PSEUDO–CLASSIFICATION OF EXECUTIVE BRANCH DOCUMENTS: PROBLEMS WITH THE TRANSPORTATION SECURITY ADMINISTRATION'S USE OF THE SENSITIVE SECURITY INFORMATION DESIGNATION

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

MAY 29, 2014

Serial No. 113–121

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 PRINTING OFFICE

88–973 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing 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

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DESANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico
Vacancy

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
STEPHEN CASTOR, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

JOHN L. MICA, Florida, *Chairman*

TIM WALBERG, Michigan
MICHAEL R. TURNER, Ohio
JUSTIN AMASH, Michigan
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
JIM COOPER, Tennessee
MARK POCAN, Wisconsin

CONTENTS

Page

Hearing held on May 29, 2014 1

WITNESSES

Ms. Annmarie Lontz, Division Director, Office of Security Services and Assessments, Transportation Security Administration
Oral Statement 5
Mr. John Fitzpatrick, Director, Information Security Oversight Office, National Archives and Records Administration
Oral Statement 7
Written Statement 9
Ms. Patrice McDermott, Executive Director Openthegovernment.org Coalition
Oral Statement 16
Written Statement 19

APPENDIX

Joint Staff Report Prepared for Chairman Issa and Rep. Cummings 40
Questions for the Record for Annmarie Lontz, TSA 69

PSEUDO–CLASSIFICATION OF EXECUTIVE BRANCH DOCUMENTS: PROBLEMS WITH THE TRANSPORTATION SECURITY ADMINISTRATION'S USE OF THE SENSITIVE SECURITY INFORMATION DESIGNATION

Thursday, May 29, 2014,

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

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2154, Rayburn House Office Building, Hon. John Mica [chairman of the subcommittee] presiding.

Present: Representatives Mica, Meadows, Amash, Issa, and Connolly.

Staff Present: Molly Boyl, Majority Deputy General Counsel and Parliamentarian; Ashley H. Callen, Majority Deputy Chief Counsel for Investigations; Sharon Casey, Majority Senior Assistant Clerk; Kate Dunbar, Majority Professional Staff Member; Adam P. Fromm, Majority Director of Member Services and Committee Operations; Linda Good, Majority Chief Clerk; Ashok M. Pinto, Majority Chief Counsel, Investigations; Andrew Rezendes, Majority Counsel; Jaron Bourke, Minority Director of Administration; Krista Boyd, Minority Deputy Director of Legislation/Counsel; Aryele Bradford, Minority Press Secretary; Cecelia Thomas, Minority Counsel; and Michael Wilkins, Minority Staff Assistant.

Mr. MICA. Good morning. I would like to welcome everyone to the Subcommittee on Government Operations hearing this morning. This morning's hearing will cover the subject and the title of the hearing, in fact, is Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of Sensitive Security Information Designation. That is the title and subject of our hearing today.

The order of business will be first we will hear from members with opening statements.

Mr. Connolly, the ranking Democrat member, is delayed. I have asked one of the representatives of the minority side staff to sit in until he is able to join us. He has a markup, but we do want to proceed with the hearing. We have a long legislative day today and we want to conclude and also, of course, proceed with this hearing in an orderly fashion. So the order of business will be opening statements. We will recognize Mr. Connolly when he is able to join us, but we are going to proceed with the hearing.

After that, we have three witnesses this morning. I will identify them, they will be sworn in, and we will proceed with their testimony.

And from that point, after we hear from all three witnesses, we will go to questions.

With that, I will begin with my opening statement.

Again, I thank everyone for joining us today. One of the things, Mr. Issa, chairman of the full committee, always states is the purpose of our Oversight and Reform Committee is to be good stewards of the trust the American people have given the responsibility of Congress with, and that is to make certain that programs work efficiently, economically, and also in concert with the intent of Congress.

We are stewards of that important trust and it is important that a committee such as ours, which dates back to the early 1800s, when the founding fathers wanted to make certain that not only programs that were created worked as intended, but also that, when they were funded, they were responsibly funded and there was accountability and responsibility. So that is the purpose of our committee and this subcommittee's charge, and we take that responsibility to protect the rights and also the trust of the American people in making certain that the Federal bureaucracy, those responsible, operate in an accountable manner.

So, with that, let me start with my opening statement.

We are actually going to hear the culmination of a committee's investigation over the past year and a half into problems with the TSA's use of sensitive security information designation. The report that has been prepared by the inspector general unfortunately confirms the fact that TSA gamed the system to use a security classification or those classifications to keep Congress and the public from having access to key information in order to protect their own turf. That is what I believe the report shows. I also believe the TSA must end its arbitrary use of sensitive security information designation and use of it improperly, and ensure the security and accountability the public becomes its primary concern.

So today we are going to examine the misuse of the designation. We will explore the improvements TSA has made, some of the report covers some earlier years. We will look at that. And we will also see what the agency has done to educate staff since the committee's investigation began and address the labeling of non-classified information beyond TSA throughout the Federal Government, because we found some similar abuses in other agencies.

Pursuant to the Air Transportation Security Act of 1974, the Federal Aviation Administration created a category of security classification and it is entitled Sensitive Security Information, or SSI, as it is commonly called, a category of sensitive but, in fact, unclassified information.

It is important to note that we are not talking about classified information today. We are not going to discuss classified information. Rather, the subject of this hearing is the realm of unclassified information in this particular designation, SSI. The SSI designation is a pseudo-classification and is not afforded the same protection as other classified information, such as top secret or secret. The SSI regulation restricts the disclosure of information des-

ignated as SSI because public disclosure would be detrimental to, in this case, transportation security.

When used properly, the SSI designation protects sensitive information from public disclosure, which could in some cases be detrimental to certain security interests. Because SSI is an internal TSA, and again we term it pseudo-classification; however, there is potential for misuse of the designation and, unfortunately, we have seen that to be the case.

Bipartisan concerns about TSA's use or misuse of the SSI designation have existed since the promulgation of the regulation in 2004. Following a congressional request to review how TSA used its SSI authority to withhold information from the public, GAO released a report in 2005 finding that TSA lacked adequate internal controls to provide reasonable assurance that the agency is applying the SSI designation consistently.

In July of 2011, DHS Deputy Secretary Counsel Joseph Mayer alleged that subcommittee of this full committee, the chairman, Jason Chaffetz, had unlawfully released portions of a DHS PowerPoint presentation designated as SSI, and that alleged offense, according to, again, DHS, took place during a National Security Homeland Defense and Foreign Operations Subcommittee hearing, and that is one of the subcommittees I am privileged to serve on with Mr. Chaffetz.

Chairman Issa responded to the allegations to then Secretary Napolitano, explaining that Congress is not covered by the regulation governing SSI protection. Such a lack of understanding or disregard of the SSI designation at the highest levels of DHS was concerning.

The subsequent exchange between the committee and DHS prompted a whistleblower at TSA to contact the committee with information regarding the misuse of the SSI designation by political staff at TSA. Our committee, perhaps more than any other, relies on whistleblowers that come forward from the Federal Government departments and agencies, and they often give us tips and information in identifying waste, fraud, and abuse.

As a result of that whistleblowing information, the committee conducted and transcribed interviews with current and former TSA SSI office staff and we obtained hundreds of pages of documents responsive to formal document requests made to TSA.

I am pleased today to announce that Chairman Issa and Ranking Member Cummings are releasing a joint staff report that contains our investigation findings and recommendations. We look forward to making this report a full committee report and we will have it under consideration, I am told, at the next full committee business meeting.

I would like to ask unanimous consent to enter a joint staff report into the record at this time. Without objection, so ordered.

Mr. MICA. The witness testimony and documents show that TSA officials manipulated SSI designations to prevent the release of non-SSI documents. This was first against the advice of TSA's SSI office, whose mission is to evaluate information and determine whether it qualifies in the very beginning as SSI and for that designation. TSA also released SSI documents against the advice of career staff at the SSI office.

While the TSA administrator has the final authority to determine whether information is classified as SSI under the regulation, the administrator must submit written explanations of the SSI decision to the SSI office in a timely fashion. Unfortunately, repeated failures by TSA officials to submit written determinations supporting the release or withholding of SSI caused a rift between senior TSA leadership and the SSI office. This rift resulted in the inconsistent application of the SSI designation. Such consistency, unfortunately, is also shown to be detrimental to the process of protecting sensitive transportation security information.

As a result of the committee's investigation, TSA has made some changes and improvements to its processes for the handling of this SSI information. We look forward to hearing from the witnesses today to hear more about the progress that has been made and improvements by the agency.

TSA's handling of SSI, again, information and use of that designation reveals a broader problem, again, of pseudo-classification of information across Federal departments and agencies, so we found in looking at TSA, unfortunately we found also extends beyond the borders of that agency, and there are broad concerns that agencies, other agencies are using pseudo-classification designations to make it difficult for requesters such as Congress and others to acquire unclassified information.

This raises the possibility that officials may use such information labeling to control the release of non-classified information for political reasons or purposes, again, some serious concerns, and again keeping both the Congress and the public from obtaining information of sort of covering their turf base or improperly using that designation.

Limits on pseudo-classifications are needed, in fact, we think to provide greater transparency and accountability to the public while promoting information security. We have to do both. The committee plans to examine this issue in greater detail and I look forward to future hearings on our findings.

I am grateful for the witnesses who are appearing today and others who have cooperated with the committee. This has been a fully bipartisan effort and investigation, and the product that they have produced that will be made part of the record and accepted by the full committee is again a work developed by both sides of the aisle. So I look forward to hearing testimony today and at this time prepared to hear opening statements or comments from other members. Mr. Meadows?

Mr. MEADOWS. I will be very brief. Thank you, Mr. Chairman, for calling this hearing and for this bipartisan effort to address this issue.

Truly, from the witnesses, what I would look for is how we can improve the process. I think the American people deserve transparency, and any time that that doesn't happen, whether it is intentional or not, it gives a level of distrust, and right now we need to build back that trust in terms of our Government. There are hundreds of thousands of great Federal workers, and for each occasion where something like this gets classified in a wrong setting or the impression is that we are hiding information, it undermines their credibility.

The American people can handle the truth; we just need to make sure that we give them the truth and that we are not doing that. So at this point I just look forward to your testimony. I thank each one of you for being here, and I thank the chairman for his leadership on this particular effort.

I yield back.

Mr. MICA. Thank you, Mr. Meadows.

Members may have seven days to submit opening statements for the record.

When Mr. Connolly returns, he will have adequate time to present an opening statement or participate fully in the hearing, and we will, as I said, proceed because we do need to keep up with the agenda today, a full legislative schedule.

I will now recognize the first panel that we have.

We have Ms. Annmarie Lontz. She is the Division Director of the Office of Security Services and Assessments at the Transportation Security Administration.

