chair now recognizes Mr. Massie for 5 minutes.

Mr. MASSIE. Thank you, Mr. Chairman. I'm so glad we're having this hearing today. I've been looking for the opportunity to talk about something that's very important to me, and I'll be very careful not to disclose anything that's classified.

About a month ago I went back down to one of those SCIFs that Mr. Blanton was talking about. You can't take notes out. And what I did is a reread the 28 pages, but I brought the redacted version with me so that I could see in what manner it was redacted. By the way, I want to ask you guys a question later so you can get ready with an answer.

But one of things that I would think would help is to know the reason for the redaction. There's certain reasons that might be legitimate, and maybe a law that says when you redact large swaths or even small portions, that you have to give the reason. If the reason is to avoid embarrassment or to protect a source or to protect somebody who may not be guilty, their public reputation, just dis-

close it, and then the crime or the infraction could be that you lied about the reason.

Because that's what I want to get to with these 28 pages and the reason for those redactions. And I think I can disclose my perceived reason for some of these redactions without disclosing anything classified.

Twenty percent of the redactions, I would say, were to protect specific and confidential sources. I would say another 20 percent were to withhold the names of individuals whose reputations would be irrevocably ruined, whether they were guilty or not.

But 60 percent of those redactions fall into a very troubling category for me. They changed the very nature of the document and the way it's perceived by the public and the impact that it should have had.

Some of those are probably to prevent embarrassment.

Mr. MASSIE. But I feel like—after reading that—10, 20, 40 years from now, when it's all released, this is going to be a textbook case of how the government overclassified something in an effort to control the narrative. In fact, before these pages came out, there was an op-ed in the USA Today by two of the chairmen on the commission that said these are raw, unvetted sources. Right? So the redactions, in my opinion, were made to support that presumption that these were raw, unvetted sources, because if you removed the redactions, you would say: No. Those might be credible sources, in fact. And they might, in fact, be vetted.

So that's my concern is that, you know, 20 years from now, we'll look back at this, and you'll see that key words and acronyms and sentences were removed and with the effect—with the effect—of diminishing the impression that you get from reading the unredacted pages, which is that Saudi Arabia—and I can say that name now because it's in the redacted pages—has some kind of civil liability or criminal culpability either—and not because of their citizens but because of their government acted either in, I would say, acts of omission or commission. Either one makes them somewhat culpable. And I'm afraid that has been diminished by those redactions and it's been overclassified, and this is a prime example.

So one of the questions I want to ask is, do you think it's a good idea if we required them to give the reason for the redaction?

Mr. LEONARD. Absolutely, sir. The order does require original classifiers to be able to identify and describe the damage to national security. But to my formal statement I attached an actual email that had been used as count one for a felony indictment of Mr. Drake, who was eventually not prosecuted. But the government claimed it was classified. And in preparing for the trial, the NSA was required to say—state specifically why they considered that email to be classified. Their explanation looked entirely rational when you read it, but if you compared what they said to the actual document, it was factually incorrect.

Mr. MASSIE. Right. So that supports the notion that they should be required to disclose it, and there should be some punitive ramification for misleading about the reason.

Mr. Aftergood?

Mr. AFTERGOOD. I would like it to—to make the point that the classification system is permissive. It says that information may be

classified if it meets certain conditions. And what that means is the decision to classify is actually a subjective one. Somebody thinks that classification is the right move. And because it's subjective, you or I may disagree and say: You know, that's a mistake. You're wrong.

And so providing the reason, I think, would be helpful. But it wouldn't necessarily resolve the disagreement. I just disagree with that reason. Instead, I would suggest that, in cases of significant interest, like the 28 pages, like many other cases, there needs to be a procedure where you take the decision away from the original classifier. Don't try to make the original classifier admit he was wrong. Take the decision away. Take it to a third party. There's a public interest declassification board. There may need to be a new body and say: Does this make sense? I want you to evaluate it as a third party and come back to us with a recommendation.

