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.