We have Mr. John Fitzpatrick. He is the Director of Information Security Oversight Office at the National Archives and Records Administration.

And we have Ms. Patrice McDermott, and she is the Executive Director of the Openthegovernment.org Coalition.

So I would like to first welcome all of our witnesses. I don't know if you have been before our committee before or testified in Congress. What we normally do is we ask you to try to limit your remarks to approximately five minutes. We don't have a big panel or hearing today, so we will be a little bit lenient with that. But if you have additional documents or information or extended testimony you want to be made part of the record, just a request to the chair and we will make certain it appears in the record.

We are also an investigative and oversight committee of Congress, so, therefore, we swear in our witnesses. So if you would stand at this time and be sworn. Raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give before this subcommittee of Congress is the whole truth and nothing but the truth?

[Witnesses respond in the affirmative.]

Mr. MICA. All of the witnesses, the record will reflect, answered in the affirmative, so we will proceed with our first panel.

Let me first recognize and welcome Annmarie Lontz. Again, she is the Division Director of the Office of Security Services and Assessments at TSA.

Welcome, and you are recognized.

WITNESS STATEMENTS

STATEMENT OF ANNMARIE LONTZ

Ms. LONTZ. Chairman Mica, Ranking Member Connolly, and members of the subcommittee, thank you for the opportunity to testify today regarding sensitive security information, or SSI, and the improvements made by the Transportation Security Administration regarding training, designation, and handling.

As the Division Director for the Security Services and Assessments Division for nearly one year, one of my responsibilities is

overseeing the SSI program office, whose charged with the management, consistent application, identification, safeguarding, and redaction of SSI. The SSI program office is staffed by career professionals with significant experience and a comprehensive understanding of SSI and its role in transportation security.

SSI is one of the few types of sensitive, but unclassified, information defined by statute. Congress authorized the Federal Aviation Administration to designate SSI in the 1970s and the FAA promulgated regulations to implement that congressional mandate. When TSA was created, Congress also authorized TSA to designate information as SSI, and TSA regulations to promulgate this mandate are found in 49 CFR Part 1520.

The SSI designation was designed as a tool to protect information obtained or developed in the conduct of security activities, recognizing the potential need to share this information with non-governmental entities, including airlines and other stakeholders.

When it provideD TSA with SSI designation authority, Congress also empowered the administrator of TSA to make final determinations on the disclosure of SSI. TSA's management directive and associate guidance, which governs the SSI program, provides considerations for ensuring that SSI is treated in a manner consistent with the regulation. This directive requires the release of as much information as possible without compromising transportation security, while taking into consideration the information's operational use to adversaries, the level of detail, the public availability of the information, and the age of the record. The goal is to redact as little information as possible to protect SSI.

The SSI program continually evaluates program requirements and areas for potential improvement. TSA has undertaken significant enhancements to the program's policies, training, and management of SSI, including updating the SSI training and making it mandatory for all TSA employees and contractors on an annual basis, refining the redaction process, developing a comprehensive policies and procedures handbook to eliminate gaps in previous guidance, defining specific roles and responsibilities, improving reference guides for DHS employees and contractors, leveraging available technology to improve operations and engage personnel, and standardizing the process through which the administrator may revoke the SSI designation.

Training is an integral part of program and process improvements made by TSA with regard to SSI. The SSI program office has implemented an extensive SSI continuing education training program; conducted targeted SSI advanced training and awareness activities for key TSA stakeholders, DHS components, and other Federal agencies; solidified our internal processes; and recruited and trained SSI coordinators throughout TSA.

TSA supports the efforts made by Mr. Fitzpatrick and the National Archives with regard to controlled, unclassified information and has been an active participant in the development and preparation for implementation of CUI. While there is always room for improvement, I believe that TSA has in place a robust and mature SSI program for the safeguarding of sensitive, but unclassified information and, as a result, SSI identification and safeguarding practices are unlikely to change upon the implementation of CUI.

TSA understands the importance of the SSI designation and recognizes the value of transparency and the need for the public to have access to as much information as possible. We will continue to seek out opportunities to further improve how SSI is identified, managed, redacted, and safeguarded, and work with Mr. Fitzpatrick's office to fulfill the intent of the President's Executive Order regarding controlled and classified information.

I look forward to answering any additional questions that you may have. Thank you.

Mr. MICA. Thank you.

We will now turn to Mr. Fitzpatrick and welcome him and recognize him. Thank you.

STATEMENT OF JOHN FITZPATRICK

Mr. FITZPATRICK. Thank you, Chairman Mica. Thank you for inviting me to testify before you today. I am John Fitzpatrick, the Director of the Information Security Oversight Office, which we call ISOO, at the National Archives and Records Administration.

My office is responsible to the President for policy and oversight of the government-wide security classification system, its companions for industry and for non-Federal partners, and for the controlled unclassified information program. At ISOO, we lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight of department and agency policy and practice.

I will focus today on the controlled unclassified information, or CUI, program, its policy objectives and current state of development.

Executive Order 13556 establishes a uniform system to manage the Executive Branch's sensitive unclassified information that requires safeguarding and/or dissemination controls pursuant to Federal law regulation or government-wide policy. The Executive Order designated the National Archives and Records Administration as the executive agent for the program, and the Archivist of the United States subsequently tasked ISOO with this mission.

Among the program's policy objectives is the promotion of openness and transparency. The CUI program will replace the current confusing and inefficient patchwork of agency-specific practices with a single open and uniform system of policies, procedures, and markings. This new framework is intended to both enhance interagency trust and remove impediments to authorized information sharing through increased clarity of guidance and consistency of practices.

ISOO maintains a publicly available registry of all categories and subcategories of information that meet the Executive Order's standard for protection, providing links to the text of authorizing laws, regulations, and government-wide policies. There are currently 22 categories and 85 subcategories of such information, ranging from sensitive nuclear and critical infrastructure information to personal privacy and business proprietary data, as well as a host of other information types. Sensitive security information, or SSI, is one such subcategory. It is properly authorized as CUI according to the terms of the Executive Order.

The CUI registry also contains all policies and guidance related to CUI. This serves to enhance openness and transparency by making the Government basis for establishing information controls available for all to see. These policies and procedures are being developed in consultation with affected departments and agencies. We also actively seek feedback from State, local, tribal, private sector, as well as public interest groups. Just this month we began the formal Federal regulatory process and will follow that process through agency and public comment to produce a final Federal rule.

The relationship between the CUI program and the Freedom of Information Act, or FOIA, also serves the goals of openness and transparency. Executive Order 13556 draws a bright line between the two, stating that the mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion.

In short, CUI markings and status should not serve as a basis to improperly withhold information from the public, including under the FOIA. This point has been clarified in guidance we have issued in tandem with the Department of Justice's Office of Information Policy, and we have educated agencies on this subject. To further minimize unnecessary control, the Executive Order requires that if there is significant doubt about whether information meets the standard for CUI, it shall not be designated as such.

The CUI program also seeks strong accountability and oversight. Executive departments and agencies have appointed senior agency officials and program managers responsible for program implementation within each agency. These officials are responsible for drafting agency implementing policies, training their employees on program requirements, and establishing a robust self-inspection program to ensure ongoing compliance. Our office will oversee these agency actions by reviewing agency policies, conducting onsite inspections, and requiring agencies to periodically report on the program status.

We have begun, and will continue, to incorporate CUI program progress with ISOO's other reports, which are made public. Taken together, these requirements will help ensure the program is properly and successfully implemented.

In conclusion, ISOO has established a reputation in government for effective oversight and sustainment of constructive relationships with our agency partners. We are well on our way to establishing a stable and robust CUI program for government.

Thank you very much for your time and attention, and I will be happy to answer your questions.

[Prepared statement of Mr. Fitzpatrick follows:]

TESTIMONY OF JOHN FITZPATRICK

DIRECTOR OF THE INFORMATION SECURITY OVERSIGHT OFFICE

BEFORE THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT OPERATIONS

ON

"PSEUDO-CLASSIFICATION OF EXECUTIVE BRANCH DOCUMENTS: PROBLEMS WITH THE TRANSPORTATION SECURITY ADMINISTRATION'S USE OF THE SENSITIVE SECURITY INFORMATION DESIGNATION"

MAY 29, 2014

Chairman Mica, Ranking Member Connolly, and members of the Subcommittee, thank you for inviting me to testify before you today. I am John Fitzpatrick, the Director of the Information Security Oversight Office (ISOO) at the National Archives and Records Administration (NARA). ISOO is responsible to the President for policy and oversight of the government-wide security classification system, the National Industrial Security Program, the Classified National Security Information Program for State, Local, Tribal, and Private Sector entities, and the Controlled Unclassified Information (CUI) Program. ISOO's mission is to ensure the government protects and provides proper access to information to advance the national and public interest. We accomplish this by leading efforts to standardize and assess the management of classified information and CUI through oversight of department and agency practices, policy development, guidance, education, and training.

In my testimony, I will focus on the CUI Program's core policy objectives and current state of development.

The CUI Program is designed to reform a fundamental problem in the Executive branch of an inefficient, confusing patchwork of *ad hoc* agency-specific policies, procedures, and

markings. These agency-specific policies are sometimes unclear to the public and result in inconsistent marking and safeguarding of documents, uncertain dissemination policies, and impediments to authorized information sharing.

President Bush identified the need for a uniform policy, which led to the May 2008 Memorandum[1] that charged NARA as Executive Agent to create a program centered on standardizing the handling of terrorism-related information within the Information Sharing Environment. In turn, the Archivist of the United States established a CUI Office to accomplish this task. On May 27, 2009, President Obama established a CUI Task Force[2], chaired by the Departments of Homeland Security and Justice to review Sensitive but Unclassified (SBU) information practices and make recommendations on implementing a comprehensive CUI policy. On December 15, 2009, Secretary Janet Napolitano and Attorney General Eric Holder jointly released the *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information,* which included a specific recommendation for expansion of the CUI policies beyond the original terrorism-related information scope.[3]

On November 4, 2010, President Obama signed Executive Order 13556 "Controlled Unclassified Information"[4] (the Order), establishing a CUI Program to reform the way in which the Executive branch handles its sensitive information by establishing one uniform system to help agencies manage all unclassified information that requires safeguarding and/or

---

[1] Presidential Memorandum for the Heads of Executive Departments and Agencies on "Designation and Sharing of Controlled Unclassified Information (CUI)," May 07, 2008.

[2] Presidential Memorandum for the Heads of Executive Departments and Agencies on "Classified Information and Controlled Unclassified Information," May 27, 2009.