Mr. MASSIE. Mr. Chairman, I appeal to let the other two answer the question.

Mr. HICE. You can answer.

Mr. BLANTON. Just very briefly, exactly this mechanism exists for mandatory review requests, this interagency security classification appeals panel. And it's ruled in favor of openness over 70 percent of the time. Just a third party. The simple maneuver of taking the document away from the original agency and putting it in a panel that includes the original agency, you get a completely different result.

Mr. MASSIE. Mr. Amey.

Mr. AMEY. And this is also a process with the Freedom of Information Act. There is a process there where just only a few years ago did they add where they had to list the reasons. In the old days, we used to just get a letter back with tons of blackened-out markings. And then, in the intro, they would say: We redacted things for, you know, B3, 4, 5, 6, 7. And you had to kind of guess what applied to one specific redaction. Now they're required to go through documents subject to the Freedom of Information Act and list right next to each redaction what the redaction—what exemption was being cited to justify the reason for that. And also then you also have an administrative appeal that we hope—we always hope—that it goes to a different entity inside of the department rather than the person that made that marking. And then now there's also a process through ISOO to challenge those determinations and go to an, in essence, an arbitration. And so it's funny that we have a better procedure just for that Freedom of Information Act process than we do for the classification process.

Mr. MASSIE. And I've seen those documents with those markings. And they're somewhat helpful because they classify the stuff they even send to us, they try to not even disclose. So but I haven't seen that on the 28 pages. I've just seen op-eds that say: Oh, there's nothing to see here.

And by the way, it was released the day before Trump named his Vice President, which is another thing. But at least it was released in part.

Thank you.

Mr. HICE. Thank the gentleman.

The chair now recognizes Mr. Connolly for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman.

And thank you all for participating. I guess I'd like to explore a little bit what happens when two agencies disagree about something being classified at all. And this is not a hypothetical? In a recent investigation of emails, we had multiple examples where the State Department said one thing and the intelligence community said another. Specific example, really quite, I think, quite striking: A 2011 email sent by a State Department employee about the late Ambassador Chris Stevens of Libya was marked clearly "sensitive but unclassified." The Under Secretary for Management, Mr. Patrick Kennedy, confirmed in testimony before the committee that the State Department considered the email unclassified and that anyone reading the email would assume it was not classified. But after the email was sent, the intelligence community nonetheless claimed it was classified.

And so, in September of last year, the State Department sent a letter to Senator Corker, the chairman of the Senate Foreign Relations Committee, explaining that the intelligence community was wrong. The letter from the State Department stated that the suggestion that the email should have been treated as classified was, and I quote, "Surprising, and in the Department's view, incorrect," unquote. So what's a poor boy to do? Is it classified, or isn't it?

Mr. LEONARD. As has been mentioned, sir, there are appeals processes in the system, but they're admittedly rather cumbersome and time-consuming. But Tom Blanton referred to the Interagency Security Classification Appeals Panel. I used to serve as the executive director of that. Interestingly enough, last year for the year that the full last numbers are available, for appeals that came to that panel, which consists of executive branch representatives from various agencies, 95 percent of the time the determination made by the agency that owned the information was overridden at least in part or in whole—95 percent of the time, since 1995——

Mr. CONNOLLY. Yes, but in this case, Mr. Leonard, the originating agency didn't want it to be classified.

Mr. AFTERGOOD. I think the short answer to your question is that each agency has classification authority over its own information. And in the dispute you're referring to, I think the intelligence community considered that the information at issue was its information, even though it was in the State Department document——

Mr. CONNOLLY. And the State Department——

Mr. AFTERGOOD. The State Department said: No, it isn't.

Mr. CONNOLLY. That's right. The State Department took direct issue with that saying: We understand that's what you think, but that's not how we got the information.

Mr. AFTERGOOD. Yeah.

Mr. CONNOLLY. And then we could even add another layer. So let's hypothetically say we invite the FBI, a nonpolitical organization, to come and look to see if there were violations of our secrecy laws. Well, how is it supposed to determine whether a violation occurred when the two major agencies or entities looking at classification have unalterably different views about the nature of the document, the sourcing of document, and what it should be classified as?

Mr. BLANTON. Part of the problem for the Federal Bureau of Investigation is it's part of the intelligence community, so it leans one way on that question. And the real answer to your question, is it classified or is it unclassified, the answer is both. And that's the reality of our classification system. I showed you documents here that are both classified and unclassified simultaneously because different people or different agencies or sometimes the same reviewer came to a different conclusion.

Mr. CONNOLLY. I know. But there's a certain, Mr. Blanton, Kafkaesque quality to this. I mean, I was a staffer on the Senate Foreign Relations Committee a long time ago. Right? And we were very careful about classified material and how it was stored and make sure it was never on your desk, and as are executive branch employees. Well, if I got one agency saying that's—you know, "Give it to your grandmother; I mean, it's unclassified," and the other one saying, "Don't you dare; it's classified," what's my liability as an employee? I'm trying to be diligent. What is it? And am I exposing myself by leaving it on my desk, for example?

Mr. AFTERGOOD. The executive order on classification includes provisions for resolving disputes about implementation of the order. Ultimately, those disputes can be directed to the Attorney General and, you know——

Mr. CONNOLLY. Yeah, but, Mr. Aftergood, that's not how it works practically.

Mr. AFTERGOOD. It's not. No.

Mr. CONNOLLY. Somebody goes around—listen, I was in the private sector and I was the OODEP. I was the head of all of this for a private sector entity. We went around checking to make sure nobody was sloppy. And that's not going to go to the Attorney General. You've got a ding on your mark, Mr. Blanton, because I saw that document on your desk. Well, in good faith, you were counting on the State Department judgment it was not classified. There was no issue. And I'm deciding as, you know, the security chief that I don't care; the intelligence community is what I listen to, and they said it is. I mean, it puts people at risk. And, frankly, I'm glad it could be arbitrated at some point, and I'm certainly glad the Attorney General can ultimately adjudicate. But if we're talking about, you know, thousands of documents, thousands of judgment calls, I think you mentioned it was subjective, but disputes between agencies are a real dilemma for people trying in good faith to comply with the law.

Mr. AFTERGOOD. You are absolutely correct. And the arbitration is really a technicality. The reality is that these kinds of disputes drive the issue to the lowest common denominator. They result—when there's doubt, they end up adopting the view that it's classified.

Mr. CONNOLLY. Thank you.

Mr. BLANTON. And the executive order says, when there's doubt, it should not be classified. And exactly the opposite happens. So my answer to your question: Send it to your grandmother. Send it to your grandmother.

I have an opinion from Mr. Leonard when he was the head of the Information Security Oversight Office, he said: If the National Security Archive got a version of this document under legal authority,

declassified with somebody with the power to do that, you can take it to the bank. You can keep it on your Web site. Even if somebody else at the Energy Department or Defense says, "Sorry, Mr. Blanton, that's classified," no, wrong. Send it to your grandmother.

Mr. HICE. Thank the gentleman.

Now recognize Mr. Grothman for 5 minutes.

Mr. GROTHMAN. Sure. First question I have, and this is really for anybody that wants to answer it. In the stuff that we have here, we're told the government spends $16 billion on classification activities and $100 billion over 10 years, which is a stunning amount of money. And if it's $100 billion over 10 years, it must be going up like a rocket. And I assume that means like $5 million 10 years ago and $16 million today. Does anyone care to comment on, is that a good investment of funds? And how do you wind up spending that amount of money? I mean, it just seems like a phenomenal amount of money. Do you think it's accurate?

Mr. LEONARD. That's a difficult thing to evaluate. Let's put it this way. I spent many a year in the Defense Department. And I had to deal with the consequences of major failures, major compromises in espionage cases and things along those lines. And what the challenge is, is that, whether rightfully or not, the mentality is, is zero tolerance for those types of things. How many espionage cases are you willing to endure? How many major leaks or releases of—unauthorized releases are you ready to endure? The mindset is zero tolerance. And as a result, there tends to be a lack of risk management. And when you have a lack of risk management, you end up paying premium dollars then.