[3] http://www.dhs.gov/news/2009/12/15/presidential-task-force-controlled-unclassified-information-releases-report-and

[4] Executive Order 13556 "Controlled Unclassified Information," November 04, 2010.

dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. The Order rescinded the May 2008 terrorism-related memorandum and identifies NARA as the Executive Agent to implement the program and oversee department and agency actions to ensure compliance. The Archivist of the United States subsequently tasked ISOO with this mission.

One of the program's core policy objectives is to promote openness and transparency. The CUI Program will replace the current patchwork of agency-specific practices with a single, open and uniform system of policies, procedures, and markings. In addition to helping agencies protect sensitive information, this new framework is intended to remove impediments to authorized information sharing through increased clarity and consistency of practice. Open and clear guidance is expected to enhance trust among agencies and result in increased information sharing. Transparency of these practices should increase the confidence of the American public in the new CUI Program.

We maintain a publicly available CUI Registry of all categories and subcategories of information that meet the Executive Order's standard for protection, namely, the requirement that law, Federal regulation, and government-wide policy require control of the information. Following issuance of the Order, Executive branch agencies reviewed their respective SBU information practices and submitted to the Executive Agent those categories and subcategories that they wished to continue to employ. ISOO reviewed more than 2,200 category and subcategory submissions from 47 agencies and led interagency discussions to consolidate redundancies, provide consistency among like categories and subcategories, and ensure consistency with the standards of the Order. To minimize unnecessary control, the Executive Agent rigorously applied the requirement of the Executive Order that "if there is significant

doubt about whether information meets the standard for CUI, it shall not be so designated as such."[5]

The authorized categories and subcategories of CUI are defined in the CUI Registry along with hyperlinks to authorizing laws, regulations, and government-wide policies that establish the basis for the control of the information. There are currently 22 categories and 85 subcategories of such information, ranging from sensitive nuclear and critical infrastructure information, to personal privacy and business proprietary data, as well as a host of other information types.

Sensitive Security Information (SSI) is one such subcategory and is properly authorized to be controlled on the basis of 49 USC 114 (r), 49 CFR 1520, 49 USC 40119(b)(1), and 49 CFR 15. Under the CUI Program, the specific statutory and regulatory requirements for SSI, such as the safeguarding, dissemination, and disposal of the information will stay the same, while global CUI marking requirements for SSI will be implemented.

Under the CUI Program, the CUI Registry will also contain all policies and guidance for the proper marking and handling of CUI, once these are finalized. This serves to enhance openness and transparency by making the government basis for establishing information controls available for all to see. These policies and procedures have been developed in consultation with the CUI Advisory Council, an interagency body established in June 2013 to advise the CUI Executive Agent on the development and issuance of policy and implementation guidance for the CUI Program. The Council is chaired by the Director of ISOO, and current membership is based on that of the Chief Financial Officers' Council with representatives from 28 agencies to include the Departments of Transportation and Homeland Security, who are regular participants. We

[5] Section 3(b).

also actively seek feedback from State, local, tribal, private sector, as well as public interest groups. ISOO has met with public interest groups throughout the policy development process and incorporated their comments and suggestions.

With formal input from the Council, Council-nominated subject matter experts, and other stakeholders (both Federal and non-Federal), policy has been developed concurrently on multiple levels:

1. An implementing directive to be incorporated into the Code of Federal Regulations (CFR) will include principles and guidelines of the CUI Program applicable to all information and Executive branch users with a lawful government purpose;
2. Supplemental Guidance, including, but not limited to, more detailed procedures, definitions and protocols for appropriate safeguarding, dissemination, marking and decontrol of unclassified information; and,
3. Expansion of the CUI Registry to reflect any additional authorized categories and subcategories, markings, designation authorities, specified CUI requirements, and a glossary of terms.

The draft regulation is currently being reviewed by other Executive Branch agencies and ISOO will collect and respond to their comments. After the inter-agency review process, ISOO will proceed with the balance of the federal rule making process.

The relationship between the CUI Program and the Freedom of Information Act (FOIA) provides further evidence that openness and transparency are desired outcomes of the CUI Program. Executive Order 13556 draws a bright line between the two, emphasizing that "the mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter

of discretion."[6] Decisions to disclose or withhold information must be made solely based on the applicability of the statutory exemptions contained in the FOIA (or other applicable laws, regulations, or policies) and at the time of a request for information.

In short, CUI markings and status should not serve as a basis to improperly withhold or improperly disclose information from or to the public, including under the FOIA. This point has been clarified in guidance we jointly issued with the Department of Justice's Office of Information Policy.[7] In addition, we developed publicly available on-line training based on the joint guidance to educate and provide additional clarity.[8]

Another core objective of the CUI program is strong accountability and oversight. The first step toward meeting this objective entails requiring Executive branch agencies to appoint a senior agency official and a program manager responsible to their agency head, and ISOO, for program implementation within that agency, which ISOO required through its April 11, 2013 memorandum to the agency heads.[9] These designated officials are responsible for drafting agency implementing policies, training their employees on program requirements, implementing new practices while phasing out old ones, and establishing a robust self-inspection program to ensure ongoing compliance.

In consultation with the CUI Advisory Council and OMB, consistent with the Executive Order[10] the Executive Agent is looking to establish deadlines for phased implementation for the

---

[6] Section 2(b).

[7] "Guidance regarding Controlled Unclassified Information and the Freedom of Information Act", November 22, 2011.

[8] http://www.archives.gov/cui/training.html

[9] "Appointments of Senior Agency Official and Program Manager for Controlled Unclassified Information (CUI) Program Implementation," April 11, 2013.

[10] Section 5(b).

Executive branch that will be set forth in a National Implementation Plan. Implementation will begin with the publication of the final regulation in the CFR and the issuance of the supplemental guidance. ISOO expects that agencies will require about one year after publication of the final regulation to reach initial operating capability, by preparing their internal implementing policies based on the national guidance and conducting their training of employees to handle, recognize, and receive CUI. We plan to assist these efforts by providing online basic CUI training that will be published on ISOO's website. It is anticipated that based on budgetary cycles and the required transition of information systems, the elimination of old SBU markings and their replacement by the new CUI standards, procedures, and markings will take place within two to three years after initial operating capability is reached.

ISOO will oversee these agency actions in multiple ways, including reviewing agency policies, conducting on-site inspections, and requiring agencies to periodically report on the program's status. We are also required under the Executive Order to regularly publish a report to the President on the status of agency implementation. These reports are made public along with ISOO's other reports on the status of the classification system. Taken together, these requirements will help ensure this program is properly and successfully implemented.

In conclusion, ISOO has established a reputation in the government for effective, objective oversight, consistency in practice, and maintenance of mature, constructive relationships with our agency partners. We are well on our way to establishing a stable and robust CUI Program, effectively integrating CUI into ISOO's Executive branch-wide role. Thank you very much for your time and the opportunity to appear before you today. I will be happy to answer your questions.

Mr. MICA. Thank you for your testimony, Mr. Fitzpatrick.

We will now turn to Ms. McDermott. She is the Director of Openthegovernment.org Coalition. Welcome, and you are recognized.

STATEMENT OF PATRICE MCDERMOTT

Ms. MCDERMOTT. Thank you very much and thank you, Chairman Mica and Vice Chair Meadows, for the opportunity to speak today on the continued use of sensitive but unclassified markings in the Executive Branch, three and one-half years after the issuance of President Obama's Executive Order.

My name, as you said, is Patrice McDermott, and I am the Executive Director of Openthegovernment.org, a coalition of nearly 90 organizations dedicated to openness and accountability. My remarks here today do not necessarily represent the positions of all of our partner organizations.

Let me start with a little history on the issue of the use of sensitive but unclassified markings in the Executive Branch.

In May 2008, President Bush issued a presidential memorandum with a stated intent to standardize control markings and handling procedures across the information sharing environment, a term codified in the Intelligence Reform and Terrorism Prevention Act of 2004, to indicate the intelligence, law enforcement, defense, homeland security, and foreign affairs communities. The CUI Council called for in the memorandum was a subcommittee of the Information Sharing Council within the Office of the Director of National Intelligence and, therefore, entirely outside any public access or accountability.

That memorandum did nothing to rein in the use of what were called sensitive but unclassified markings. In fact, the memo allowed agencies to continue to make control determinations as a matter of department policy, meaning that the public was given no notice or chance to comment on the proposal.

Under President Bush's proposed framework, control designations could easily have been treated as simply another level of classification, reducing the public's access to critical information.

On November 3rd, 2010, President Obama issued the Executive Order on controlled unclassified information, 13556. The order limits control markings to those, as Mr. Fitzpatrick noted, based on government-wide policy, as well as statute or regulation. This is an enormous victory for openness. This limitation will, when fully enacted, both significantly limit the number and end the spiraling proliferation of agency policy markings, most particularly for official use only.

Organizations working on government openness and accountability and on whistleblower protections welcome the release of the Executive Order, which rescinded the Bush Administration memorandum and which requires standardizing and limiting the use of control markings on unclassified information. The openness community applauded the Obama Administration for making this an open government document, when it could easily have become quite the opposite.

Earlier drafts of the Obama order would have allowed agencies to continue using the designations that were not based in either

statute or regulation. Previous drafts would have created a system of sanctions which the openness community was concerned would impede needed sharing and could lead to repercussions outside current law for whistleblowers. The new order has none of this language, reflecting its role as a government-wide information policy.

A key aspect of the order is that it makes clear, as Mr. Fitzpatrick noted, that a CUI marking has no bearing on the decision to disclose information under the Freedom of Information Act or on the disclosure to the legislative or judicial branches of the U.S. Government. Finally, the order involved the public in consultation on the implementation of the new framework.

It was significant that the process in the Obama Administration began in a manner not dissimilar to that under the Bush Administration. While we did have opportunities to meet with government officials involved in the work on CUI and there were officials involved who were deeply committed to government transparency, the early discussions and drafts were led by the National Security staff and based on a report from a task force led by the attorney general and the secretary of Homeland Security. They came to this with an approach quite similar to that of the Bush Administration, that this was about controlling dissemination of and access to sensitive but unclassified information to those with a recognized need to know.

We had numerous meetings and were able to review drafts in the meetings, and we provided extensive comments. Finally, we were presented with what government officials considered the final draft and we were asked for our headline. We responded that the headline of the openness and whistleblower communities would be Obama Creates Fourth Level of Classification. Apparently, this derailed the train that had been moving down the track. At some point in this time frame, OMB also became involved in the process. The draft that came out next took what essentially had been a National Security-driven effort and turned it into what it properly was, a government-wide information management policy.

So the agency policy markings are to be ended. The question for us is when. Regrettably, here is where the rub comes in. The CUI staff worked extraordinarily hard, with very limited resources, to create the registry of approved CUI categories and subcategories that was released in November 2011. It is accompanied, however, with a "reminder from the executive agent" which says existing practices for sensitive unclassified information remain in effect until the CUI marking implementation deadline TBD, to be determined.