Mr. GROTHMAN. Even though those numbers are accurate though: $16 billion bucks——

Mr. LEONARD. Those numbers are at least accurate from the point of view that they show, I think, consistent trends from year to year.

Mr. GROTHMAN. Okay. We have a new ISOO director, Mark Bradley. Does anyone want to give us their opinion? Do you think that's a good pick? And what goes into making a good pick?

Mr. AFTERGOOD. You know, it was never going to be an openness advocate who led the ISOO. But I think Mr. Bradley is a good pick because he has a broad understanding of the problems of secrecy. He was an aide to the late Senator Moynihan and is well attuned to an understanding of the problems that the secrecy system suffers from. He also, as a former intelligence officer and a DOJ national security lawyer, has a degree of credibility with the national security agencies that others might have trouble matching.

Mr. GROTHMAN. Okay. Go ahead.

Mr. BLANTON. Just the proof's in the pudding. We look forward to meeting with Mr. Bradley as soon as he's on the job. You can look at the Information Security Oversight Office's previous Directors like Steve Garfinkel and Bill Leonard and Jay Bosanko, and you can see those folks made some real differences in the security system in a more rational direction. I can hope for that trend to continue.

Mr. AMEY. Certainly, we hope that they reach back out to our community. I mean, that's one of the nice things with all the gentlemen that Mr. Blanton just mentioned is they have been very

open. There's been a dialogue back and forth, and they know that there is a burden on secrecy but then on openness and have, you know, provided the proper weight test to that. And that has been, I think, beneficial to the system.

Mr. GROTHMAN. Okay. There was an inspector general report in 2013 that said that 33 percent of DIA employees didn't understand their role. And even more outrageous in that report, they said 80 percent of the documents reviewed were misclassified. I guess, first of all, I should ask you how many different classifications there are, because it seems like you could almost throw darts at a dart board and do better than that. But could you comment on that and as to why that happens? Comment on it. Do you think things are better today than it was 3 years ago? That seems—or maybe it was a flawed report. Can you—are you familiar with the report?

Mr. LEONARD. I would suspect it's not a flawed report. I think, based on my experience for over 40 years, that's rather typical. It's a reflection of, as much as we spend tax dollars to investigate people, to establish secure IT systems and things along those lines, we do not spend a comparable amount of money in terms of trying to train people in the basics. One of my concerns is, is that, you know, we make a distinction between original classification and derivative classifications. My experience has been is that when people ostensibly are derivating classifying information, they're actually just classifying information based on gut instinct, more than anything else.

Mr. GROTHMAN. Any other comments? By the way, unless I'm doing the arithmetic wrong—and I did it twice—on the cost of this thing, for that, you could hire 200,000 people at 80 grand compensation a year. That's how much we're spending on classification—200,000 people. Now, I realize some of it's for things, not people, and maybe some people are making more than 80 grand a year, but my goodness. My time is——

Mr. HICE. Thank the gentleman.

The chair recognizes Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

First of all, I want to thank the panel for helping us think about this and how we might approach the problem. I had the pleasure of working with Mr. Massie and also Walter Jones on the 28 pages. It took us 15 years to get that information out there, which is far too long. It was interesting because, as we were asking for disclosure and declassification, the administration was pushing back and saying: No. This is too sensitive. We had some of the agencies saying: No. It's methods and sources. And then, finally, when it was eventually declassified, they flipped. They flipped and said: Well, there's nothing here. And it's—the information is not valid. And they took a totally different tack.

We're now struggling with the DEA and the FBI in regard to classified—excuse me, confidential informants. So we've learned from the Office of the Inspector General for the DEA that we've got 18,000—they've got 18,000 confidential informants out there that are under contract being paid by the DEA, and last year, we spent $237 million paying confidential informants. And Congress knows zero about that. They don't know about the crimes they've been committing. They don't know the way they're operating. The DEA

headquarters isn't intimately involved. This is all being operated at the field level. So that's—and that's just the DEA. From our conversations with the FBI, I believe that the numbers are double, probably about $500 million that the FBI is paying the confidential informants. Probably double the number. Probably in the area of 30,000 or 40,000 informants, confidential informants. That is totally out of our purview.

So I'm wondering—you know, you've all hit on this, you know, with the interagency panel reviewing classifications—is there some way to supercharge that process? Because it is painstakingly slow, and it doesn't work in the timeframe in which the information would be useful to us.

Mr. Leonard, I know that you said that the last time somebody took a good swing at this was during the Clinton administration in your remarks, your earlier comment. Is there some way we can get this interagency declassification review panel resourced and equipped to give Congress, and I've seen—I've seen my colleagues across the aisle tear their hair out when they couldn't get information, and I've been in the same position. Is there some way that we can formalize this process to get the information in a timely manner that should be public?

Mr. LEONARD. One way I would suggest would be to make provisions to allow appeals directly to that panel under certain circumstances. Right now, requesters have to go to the individual agency. If they get turned down in whole or part, they have to appeal to that same agency. And it's only after that process then that they can go to this interagency panel. And even that interagency panel, then, has its own coordination things which can be problematic, but which is a lot easier to address. But the individual agency time delays is—can be problematic. Also, for purpose of Congress, Congress does have the public interest declassification board that they can refer to. And that is another avenue that, quite frankly, I never believed is utilized enough. But that's another avenue.

Mr. LYNCH. Yeah. To expedite it, you know, maybe we've just got to figure this out legislatively to introduce an expedited process where the information we believe is so critical. And I guess, you know, I'm just thinking, is there a way to get the judiciary involved here so they would review—I don't want to create a political question that the courts can't rule on, but we're being stonewalled in wide areas of public interest. And I feel like it's hampering Congress' ability to do its job.

Mr. LEONARD. Well, one of the things is the interagency panel is actually exercising on behalf of the President. It's exercising his article II authority. And the Public Interest Declassification Board. Ultimately, they just make recommendations to the President, who makes the final decision. So from that point of view.

Mr. LYNCH. Mr. Amey, you got something you want to add? Or Mr. Blanton?

Mr. BLANTON. Yes, sir. You mentioned sources and methods is a blame. And then I think this goes right to you informants problem, and it goes right to one of the big drivers of classification, which is, under the current statutory system, anything that's a source or a method can be claimed to be withheld, whether or not it's release would actually harm a security value or get a source killed. And

I think Congress can take very simple action, both in the intelligence field and the law enforcement field, to say sources and methods is not a burka. It should over-cover the things that would do damage, get somebody killed, ruin an investigation. Right now that identifiable harm standard, which is now in the Freedom of Information statute, it doesn't apply in this informants and sources method. It needs to apply. Congress has to take that action.

Mr. LYNCH. Yeah. Mr. Amey.

Mr. AMEY. And that recommendation was actually in the Moynihan Commission report. And it hasn't been acted on now in almost 20 years since. And so it may be time for Congress to enter that world.

Mr. LYNCH. Yeah. I know that Attorney General Reno issued some guidelines, but they're not being followed right now. I actually have legislation. I don't even want to know who the confidential informants are. I just want to know how many are out there, what they're being paid, and what crimes, if any, they have committed while they've been part of this government program. And we have had a difficult time getting that through. But thank you.

That's all I have, Mr. Chairman. Thank you for your indulgence. I yield back the balance of my time.

Mr. HICE. Thank the gentleman.

The chair now recognizes Mr. Duncan for 5 minutes.

Mr. DUNCAN. Thank you very much, Mr. Chairman, and, first of all, I want to say that—I want to go on record as saying I agree with Mr. Grothman in saying that I'm astounded by the amount of spending that's being done on this, this $16 billion estimate and over $100 billion over the last 10 years. I think we lose sight up here of how much a billion dollars actually is.