Again I want to stipulate that the CUI staff housed that ISOO have been very open. They have initiated meetings with our communities and have been willing to meet with us at our request. They have taken our concerns and our comments on various implementation drafts very seriously and have made changes along the way.

Our concern is that the process is, from our perspective, at least, a long way behind schedule. We suspect this is due to the intransigence and resistance from some agencies, and the adjudication the CUI staff had to do with them. The executive agent expect the CFR, which is now at OIRA and about to go out for agency com-

ment, to become effective in April 2015. That begins an extended progress, in six month segments, of agencies only then beginning to develop the budget, IT, and training toward a requirement of which they will have been aware for almost five years.

Agencies will not begin to implement CUI practices or to phase out obsolete practices until April 2016, and not until 2017 and beyond, into the next decade, will agencies finally begin to eliminate old markings and assure use of only new markings that are on the registry. The executive agency indicates an expectation that this process will extend into 2018, 2019, and beyond, well beyond the end of the current Administration.

What does this mean in practice? The President was clear that the mere fact that information is designated as CUI shall have no bearing on determinations pursuant to any law requiring disclosure of information or permitting disclosure as a matter of discretion. Agencies, however, continue to use not CUI registry markings, but the existing practices, especially FOUO.

I will stop here, as I am well over time, but I do have some examples, if I have time in the questioning.

Mr. MICA. If you would like, we will grant you an additional minute or two.

Ms. MCDERMOTT. Okay, good. Thank you.

So, as an example, the Project on Government Oversight recently reported on a DOD IG report that the Pentagon labeled FOUO. It says in such cases, the DOD IG will only post the report's title or summary on its website. The complete report must be requested through FOIA. POGO was fortunate enough to have obtained the contract overbilling report through non-FOIA means, but they are still waiting on requests for two other DOD IG reports. Both of these reports are unfavorable assessments of other Defense contracting programs.

And just this morning there is a story in The Guardian by Jason Leopold that quotes from internal NSA emails about both journalist and citizen requests under FOIA. They dismiss the citizen requests pretty summarily and note that journalists are a little harder to get rid of. And one of the officials is quoted as saying the classified and FOUO we can deny; the rest we may have to process.

Well, according to the Executive Order, they are not allowed to deny, to withhold stuff just because it is marked FOUO. But it is apparently a continuing attitude throughout the Government, and we are as frustrated as you are and very concerned that this attitude will continue for many years to come.

Thank you for the opportunity to speak to you on this important issue. I am happy to answer any questions you might have.

[Prepared statement of Ms. McDermott follows:]

OPEN THE GOVERNMENT.ORG
AMERICANS FOR LESS SECRECY, MORE DEMOCRACY

Statement
Of
Patrice McDermott
Executive Director
OpenTheGovernment.org

Subcommittee on Government Operations
Committee on Oversight and Government Reform
On
The Growing Use of the Unclassified Designation of Information in
the Executive Branch Departments and Agencies
May 29, 2014
2154 Rayburn House Office Building
10:00 am

Thank you, Chairman Mica, Ranking Member Connolly, and Members of the Subcommittee, for the opportunity to speak today about the continued use of Sensitive But Unclassified markings in the Executive Branch, three and one-half years after the issuance of President Obama's Executive Order. My name is Patrice McDermott and I am the Executive Director of OpenTheGovernment.org, a coalition of nearly ninety organizations dedicated to openness and accountability. My remarks here today do not necessarily represent the positions of all our partner organizations.

Let me start with a little history on the issue of the use of Sensitive But Unclassified markings in the Executive Branch. In May 2008, President Bush issued a Presidential Memorandum with the stated intent to standardize control markings and handling procedures across the "information sharing environment," a term codified in Intelligence Reform and Terrorism Prevention Act of 2004 to indicate the intelligence, law enforcement, defense, homeland security, and foreign affairs communities. The CUI Council called for in the Memorandum was a subcommittee of the Information Sharing Council within the Office of the Director of National Intelligence and, therefore, entirely outside any public access or accountability.

That memorandum did nothing to rein in the use of what were called Sensitive But Unclassified markings; in fact, the memo allowed agencies to continue to make control determinations as a matter of "department policy" — meaning that the public was given no notice or chance to comment on the proposal. Under President Bush's proposed framework, control designations could easily have been treated as simply another level of classification — reducing the public's access to critical information.

On November 3, 2010, President Obama issued the Executive Order on Controlled Unclassified Information. The Order limits control markings to those based on government-wide policy, as well as statute or regulation. This is an enormous victory for openness. This limitation will, when fully enacted, both significantly limit the number and end the spiraling proliferation of "agency policy" markings, most particularly "For Official Use Only."

Organizations working on government openness and accountability and on whistleblower protection welcomed the release of the Executive Order, which rescinded the Bush Administration CUI memorandum, and which requires standardizing and limiting the use of control markings on unclassified information. The openness community applauded the Obama Administration for making this an open government document when it could have become quite the opposite.

Earlier drafts of the Obama order would have allowed agencies to continue using designations that were not based in either statute or regulation, but were created by "agency policy." Previous drafts would have created a system of sanctions, which the openness community was concerned would impede needed sharing and could lead to repercussions outside current law for whistleblowers. The new Order has none of this language, reflecting its role as government-wide information management policy.

A key aspect of the Order is that it makes clear that a CUI marking has no bearing on the decision to disclose information under the Freedom of Information Act, or on disclosure to the legislative or judicial branches of the U.S. government. Finally, the Order involves the public in consultation on the implementation of the new framework.

It was significant that the process in the Obama Administration began in a manner not dissimilar to that under the Bush Administration. While we did have opportunities to meet with the government officials involved in the work on CUI – and there were officials involved who were deeply committed to government transparency – the early discussions and drafts were led by the National Security Staff and based on the Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information, a task force led by the Attorney General and the Secretary of Homeland Security. They came to this with an approach quite similar to that of the Bush Administration – that this was about controlling dissemination of and access to 'sensitive but unclassified' information to those with a recognized need-to-know. Recognized within the information sharing environment, of course.

We had numerous meetings and were able to review drafts in the meetings, and we provided extensive comments. Finally, we were presented with what the government officials considered the final draft of an Executive Order and we were asked for our 'headline.' We responded that the headline of the openness and whistleblower communities would be "Obama Creates 4th Level of Classification."

Apparently, this de-railed the train that had been moving down the track. At some point in this timeframe, the Office of Management and Budget also became involved in the process. The next thing we heard was that a new draft was in the works. That draft took what essentially had been a national security driven effort and turned it into what it properly was – a government-wide information management policy.

So, the "agency policy" markings are to be ended. The question for us is "When?" Regrettably, here is where the rub comes in.

Implementation

The CUI staff worked extraordinarily hard, with very limited resources, to create the Registry of approved CUI categories and subcategories. It was released in November 2011. It is accompanied, however, with a "Reminder from the Executive Agent: **Existing practices for sensitive unclassified information remain in effect until the CUI marking implementation deadline (TBD).**"

I want to stipulate that the CUI staff housed at ISOO (at NARA) have been very open: they have initiated meetings with our communities and have been willing to meet with us at our request; they have taken our concerns and our comments on various implementation drafts very seriously and have made changes along the way.

Our concern is that the process is – from our perspective, at least – a long way behind schedule. We suspect that this is due to intransigence and resistance from some agencies and the "adjudication" the CUI staff has had to do with them. We saw and commented on draft language in March 2011, again – after two years – in January 2013, and most recently in the early part of this year. The process has now moved to OIRA and to agency comment and, again, adjudication. Later this summer, the public will have an opportunity to comment.

It is the timeline after the review process that especially troubles us. The Executive Agent expects the CFR to become effective in April 2015. Then begins an extended process, in 6-month segments, of agencies only then *beginning* to develop the budget, IT, and training toward a requirement of which they will have been aware for almost five years. Agencies will not begin to "implement CUI practices" or to "phase out obsolete practices" until April 2016. And not until 2017 – and beyond into the next decade – will agencies finally *begin* to "eliminate old markings" and "assure use of only new marking" that are on the Registry. The Executive Agent indicates an expectation that this process will extend into 2018, 2019 and beyond. Well beyond the end of the current Administration and its openness impetus.

So, bearing in mind the Executive Agent's reminder that "Existing practices for sensitive unclassified information remain in effect until the CUI marking implementation deadline (TBD)," the public – and Congress – will not stop seeing markings like FOUO until sometime in the third decade of this century.

What does this mean in practice?

The president was clear that "the mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches."

Agencies, however, continue to use -- not CUI-registry markings -- but the "existing practices," especially FOUO, to either withhold or to make it difficult for requestors to get information that should otherwise be public. As an example, the Project on Government Oversight recently reported on a DOD IG report that the Pentagon labeled FOUO: in such cases the DoD IG will post only the report's title or a summary on its website. The complete report must be requested through the Freedom of Information Act (FOIA).

POGO was fortunate enough to have obtained the contract overbilling report through non-FOIA means, but they are still waiting on requests for two other DoD IG reports, one of which they filed nine months ago. Both of these reports are unfavorable assessments of other defense contracting programs.

We are as frustrated as you and continue to push the Executive Agent and OMB to move the implementation along in a more timely manner.

Thank you for the opportunity to speak to you on this important issue. I am happy to answer any questions you might have.

Mr. MICA. Well, thank you.

We will withhold questions for a minute. We have been joined by our ranking member, Mr. Connolly, and I would like to recognize him at this time.

Mr. CONNOLLY. Thank you, Mr. Chairman. Again, my regrets for being late. I had a markup at the House Foreign Affairs Committee on a North Korea sanctions bill I am coauthor of, and I had to be there for my own bill. So forgive me for being tardy in coming to this hearing.

Thank you all for participating and thanks, Mr. Chairman, for holding this hearing examining the categories of controlled unclassified information, CUI, particularly the Transportation Security Administration's designation of sensitive security information, SSI.

Pseudo-classification designations are often vague and involve undefined markings that prevent interagency sharing or delay public access to information, as Ms. McDermott was just telling us. The Executive Branch's use of pseudo-classification designations is a longstanding national security challenge, and it certainly encompasses many administrations of both parties and transcends partisan division.

The 9/11 Commission observed, in its final report officially on the September 11, 2001 terrorist attacks, that excessive barriers to information sharing among Federal agencies and between Federal agencies and local law authority agencies actually contributed to the confusion, if not to the actual successful prevention of the tragedy. That is pretty strong stuff. Simply put, the Government agencies keep too many secrets from other Government agencies and the public, and that is both bad for public safety and, in my view, can compromise national security unintentionally.

Our committee has been concerned with the effects of pseudo-classification for many years. This committee requested that the GAO study the matter and, in 2006, during the Bush Administration, GAO reported that the problems posed by excessive and inappropriate use of CUI remain pervasive, pervasive, across the Federal Government.

Our committee's concern, Mr. Chairman, about the TSA's utilization of SSI designations dates back to 2008, six years ago, when former Chairman Waxman and Ranking Member Tom Davis, my predecessor, initiated a bipartisan inquiry questioning TSA's release of SSI to CNN for use in a news story, when the agency had asked GAO not to publicly disclose the same type of information, seemingly a contradiction in policy.

Further, conflict over the proper handling of SSI continued in 2011, when the U.S. Department of Homeland Security expressed serious concern over the disclosure of SSI by a member of this committee, the Oversight Committee, at a public hearing.

As recently as 2012, the Controlled Unclassified Information Office within the National Archives and Records Administration found: "Historically, executive departments and agencies have employed ad hoc agency-specific policies, procedures and markings to safeguard and control the dissemination of sensitive but unclassified information." "As a result," it found, "more than 100 different policies and markings have evolved for handling such information across the Executive Branch." It goes on: "This inefficient confusing

patchwork system has resulted in inconsistent markings and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing."

Fortunately, the Obama Administration has taken steps to try to get CUI policies under control. I was pleased that President Obama issued the November 4th, 2010 Executive Order 13556 on CUI that mandated that NARA establish categories and subcategories to serve as the exclusive designations for identifying unclassified information that requires safeguarding or dissemination controls pursuant to statute, regulations, or government-wide policy.

In April 2012, TSA Administrator John Pistole issued a new SSI handbook applicable to all TSA personnel that established standard operating procedures for handling SSI and consolidated and clarified SSI policy guidance. These new policies include standardizing policies for the revocation of SSI, creating a system for reporting breaches, and improving employee training on how to handle SSI.

In closing, Mr. Chairman, it is my hope that the stakeholders gathered here today will recognize we all have a shared goal with respect to increasing transparency and strengthening aviation security, and that balancing these interests need not be a zero sum proposition, it is either transparency or it is keep it close to the vest and nobody knows what anyone else is doing.

I want to thank our witnesses for participating in this morning's hearing and, Mr. Chairman, I look forward to examining, together with you, how we can better ensure CUI is effectively, consistently, and appropriately managed across the entire Federal Government.

Thank you. I yield back.

Mr. MICA. Thank you, Mr. Connolly.

We will go right to questions. I want to lead off on some of the points that the ranking member articulated. First of all, he cited the Executive Order 13556 which President Obama issued, and I think you spoke about it too, Ms. McDermott, and had some good intent, but it has had no bearing on decisions to disclose information pursuant to FOIA or disclosures to judicial or legislative bodies such as this committee. Despite this, Ms. McDermott, are you currently observing Federal agencies that use existing practices to thwart release of unclassified information?

Ms. MCDERMOTT. As I mentioned—yes?

Mr. MICA. I am just asking you to confirm again what you said.

Ms. MCDERMOTT. Oh. Yes.

Mr. MICA. Mr. Connolly brought this up, but you are seeing that.

Ms. MCDERMOTT. But I would also note that——

Mr. MICA. And how prevalent is the practice today?

Ms. MCDERMOTT. Okay. I don't know that it is all that prevalent. We do know examples, but you usually only hear when there is a problem. I mean, you can't disprove a negative, but if agencies aren't doing it, there is no way to know.

Mr. MICA. And you cited some problems. What agencies is this prevalent or have you seen?

Ms. MCDERMOTT. The Department of Defense Inspector General's Office and the FOIA folks at NSA.

Mr. MICA. Okay. Is there anything more that can be done? We have an Executive Order. What do you think? Now, TSA, we will get to them in a minute; they have issued a handbook. But what do you see government-wide?

Ms. MCDERMOTT. Well, I think government-wide the process has been moving forward in terms of the work that the executive agent, the CUI Office, has been doing. I think, from our perspective, the problem is that somewhere along the line time has been lost and we feel that the process is taking longer than we anticipated and that I think probably the President anticipated.

Since the issuance of the Executive Order, we are already now four years out, and the rule is just going out for comment. We had seen earlier versions in 2011 and then not again until 2013, and then again this year. So the process, our sense is that it is being slowed by at least some agencies who—again, this is my perspective and my community's—who don't want to see this because it will control their ability to use these markings as they see fit. But I think it is our sense from talking to CUI staff that there are a lot of agencies also that are fully onboard, ready to go, and who will move forward quickly.

Mr. MICA. Well, that is a perfect sequence to ask Ms. Lontz why did it take four years for TSA, after the management directive, to roll out the handbook? Now, Mr. Connolly also spoke of successive TSA and finally getting a handbook, but it took four years and you just testified that they have been slow-rolling this, Ms. McDermott. So what is happening that took four years to do this in TSA?

Ms. LONTZ. Mr. Chairman, so the joint decision to move the SSI program into the Office of Law Enforcement and Federal Air Marshal Service from the Office of Intelligence, that occurred in December of 2010, and Mr. Pistole did sign our TSA management directive in April of 2012.

Mr. MICA. The structural placement was also almost four years ago, but it has still taken almost four years to get, again, the handbook on SSI.

Ms. LONTZ. So the handbook is a comprehensive resource of 74 pages, and it is a guide to all employees.

Mr. MICA. So they did about 20 pages a year.

Ms. LONTZ. We do annual training on SSI to all employees at TSA.

Mr. MICA. The handbook was just issued, so has that just begun?

Ms. LONTZ. So the annual training occurs and also began in 2012, so each employee at TSA has received it now at least twice. So the program office itself has a standard operating procedure that is a 40-page document that they use daily in the practice of reviewing documents, and we also have standardized the way that requests are made so that it is documented appropriately, and we also have incident reporting tools for the agency to utilize.

Mr. MICA. Now, tell me again where the SSI office falls, under what jurisdiction was it set?

Ms. LONTZ. So it originally was with the Office of Intelligence. It is now under the Office of Law Enforcement Federal Air Marshal Service.

Mr. MICA. And why does it fall under that particular one? It seems like Intelligence would be the logical one. Why was it re-

moved and what is the advantage to have it under law Enforcement?

Ms. LONTZ. So we felt that it more closely aligned to the duties and responsibilities of the chief security officer, and the chief security officer is part of the Office of Law Enforcement.

Mr. MICA. And how many FOIA requests does TSA receive in a year, do you have any idea, for instance, 2013 FOIA requests?

Ms. LONTZ. I can tell you to date we have received 72 requests, just under about 10,000 pages to review this year.

Mr. MICA. Just this year.

Ms. LONTZ. Correct.

Mr. MICA. But you don't have a figure for a number received in 2013?

Ms. LONTZ. I don't.

Mr. MICA. Maybe you could provide that to the committee.

Ms. LONTZ. Certainly.

Mr. MICA. What percentage of FOIA requests to TSA are denied or redacted due to the targeted information carrying the SSI designation, do you have any idea?

Ms. LONTZ. I don't have an idea on that. We review all FOIA request material that is sent to our office. Each review is done the same as it would be for any other request that would come through SSI, and it is all memorialized in a memorandum of what was reviewed and what the findings were, and then it is returned back to the FOIA office.

Mr. MICA. Has the TSA implemented proper protocols to ensure that the TSA administrator is documenting support for releasing SSI prior to releasing the information?

Ms. LONTZ. So there is a process for revocation as well, and it must be in writing, and it should be in the interest of security, of course.

Mr. MICA. Do you know if there is compliance now? I mean, it was pretty spotty. The reports were spotty as to compliance with that requirement, again, prior to releasing the information. Do you know where we are on that now? In almost every instance is that complied with?

Ms. LONTZ. Yes, sir. So Mr. Pistole is our administrator and he is the designated authority on the release, so anything that would be released would go through his office.

Mr. MICA. Well, it sounds like TSA has cleaned up some of the problems.

Ms. McDermott, you have been observing this. Is that your observation or assessment?

Ms. MCDERMOTT. We have been really looking more at the CUI process and the rollout of the rule relating to the Executive Order, how it is being implemented. I have colleagues who work more at agency level, so I really can't speak to that.

Mr. MICA. Okay. You have not had any specific observation or have you found improvement in that regard, Mr. Fitzpatrick, from TSA?

Mr. FITZPATRICK. So our office does not look at or have authority to look at the specific transactional actions of release or withholding under the FOIA or any other statute. What we look at is management approach to an authorized category, which SSI is, and

how is it managed within the organization and are its procedures for safeguarding dissemination, control, and marking, how are they promulgated and will they be consistent with the forthcoming rule. So the retention of information under a separate authorization is not within our oversight purview but, rather, the administration of the security program.

Mr. MICA. Well, I asked Ms. McDermott before about the prevalence of the pseudo-classifications in other agencies. Would you like to comment on that?

Mr. FITZPATRICK. Yes, I would, because I think we have both described the scope of the Executive Order. When it shifted from the Bush Administration's focus on homeland security and counterterrorism information to any type of information for which control is authorized under law government-wide policy or government-wide regulation. That is a vast amount of information, and while it does provide the opportunity to define the universe of CUI and to identify that which is not authorized for withholding or retention, so that is a primary division of the universe of unclassified information into two halves.

The half that is authorized is substantial. As I mentioned in my testimony, there are 22 categories, 85 subcategories, so we have organized information in a plain English sort of way to describe categories and subcategories, but there are 314 unique citations in law, government-wide policy, or Federal regulation that authorize control of unclassified information. Four of those apply to the SSI category; many of those categories and subcategories have multiple citations in law and regulation.

So what we have discovered in the time that it takes to sort of understand the scope of the Executive Order and to build this registry is that the Legislative and Executive Branch, in almost equal measure, have authorized agencies to assert control over information types of a very broad range. One hundred fifty-seven of those controls are in statute, 129 in Federal regulation, and 28 in government-wide policy of the type of an OMB circular, something that would have come out of the Executive Office of the President.

So that is a lot of information, a lot of agencies that are authorized to withhold this information. So our program is created to identify which those are so that you can know which information types aren't, and then to establish handling and marking procedures of a uniform nature rather than I think the ranking member indicated the 100-plus marking types and bins that information had been put on and labeled, to have a uniform control marking.

I am sympathetic to the amount of time that this is taking. When you understand the scope of this and how many agencies have this type of information, to try to understand all of their practices today in order to create a uniform baseline that all will observe, it is a very time-consuming effort.

Mr. MICA. Well, unfortunately, today we are just talking about unclassified information, and, you know, this is an important issue because Government information and the management of it can be manipulated and agencies use it to cover their own tracks, to keep information from Congress and from the American people, and that is just in an unclassified category, and then trying to set the parameters for that. Then you have so many agencies that have par-

ticipated and then trying to make certain there is some objective evaluation of what they are using these classifications for and denying Congress or the public or information getting out.