But having said that, I had two other meetings, and so I didn't—unfortunately, I didn't get to hear your testimony. And I apologize if you've gone into some of this earlier. But, Mr. Blanton, in skimming over some of this testimony, I was fascinated by your report about the Moynihan Commission and that we went through all this 20 years ago, basically. And also I think the thing that impressed me the most was, I mean, there seems to be general agreement here today that there is a real problem of overclassification. But I saw where Mr. McDaniel—who was President Reagan's national security adviser said that only 10 percent of what's being classified probably really needed to be classified. Is that correct? And why do you think—you mention there that this was a tremendously bipartisan commission. It had Jesse Helms and Daniel Patrick Moynihan and various others. And obviously you're disappointed that not—or very little was done with that—those recommendations. Why do you think that was? And do you think we should take another look at that? What do you—just go into that a little bit for me.

Mr. BLANTON. Yeah. I think in the testimony I quoted Mr. McDaniel, who the Moynihan Commission quoted, and said that based on my experience with few million pages of declassified documents, he's right, especially about the historical materials. I think an estimate that's closer to reality for current material, the material related, say, on terrorists and ISIS, that the best estimate really came from the Republican head of the 9/11 Commission, Tom

Kean. He said 75 percent of what I read about Al Qaeda and Osama bin Laden that was classified shouldn't have been, and we'd have been safer as a country. So I think the ranges in there, the 75 to 90, it's a bureaucratic problem. Bill Leonard knows it better than anybody from both the inside and the outside. Steve Aftergood's been studying it for, lo, these many years. POGO. Every incentive is to classify. There's almost no disincentive. There are no penalties. There has to be—I think this is the main reason why Congress needs to take action. Because you all can change the minds of the bureaucracy and how it actually works. You can, you know, change the law and their hearts and minds will follow.

Mr. LEONARD. I actually believe that the executive branch and general agencies in particular actually want the ambiguity because the ambiguity gives them almost unlimited discretion in dealing with issues. And, yes, it results in dumb things. But it's the ultimate trump card to pull out, whether you're dealing with the courts, whether you're dealing congressional oversight or whatever. Nobody wants to be the one who compromises truly sensitive information. And so there tends to be this overdifferentiation to any sort of assertion. And more often than not, that's what it is; it's a simple assertion. It cannot be demonstrated that it truly should be classified.

Mr. DUNCAN.Well, there's so many other things I would like to add or comment on, but Mr. Amey, I'm assuming that you—you know, this committee has requested through the years a great deal of classified material. And do you think that agencies are classifying some material or a lot of material that really doesn't need to be classified just to avoid or get around congressional—effective congressional oversight?

Mr. AMEY. Yes. But it's hard to know at what level. You know, I don't know what I don't know. And that's—unfortunately, when something shows up and it's a blackened out page and it's marked "classified" or, you know, and then some FOIA exemption attached to it, at that point, it's hard to know. Sometimes we do get documents released to us. And at that point, then you can do the comparison. And so, you know, that can add and that can allow you to ask some questions. But, you know, unfortunately, with the amount of classification that we have, it's very difficult to put your finger on a—you know, the experts that have taken a look at it, the 75 to 90 percent. But the culture, I mean, I think that's it, is, even after 9/11 with the 9/11 Commission, you have a culture to—the default setting is err on the side of caution.

Mr. DUNCAN. Well, I've run out of time. But I will say this. We're going to have to, it seems to me, to go to much more of a carrot-and-stick approach on all of this and incentivize good behavior and penalize bad behavior in this area.

And at any rate, Mr. Chairman, thank you very much.

Mr. HICE. Thank the gentleman.

The chair now recognizes Ms. Lujan Grisham for 5 minutes.

Ms. LUJAN GRISHAM. Thank you, Mr. Chairman.