The classified is a whole different one with TSA. I would like to see, at some time, information on the failure of performance of TSA. Most of that has been kept in a classified realm, declassified on a periodic basis, so I think the public deserves to know the performance of some of the people who are supposed to provide important transportation security. That has been kept under wraps or some things have been put under classified wraps to keep their performance secret, and there are definite reasons to do that.

I know in the past some classified information has been released and I have flipped out a couple of times when I saw it in the paper and actually asked agencies to go after folks who had released the information, because it can be very harmful. But, by the same token, there is some other information, I think, that the public should know that deals with the performance of agencies.

Now we have, it is not classified, but we are seeing the secret lists of the VA and people trying to cover up again their poor performance, and that was outrageous by any standard.

Well, it is an interesting subject. Difficult to get a total handle on, but we are trying to make some sense out of it in a bipartisan fashion. Part of the report goes back, I noticed, some time and predates current practices, but this is a meat and potatoes hearing where we have been, where we are, and where we are going. So I thank you all.

Let me yield to Mr. Connolly for questions.

Mr. CONNOLLY. Thank you, Mr. Chairman. Actually, to me, it is kind of a thought-provoking panel and discussion, but to your very last point, so here we are looking at the operations of government, can we improve them and make them better and more efficient, better serve our public. There is not a single member of the press at the press table, not one.

Mr. MICA. Nobody is interested.

Mr. CONNOLLY. And in the system of reward and punishment, there is not a lot of reward for what we are doing today, Mr. Chairman, but virtue is its own reward, I guess, right?

But thank you for being here, because it is actually kind of an important topic.

The chairman talked a little bit about the misuse of types of information for various and sundry purposes, either hiding it from the public and/or Congress or deliberately getting it out there when you shouldn't.

Ms. Lontz, we issued a committee staff report today that found TSA for years had issues with consistently implementing its policies for designating and undesignating information as sensitive security information. The committee heard from a former director of TSA's SSI Office, Andrew Colsky, that TSA's Office of Public Affairs released information strategically in what he described as security theater. He said, "If they felt they needed to do something to get it in the press to change the public perception, that was more important than the security concerns involved."

That same director said that the release of SSI by the Office of Public Affairs decreased when the personnel changed in 2009 with the new administration.

What is the current relationship between the SSI Office and the Office of Public Affairs, and how disputes regarding SSI, how are they resolved?

Ms. LONTZ. Certainly. So the relationship really of the SSI Office to really any of the other directorates, we operate autonomously. We receive in information that needs review and we do that and review in accordance with all of the requirements and then return it. We do not engage regularly with any of those offices other than to be the recipient and provide our service and provide it back. So there isn't any direct back and forth between the Office of Public Affairs and our SSI Office other than the service that we provide.

Mr. CONNOLLY. Well, but what are the systems in place for ensuring, the chairman cited it, that someone misuses information for entirely a PR purpose? It did happen at your agency before your time. What are the mechanisms in place to ensure that there is an understanding, to pick an office, between the Public Affairs Office and the SSI Office that the misuse of such information for perhaps a noble reason, but nonetheless the misuse of information is protected, that that practice is controlled?

Ms. LONTZ. So we did some significant training with the various offices after 2010, or actually after 2012. We did specific training in offices like the Office of Chief Counsel, Office of Public Affairs to provide them with in-depth understanding of what SSI is and is not. So they have received more than just the annual training that all TSA employees receive so that they have a greater knowledge of what we would consider SSI and how to handle it properly.

Mr. CONNOLLY. Mr. Fitzpatrick, you honed in on my reference to the fact that we have 100 different standards, apparently, maybe more. Ms. McDermott, I welcome your comment as well. When one looks at a statistic like that, I often ask the question, rhetorically, What could go wrong with that? If the public were watching this hearing, I think they would get a headache from all the acronyms and maybe lose sight, easy to lose sight of, well, what is the context here? What is it we really are concerned about?

We are not just concerned about juridical processes. We are concerned about preserving that which must be preserved, concerned about proper information sharing and encouraging that, instead of people hoarding information that should be shared, and trying to have a streamlined system so that rules of engagement are clear-cut and everybody adheres to them. How are we doing on that? I mean, how much progress since the Executive Order, and to what extent has the Executive Order encouraged such progress, are we getting to have a more uniform standard across the Federal family?

Mr. FITZPATRICK. So thank you, because that is the wheelhouse of building a CUI program, is to address those very things. Let me put some of these numbers into context.

That number, 117 different markings, actually comes from an appendix of the report that Patrice mentioned that the attorney general and the secretary of Homeland Security provided President Obama in the year before the Executive Order was issued, and they took an inventory. How many different ways are we marking

things? How confused is this? You quoted one of my office's reports, a Confused Inefficient Patchwork.

So what is in play or what the practices were allowing 1,000 flowers to bloom? An agency could and did make up its own rules and there was no canopy type of guidance that said it had to follow some stricture or some consistency across government. So you had people marking any kind of information with a special marking. Maybe it was just sensitive, do not disseminate; limited distribution; source selection information; help related information. Some of these are instructions and some of these are categories of information.

So what the Obama Order does is it says, okay, the only ones that are authorized for some type of control are the ones where a deliberative process, a statute, regulation, or government-wide policy, has already provided that authority; everything else is not permitted to have some control. So it said, executive agent, find out what that universe of information is, put a registry together and put it out on the internet so everybody can understand what have we done through statute and regulation to provide these authorities, and then work with agencies to come up with practices that will be uniform, one set of markings, one set of handling requirements.

We are in touch with 150-plus government entities to try to find out what kind of information do they have, what kind of resources do they have, what kind of practices do they have. There is a lot in common; put it in a locked drawer. Some of this guidance the lock has to be this kind of lock, the drawer has to be this kind of drawer; wrap it in one envelope, two envelopes, three envelopes. Again, 1,000 flowers blooming. So we are creating a single baseline and these are represented in the draft rule that we have mentioned, finally getting enough interagency agreement to say that would work for us to put it into practice and for agencies to implement.

The category types that remain are information types that you would expect every agency to handle: privacy, financial. Agencies that handle taxpayer information, there is a specific regime for protecting taxpayer information. SSI is an example. Another good example that exists only in a particular space in government activity is unclassified controlled nuclear information. So Energy, Defense, Transportation, they handle nuclear materials; that is special stuff. So we have catalogued across the whole of Government agency practice and our attorney and other resources have put that together in this registry that says 314 unique citations, 157 laws that say the secretary may withhold or must control or may disseminate.

Mr. CONNOLLY. That you have to take into account.

Mr. FITZPATRICK. Right. So we are trying to wrap an umbrella over this vast authorized practice.

Now, identifying the authorized practice allows you to identify the unauthorized and discontinue the unauthorized, and that is naturally where Patrice and her Coalition's interest lies, with the ability to regulate the authorized practice across global organizations with however many Federal employees have to be trained. It is a daunting effort, and it can't start until the flag is waived. The

flag gets waived when the rule is final. So we are in the process right now with the rule out for agency comment; it will then go out through public review and comment and keep going.

Mr. CONNOLLY. But let me follow up on something the chairman—and I am going to call on you, Ms. McDermott. I just want to stay with this, but I will ask you to comment as well, if the chairman will allow.

Mr. MICA. Go right ahead.

Mr. CONNOLLY. Thank you, Mr. Chairman.

I want to follow up on something the chairman made a point of, though; and he and I share this characteristic. In politics and public policy, sometimes patience is a real virtue. Sometimes it is not; sometimes impatience is a virtue because it gets things done and moving. And sometime it strikes the chairman, and me as well, that we move at a glacial pace in the Federal Government, when we need to be moving with more alacrity.

You make a very good point; this is a daunting, big challenge. It may not seem it. It sounds simple. Let's have some simple rules of engagement we all adhere to and move on so that Ms. McDermott can get the information she needs. Well, not so fast; not so simple; there are all kinds of intruding laws and regulations; there are 100-plus different practices we have to kind of rein in and look at. But the chairman pointed out the Executive Order, however well intentioned, was four years ago. Here we are four years later and we are at the draft rule stage.

So what was the time line for implementing this and how are we doing in trying to meet those metrics?

Mr. FITZPATRICK. Certainly. The Executive Order laid out a few deadlines for agency consideration and then the deadlines, I will say, stopped. The first year essentially was to define the universe of information that is CUI. So agencies were given six months to make submissions. What are the categories that you feel meet this threshold of having a basis in law, government-wide policy, or regulation, and how would you describe them and how can we put them together in a registry? Agencies produced 2,200 submissions. So if you get an idea of what agencies feel their authority ought to be, and that came from, I will say, not the 150 agencies we deal with now, but some dozens of them submitted 2,200 individual 3x5 cards saying I can control this, I can control this, I can control this.

Mr. CONNOLLY. Can I interject, if I may?

Mr. FITZPATRICK. Yes.

Mr. CONNOLLY. Just an ironic observation, Mr. Chairman. The press may not think this is all that interesting, but clearly Federal officials did, because it affects how they operate.

Mr. FITZPATRICK. Absolutely. And it affects a level of latitude they felt they had to do as they pleased, or wished, or felt was most effective for them.

Mr. CONNOLLY. Right.

Mr. FITZPATRICK. And, instead, this umbrella of constraint was, I will say, beginning to be spread.

So 2,200 submissions, many of them the same types; personnel information, privacy information, budget information. But many of them simply my agency directive says I can do this, so they submitted it. Well, that is below the threshold. That did not make it

into the registry. So the production of the registry, putting the registry out on the rolls.

We then began an inventory of practices to say what do you do with this information today and how do you safeguard it? How do you provide information systems security for it? How does dissemination control work? How far and wide are complex are your agency directives and instructions so we know how much is going to have to be torn down and rebuilt?

We took a shot at, as Patrice mentioned, a draft rule through our interagency council that basically the interagency choked on. We put all of the principles of CUI and sort of in the nature that we have been discussing them today and all of the how-to's of the CUI in the same document. That was, I will just say, ineffective and did not succeed the interagency coordination process. We had to rewrite it so that we could separate the two.

And what is going around the agencies now is this set of principles in the rule which point to practices and authorities that the CUI Council, under the executive agent's coordination, will issue. So you have a draft rule, and the draft supplemental guidance says here is what marking and dissemination mean; here is what the constraints are on agencies; and then over in a separate document here is how to do it.

Mr. CONNOLLY. Thank you.

Mr. Fitzpatrick, my time is up. The chairman has graciously agreed to allow Ms. McDermott to also comment because I don't want to impose on my colleagues, and I see the distinguished chairman is here as well.

Thank you, Mr. Chairman.

Ms. MCDERMOTT. So, yes, we are aware of and support all of the work that they have been doing. We do feel, though, that there has been some, the chairman called it slow-rolling. I might call it, because of its loss of control by the agencies, it is foot dragging, it is throwing some sand. But, again, that is from an entirely outside perspective.

I do want to go back to two points that you made, though. This was about the need to protect information and also to share it. And one of the things that we have been very concerned about all along is that where it is appropriate and where the statute or the regulation allows it, that there be put time limits on these markings so that they don't continue to be used passed when they are authorized to be used. And that is a whole big issue of how you unmark something that has been marked.

The other thing that we are very, very concerned about is that, in terms of the sharing, both sharing and protecting, that these markings, it needs to be clear, they need to be clearly marked, any documents, so that somebody who shares a document with the public, certainly shares it with Congress, shares it with the Judicial Branch, although those are already covered under the Executive Order.

If it is not marked, they cannot be held accountable for inappropriately sharing information. This is like, you know, something that was part of the Intelligence Authorization Act that President Clinton vetoed back toward the end of his thing that said any document that is classifiable, you can be held criminally liable for re-

leasing. Well, no, you can't, because that could be anything. So that is a very big concern of ours, to protect whistleblowers, but also to allow useful sharing throughout the Government of information as it needs to be protected and of information that doesn't need this kind of protection.

Mr. MICA. Thank you.

Let me yield now to the chair of the full committee, Mr. Issa, who has joined us. Mr. Issa.

Mr. ISSA. Thank you, and thank you for being here.

The fact is this is probably the one nearest and dearest to my heart of all the hearings. You might wonder why. Well, the CUI Council, how do I know it is not a CYA council? I am serious, Mr. Fitzpatrick. I am the beneficiary of 20 months of having subpoenaed documents that are unclassified held and not delivered to this committee, even though they were subject to subpoena, because they were unclassified but embarrassing. In those 2,200 different classifications, did you see that classification, unclassified but embarrassing?

Ms. Lontz, is that one that you plan on using?

Ms. LONTZ. No, sir.

Mr. ISSA. You use it every day. Transportation Safety uses it all the time. We subpoena documents and, Ms. McDermott, I know you are on our side, but, quite frankly, when you say it is already covered, no, it isn't. This Administration systematically does not reply honestly and fully with even subpoenas of the various committees. That is just a fact. It is a reality. One of the things that we have seen is that the best way to get evidence, unclassified evidence is we depose somebody, and on the evening before we are going to depose them, we get a ration of documents that are somehow responsive to it.

The fact is this is near and dear to my heart because I don't think you should have a right to any of them. I think the whole idea that there is anything below secret is hogwash. I think the idea that other than personally identifiable information, meaning information is sensitive because it doesn't truly belong to the Government to release, such as your email address, even if it is a Government one, being released to the entire public; your birthday; personal information about your home. We can all agree that that information is not secret, but, by definition, shouldn't be released. Do we agree with that?

Is there really any other area that people get to see without a background check, people get to handle without knowing whether they are pedophiles, whether they are drunks, whether they are going through personal traumas in their lives, etcetera, etcetera? In other words, we have no security on them other than they are a Federal employee or a Federal contractor. They get to see all this information and then, when Congress subpoenas it, we don't even get it. Is there anyone that is going to justify those 2,200 categories here today? I would love to hear it. Ms. Lontz?

I mean, I am thrilled to hear that there are 2,200 requests for unclassified information to be withheld. Of that 2,200, I will take out of it as many as you say include personal identifiable information. Give me another one.

Mr. FITZPATRICK. If I may clarify that number.

Mr. ISSA. Please.

Mr. FITZPATRICK. And understand that you entered midstream. Twenty-two hundred was the number of individual submissions that came in from agencies where they thought they had some authority.

Mr. ISSA. A lot of redundancy.

Mr. FITZPATRICK. There is a lot of redundancy and a lot of it did not meet the threshold established in the Executive Order that authority can only be established if it has been granted by law through the Federal regulations or through government-wide policy. Those numbers, there are 2,200 high level categories, 85 subcategories based on 314 individual citations of either law, regulation, or policy.

So while I do not dispute the characterization of agencies' desire to withhold information to their advantage, what is authorized under the CUI program is only information in these categories, these narrow 2,200 and 85 subcategories, can be safeguarded or dissemination control. Their disclosure through other processes, or the eventual decontrol, are matters of discretion.

Mr. ISSA. We fully understand that, but understand that the President signed the Data Act just a few days ago. That Act intends on making across Government the vast majority of information that exists in our databases searchable, addressable, downloadable, which would include a system in which, because of the strength of the metadata, you would be able to exclude personally identifiable information.

But essentially, and we are not talking about emails for a moment; we will leave those aside, the intent of it would be to open up all of Government, to make you able to say that a particular data point is not to be released, such as personally identifiable information, locations or times, certain things like that, predictive information about events that have not yet occurred.

If we are going to open that up, we can't have these levels of classification because it will essentially close systematically all these databases, won't it?

Ms. McDermott, you really don't care about hunks of paper being delivered anymore; you really care about the data wealth being mined in order to get real information, don't you? Isn't that really the modern America?

Ms. MCDERMOTT. That is part of modern America. But we actually are still very concerned about the paper getting delivered to nonprofit organizations that make it available to journalists, to that sort of thing.

Mr. ISSA. Let me explain one thing to you that I have learned the hard way in five years in the, if you will, leadership of this committee. Until today, if I subpoena the EPA for emails, they send out to the people they think may have responsive information asking them to voluntarily look through and see if they have something that we would be interested in, and then they get to submit it.

That is a systematic system of exclusion of at least unclassified but embarrassing information. Only through direct access are you ever going to get what you want versus getting the paper they want to give you and then searching through it saying, if this ex-

ists, where is this other piece, and then having to—how many times do you reapply again and again because a tranche of information tells you that they are not giving you it all?

Ms. MCDERMOTT. I would love, if I may, respond just on the email part of it.

Mr. ISSA. Please.

Ms. MCDERMOTT. Regrettably, that experience about asking people to search their hard drives is because until very recently, because of regulations that were promulgated by NARA back in the 1990s, agencies were not required to organize their email. They were not required to treat it as records of offices; they could treat it all the same. And what has happened over time is that it is on people's hard drives; it has not been centrally collected.

It is unfortunately true that that agencies don't know how much email they have that is responsive. And it is not just Congress that gets this response; it is our colleagues in the nonprofit world who ask agencies for responsive email and they say we will look, but it is going to take a long time.

Mr. ISSA. Yes, we were told by the IRS commissioner just the other day that it could take two years to respond to our questions, far longer than the IRS gives you in an audit to respond to theirs.

Let me just close quickly with a question. If we are going to have classifications below secret, and this committee, among its jurisdictions, controls basically the question of people holding clearances, how many categories of cleared people are we going to have to decide what level of background investigation, what level of denial?

If somebody is going to look at unclassified information that has some pseudo-classification level that keeps the public from seeing it, do I need to know whether they are currently on probation, whether they have DUIs, whether or not they are convicted pedophiles? And if so, how do I come up with all those classifications? How many will I need, Mr. Fitzpatrick? Cleared information, cleared people, right?

Mr. FITZPATRICK. It actually requires no specific personal security vetting for access to controlled unclassification information.

Mr. ISSA. So, in summation, what you are telling me is below secret we can deny the public, through a maze of different processes, access to information, while allowing people who happen to work for the Government, either as contractors or as Federal employees, to have unfettered access, even if they have things which would make us question that access, right?

Mr. FITZPATRICK. Well, no. The standard is only for that information which requires a safeguard or dissemination control and is accompanied by a lawful Government purpose, regardless of your status, in Government or outside of Government.

Mr. ISSA. So tax cheats at the IRS get access to my tax information, while even if I have been persecuted directly by the IRS, I can't get that. I understand what you are saying. I question in this hearing whether or not you are going down a road of any sensibility.

If you can't tell me who should be excluded within Government from seeing information, if you can't tell me what level we should put as a requirement for people to be cleared for that information below secret, because we have rules for secret and top secret, then

I question whether or not you can create any category other than personal identifiable information is on a need to know basis, and other than personal identifiable information I question whether or not you really can do the process that you are asking.

And I think Mr. Connolly said it very well during his 10 minutes, which I have equaled nearly. The fact is we have waited too long, and it has been four years since an Executive Order, and this committee has a responsibility to ultimately say you are not getting it done; we may need to preempt you. And rulemaking is not lawmaking, it just looks like it.

Mr. Chairman, rulemaking is not lawmaking; it just looks like it. I am going to close on that. Thank you.

Mr. MICA. Thank you. I liked your CYA versus CUI description. Very appropriate sometimes.

Waiting most patiently, one of our outstanding junior members, Mr. Meadows. You are recognized.

Mr. MEADOWS. The chairman here says I have a lot of gray hair for a junior member, but thank you for your testimony.

Mr. Fitzpatrick, let me pick up, because as we start to hear 2,200, we start to hear regulations. Everybody is going to want to have a piece of that turf. And I guess my concern is if we are going about this new classification, how many rules and regulations are we going to eliminate? I mean, out of the 170, I think your testimony, how many of those rules and regulations? Are we going to be able to eliminate half of those?

Mr. FITZPATRICK. So we will go to a single marking system. So in the 117, the list of labels that were previously used, they varied across whether it said sensitive protect, restrict; all sorts of unauthorized types of markings. We propose a marking system that simply says controlled.

Mr. MEADOWS. Based on what criteria?

Mr. FITZPATRICK. Based on its presence in the registry, which means there is either a law that says the secretary is authorized to protect that or there is a Federal regulation that says this information may be controlled.

Mr. MEADOWS. But according to your testimony, you said it should be based on statutory exemptions in FOIA or other applicable laws, policies, and regulations. Now, the concern I have with policies is any agency can make up any policy, and it undermines the whole effort of what you are trying to do.

Mr. FITZPATRICK. So that portion of my testimony, and I acknowledge that those words are there, applies to instruction to agencies not to confuse, not to utilize the fact that something is marked CUI as somehow disposing a decision to withhold information under FOIA. The Executive Order and our guidance say clearly FOIA and other applicable laws that govern disclosure are what will govern your decision. Simply because it is marked controlled SSI doesn't then predispose, okay, then I can withhold it under FOIA. Our instructions and the Executive Order say it might be marked CUI so that you know it needs to be in a desk draw, it needs to have a cover sheet, it needs to be given to someone with a lawful government purpose. But if a FOIA request comes in on that, then the FOIA rules apply.

Mr. MEADOWS. All right, so on a scale of 1 to 10, with 10 being the most confident, how confident are you that what you are about to put in place will get rid of the politics, the CYA, the political aspect of trying to keep documents from Congress and from the American people? Scale of 1 to 10, how confident?