And hearing some of the comments at the tail end, add you may have to repeat some of that. Because representing my district—and, of course, New Mexico, we're home to world-class national security, defense, operating labs and related defense, both private

and public sector, institutions and businesses. And I understand unequivocally the need for being very clear that sensitive, classified security aspects related to information, that we have to be very clear about protecting the integrity of the those systems and that information. Having this committee work on furthering our effort at transparency and recognizing that, across agencies, that we don't have an effective handle about who's determining and what parameters apply and what circumstances before, during, and after information is being shared in a variety of what I would call sort of post- and pre-security issues, I also worry about unintended consequences. And being a longstanding bureaucrat, I could argue either way that having ambiguity can be a protective mechanism to not change anything because you fear those unintended consequences and your own accountability, particularly here where national security is at stake, right? There's no incentive, you know, to be a little bit—to talk about being less risk-averse when we need better transparency in order to inform ourselves in a way that's productive so that you can do policymaking and you can increase the way in which we address national security issues, both in the Congress, both in the bureaucracy, and defend and secure the Nation.

But I also know that it's very frustrating not to have clear direction so that you can make recommendations and include reforms. It's both.

And so, to provide those leaders with better guidance, help me with some very specific ideas about balancing our efforts, the need for transparency and the clear issue that we have, which is also protecting classified secure information and the national security interests of this country, because my constituents are going to say—and they're right—be very careful about unintended consequences here. Because once it's out of the box, it's out.

Anyone?

Mr. AFTERGOOD. I think one way to understand the issue is that classification is treated as a security function, understandably. The people who are making the classification decisions are asking about the security consequences of disclosure. That's fine. That makes perfect sense. The problem is that security is not the only consideration because classifying has implications for oversight. It has implications for public understanding, for diplomacy, for technological development. It can have all kinds of other implications. And to ask the security officer to, you know, weigh the public interest or weigh the diplomatic effects is totally unrealistic, I think. So where that takes me is that in areas of significant interest by Congress or the public, there needs to be an additional venue where this original security classification decision can be reconsidered in the light of broader issues. What is the public interest? What is the need for oversight? What are the undesirable unintended consequences of continuing to classify? Don't ask the poor security officer to make this complicated assessment. Take it somewhere else and reevaluate it in light of the big picture.

Ms. LUJAN GRISHAM. Anyone else? That is in and of itself sort of a balance and a chance for a re-review, as a lawyer and what I would fashion as sort of an appellate aspect. But, again, making those decisions and then creating the parameters for asking for

that guidance is also a set of reforms that can also have unintended consequences. Are there specifics in that regard? And the concept, I think, is one that I think I'm very interested in, but getting to the concept, are there ways to include the agencies in terms of their recommendations about what those parameters would look like, without having them sort of protect their own interests, because that's the other problem, in a way that doesn't get you then to that appellate level, which gets us right back where we started?

Mr. AFTERGOOD. Right. You know, we really need more experimentation in this area than what we have had. I think one model is this ISCAP model, this interagency panel that has been discussed. There may be others. You would want the voice of security represented, of course, but it would not be the only voice, so you would want diversity, diversity of opinion and perspective brought to bear. You would also want to define who could elevate the issue, a congressional committee, maybe just a Member of Congress. You know, who else could ask for this kind of review and under what circumstances? These are all questions that could be hashed out. I don't think the answers are obvious. They might not become obvious until they are tried in practice.

Ms. LUJAN GRISHAM. Mr. Chairman, thank you very much for giving me this extra time, and thank you very much for weighing in on what I think is a really critical issue for us to deal with. So thank you.

Mr. HICE. I thank the gentlelady. The chair now recognizes Mr. Amash for 5 minutes.

Mr. AMASH. Thank you. I yield my time to the gentleman from Kentucky, Mr. Massie.

Mr. MASSIE. I would like to thank the gentleman from Michigan. I have got tons of stuff I want to discuss. I am going to try and get three things in the last 5 minutes. The first two fall under the category of "there is good news, but." Okay. There is good news in terms of the intelligence budget, right, because the 9/11 Commission recommended that at least the aggregate number be disclosed. And so it is disclosed. And the executive branch actually in this case does a better job than the legislative branch. They disclose their request for the budget.

But the situation we had last week is you had 435 Members of Congress, probably less than 80 knew what was in the budget, but they all voted for it. And they can find what is in it 2 years from now. The 2015 number I can tell you. It is on the Web site. We still don't disclose the top-line number, aggregate number, for intelligence appropriations until a year after it has been voted on. So that is the good news, is it is disclosed. The bad news is most of Congress is voting on it to see what is in it.

Now, they could gown to the SCIF, like my colleague from Michigan and I did, and see what is in it, so that is the good news. But some of this is just lack of attention on our part.

Another "good news, but": Mr. DeSantis capably but appropriately pointed out the executive branch has to have secrets to conduct diplomacy, et cetera, et cetera. And then, Mr. Blanton, you talked about how you could use the power of the purse. Well, there is one department that does effectively use the power of the purse for oversight, and that's the Intelligence Committee. They don't

give the intelligence community a tranche of money and say: Okay, you have no strings attached, and we don't want to know anything until next year. They're continuously—that money is contingent upon certain things. And also when certain things happen, they have to be reported back to that committee.

The Judiciary Committee would do well to follow that example. The Judiciary could fence money and say: Look, we're going to give you part of it, but you are not getting the rest of it until we get this answer. So, to the theoretical point of can you get this information from the executive branch or can you not, based on the Constitution, and Article I versus Article II, well, the answer is what you provided, Mr. Blanton: The key is in the power of the purse, and you can always get that information. So that's the good news, is that you can get the information, and the Intel Committee does it. The bad news is DOJ doesn't do it. And the other bad news is the Intel Committee controls this information very tightly, and it is hard for a rank-and-file Member to access that. It is basically 20 questions in a SCIF without staff and no notes walking out. So that is the bad news.

And if I have time, I will let you all comment on that. But here is the third thing I want to talk about, and I think it falls within this committee hearing today, and this question is for Mr. Aftergood. The Federation of American Scientists keeps a bootleg copy of all the Congressional Research Service reports. Is that correct?

Mr. AFTERGOOD. Not all, but many.

Mr. MASSIE. Well, the ones that you can obtain?

Mr. AFTERGOOD. Yes.

Mr. MASSIE. The Congressional Research Service, for those that don't know about it, is this enormous, wonderful resource available to Congressmen. And they have got all the historical context for the reasons of things, and they prepare these wonderful reports, but they're confidential to Congress. And the irony here is I could disclose them to a constituent, but the CRS has no clearinghouse for this. The greater irony is, on a weekend, I go to your Web site to find out what the Congressional Research Service has prepared. How ridiculous is that? I would like your comment on that, Mr. Aftergood.

Mr. AFTERGOOD. There has been a lot of talk lately about fake news and how it is corrupting our public discourse and so forth. To me, I think of CRS reports as kind of the antidote and the opposite of fake news.

Mr. MASSIE. We get a lot of fake information here in Congress from various sources.

Mr. AFTERGOOD. We all need to be critical consumers, but I think the CRS products on the whole are extremely informative. They are balanced. They aim to educate. If you read them, you are going to get smarter than you are.

Mr. MASSIE. That is not hard to do for a Congressman.

Mr. AFTERGOOD. Well, or for a citizens. I don't have too big a chip on my shoulder about doing this. I would just as soon Congress do it the right way. I think you have a product that you can be proud of, and you should be making it available to the public.

Until that happens, I hope to be able to continue doing it through the Federation.

Mr. MASSIE. I hope you do too because I need access to that on weekends. Thank you very much.

Mr. LEONARD. And I would only suggest: It is the end of the year; you might want to contribute to Steve's Web page.

Mr. HICE. I thank the gentleman, and I also want to extend a sincere thanks to each of our witnesses for appearing before us today.

If there is no further business, without objection, the committee stands adjourned.

[Whereupon, at 11:08 a.m., the committee was adjourned.]