Mr. FITZPATRICK. The CUI program, I am going to say, sits next to, but not a part of, the disclosure regime. So however confident, however much or little confidence you have in that disclosure regime——

Mr. MEADOWS. Well, it hasn't been working too well so far, so, going forward, how confident are you?

Mr. FITZPATRICK. So I am confident you will have the basis to explain, and those seeking information will have the basis to contest, the presence or absence of authorized by law or regulation, an authorized withholding basis or not. So an example——

Mr. MEADOWS. That is a great answer to a question I didn't ask, but from politics, and getting politics and complete transparency, on a scale of 1 to 10, how confident are you?

Mr. FITZPATRICK. I am an optimist. I will give you a 6.5.

Mr. MEADOWS. Okay.

Mr. FITZPATRICK. It will be better. It won't be everything.

Mr. MEADOWS. All right.

So, Ms. Lontz, let me go to you, because you talked about training earlier. On the training aspect of it, you mentioned that they have been given this handbook that talks about seventy some odd pages that is very specific. How confident are you that we are covering all the issues in terms of the thoroughness of the training and that the new model is going to be followed?

Ms. LONTZ. So in TSA, I can say that I am very confident that the new measures we have put in place have significantly improved the way we handle SSI. It is much more consistent; there is a memorialization of any and all SSI reviews that are done. It is comprehensive in the training; we can customize it, as I explained earlier, depending on various programs so they get a more in-depth understanding of what SSI is and is not. So I am very confident that the new measures——

Mr. MEADOWS. So how are you reinforcing that? I mean, going forward, because if it is in a handbook, I don't know about everybody here, but most of the handbooks I have gotten over my 54 years, I haven't read them, or at least I haven't read all of them. And we may have somebody here that does that, and I know my good friend and colleague from Virginia is astonished at that revelation.

Mr. CONNOLLY. I have read every handbook ever.

Mr. MEADOWS. No doubt. No doubt.

So how do we reinforce it? Do you make it part of their evaluation? If they get a bonus, is it part of that in terms of saying that you have been following this? How do we reinforce it? I see one of your staffers shaking his head yes behind you.

Ms. LONTZ. I think our senior leadership does a very good job of ensuring that SSI, the importance of SSI, the job that the TSA does impacts aviation and transportation security. We do have to be very concerned with protecting SSI information. We also ensure that it is not just a once a year, there is an online training course

you need to take. We have SSI Awareness Week at TSA where there are a sundry activities and things that remind our personnel of the importance of SSI. So it isn't just a handbook that goes on the shelf and we say, hey, we have this. We really do impress upon our personnel the importance.

Mr. MEADOWS. Well, I am going to close with this encouragement in terms of any help that you might be able to give this committee. Ultimately we have two objectives. One is to get the politics out of it, to speed up the process and become transparent with the American people. And if you see areas that need to be addressed, it is incumbent upon you to get that to this committee, because in a bipartisan way we will work to not only put forth legislation to clear it up, but to make sure that the American people get it, because right now the request even from a member of Congress gets thwarted at so many different levels based on so many different regulations, policies, and I don't knows that it is unacceptable. So we look forward to your recommendations.

I yield back, Mr. Chairman. Thank you.

Mr. MICA. Well, thank you, Mr. Meadows. Thank you, Ranking Member Connolly.

And I want to thank our three witnesses, Ms. Lontz, Mr. Fitzpatrick, and Ms. McDermott, for your testimony. We have additional questions and we will probably be submitting some to the witnesses today.

Mr. Connolly moves that we keep the record open for seven additional days. Without objection, so ordered.

Again I thank you. We have raised some very interesting points, trying to work together to improve this process and the question of classification and various categories, making certain that Government information is made available both to the public and the Congress in a responsible fashion. Some enlightening information. It looks like we still have a ways to go and keeping this moving forward in a positive fashion as intended.

There being no further business today before the Government Operations Subcommittee, the hearing is adjourned. Thank you.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

PSEUDO-CLASSIFICATION OF EXECUTIVE BRANCH DOCUMENTS: PROBLEMS WITH THE TRANSPORTATION SECURITY ADMINISTRATION'S USE OF THE SENSITIVE SECURITY INFORMATION (SSI) DESIGNATION

JOINT STAFF REPORT
PREPARED FOR CHAIRMAN DARRELL E. ISSA &
RANKING MEMBER ELIJAH E. CUMMINGS
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
MAY 29, 2014

Contents

I. Executive Summary 3
II. Findings 5
III. Recommendations 5
IV. Brief History of Sensitive Security Information (SSI) 6
V. Origin of Investigation 11
VI. Inappropriate Use of the SSI Designation to Prevent FOIA Releases 12
VII. The Release of Information against the Advice of the SSI Office 16
A. SSI Related to Federal Air Marshals 16
B. SSI Related to Whole Body Imagers 19
VIII. Inter-Office Rift Causes Inconsistent Application of the SSI Regulations 22
IX. SSI Office Structure and Position within TSA 27
X. TSA's Efforts to Address the Problems 28
XI. Conclusion 29

I. Executive Summary

Under the Air Transportation Security Act of 1974, the Federal Aviation Administration (FAA) created a category of sensitive but unclassified information, frequently referred to as "Sensitive Security Information" (SSI), and issued regulations that prohibit the disclosure of any information that would be detrimental to transportation security.[1] These regulations restrict disclosure of SSI, exempting information properly marked as SSI from release under the Freedom of Information Act.[2]

After the 1988 bombing of a commercial airliner that crashed in Lockerbie, Scotland, the FAA made significant changes in aviation security, expanding the definition of SSI to include any information the FAA Administrator determined may reveal systemic vulnerabilities within the aviation system, or vulnerabilities of aviation facilities to attacks.[3] Other definitional expansions included details of inspections and investigations, as well as alleged violations and certain agency findings. The SSI regulation was later expanded in order to limit access to protected information to those persons who have a "need-to-know."[4]

While the SSI designation can protect sensitive information, it is also vulnerable to misuse. Bipartisan concerns about the use of the SSI designation by the Transportation Safety Administration (TSA), an agency of the Department of Homeland Security (DHS), have existed since the promulgation of the SSI regulations in 2004.[5] Through its investigation, the Committee obtained witness testimony and documents that show possible misuse of the SSI designation by TSA. Witnesses detailed instances in which TSA barred the release of SSI documents against the advice of TSA's SSI Office. TSA also released SSI documents against the advice of career staff in the SSI Office. The Committee's investigation revealed that coordination challenges exist among the TSA Administrator, TSA's Office of Public Affairs (OPA), and TSA's SSI Office.

Witnesses testified that many of the problems related to the SSI designation process emanate from the structure of the SSI regulation itself. TSA's SSI Office is staffed with career employees tasked with assisting in the SSI designation process. The final authority on SSI designation, however, rests with the TSA Administrator. Pursuant to the regulation, the TSA Administrator must provide certain documentation supporting his SSI designations. Yet, witnesses interviewed by the Committee stated that there were multiple incidents in which the SSI Office was not consulted or where TSA took actions against the advice of SSI Office officials. Further, such actions occurred without the TSA Administrator providing required written documentation supporting the action.

---

[1] Pub. L. 93-366, 88 Stat. 409 (Aug. 5, 1974); *see also* Transp. Safety Admin. (TSA), Statute & Reg. History: Sensitive Security Information (SSI), *available at* http://www.tsa.gov/stakeholders/statute-and-regulation-history (last visited May 1, 2014) [hereinafter TSA History].

[2] 49 C.F.R. § 1520.5; *see also* U.S. Dep't of Homeland Security (DHS), Management Directive No. 11056.1, SSI (Nov. 3, 2006), https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110561_sensitive_security_information.pdf.

[3] 14 C.F.R. § 191.7.

[4] 14 C.F.R. § 107.

[5] *See* 49 C.F.R. § 1520. TSA and the Department of Transportation issued an interim final rule clarify preexisting SSI provisions on May 18, 2004.

Due to this contentious relationship and the failure to follow proper procedures, the SSI Office struggled to carry out its statutory obligations effectively. While the TSA Administrator has the final authority to determine whether information is SSI, he is also required under the regulations to submit written explanations of his decisions to the SSI Office in a timely fashion. Unfortunately, the repeated failure to submit written determinations before taking actions on SSI caused a rift between senior TSA leadership and the SSI Office. This rift resulted in inconsistencies, which could be detrimental to the process for protecting sensitive information.

This report explores issues related to the current TSA SSI designation process and recommends improvements to ensure that sensitive information is properly protected while non-sensitive information is properly released to the public. TSA's use of SSI reveals a broader problem of pseudo-classification of information in federal departments and agencies. Limits on such labeling of information are needed to provide greater transparency and accountability to the public while promoting information security.

II. Findings

- Problems with TSA's application of the SSI designation date back to 2004, including inconsistent application of the designation.
- TSA improperly designated certain information as SSI in order to avoid its public release.
- TSA repeatedly released information to the public against the advice of the SSI office and without having produced suitable documentation to explain the decision.
- The structure and position of the SSI office within TSA has contributed to the difficulties the office has encountered in carrying out its mission. TSA has moved the office within the agency's organizational structure several times. One official stated the office moves have effectively relegated it a "throwaway office."
- TSA made significant improvements to its SSI designation process following the Committee's investigation.

III. Recommendations

- The TSA Administrator should provide documentation and an explanation for his or her decision to override a previous SSI determination in writing to the SSI office *before* the release is made in order to provide the SSI office with an explanation of the Administrator's justification and promote consistent treatment of future SSI designations.
- The Department should undertake an evaluation of the SSI Office's position within TSA's organizational structure, to ensure that the office has the support it requires to carry out its mission.
- Executive Branch departments and agencies must curtail the widespread use of pseudo-classification of information, which hinders transparency. Agencies must track and report the use of such labels on information to ensure consistency and limits on their use.

IV. Brief History of Sensitive Security Information (SSI)

A. Distinctions between Classified/Unclassified Information and SSI

The President sets the federal government's classification standards by executive order.[6] All information held by the government falls into two categories: (1) classified information, which includes the "Top Secret," "Secret," and "confidential" designations, and (2) unclassified information.[7]

Unclassified information falls into two categories: Sensitive but Unclassified (SBU), a broad category that includes information protected by federal regulation such as SSI and information protected by agency or government policy such as For Official Use Only (FOUO); and Public Information, which includes all other information not contained in the SBU category.[8]

Generally, classified information is information of which "unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security."[9] Such information must be owned by, produced by, or under the control of the federal government, and must concern one of the following:

1) Military plans, weapons systems, or operations;
2) Foreign government information;
3) Intelligence activities, intelligence sources/methods, cryptology;
4) Foreign relations or foreign activities of the United States, including confidential sources;
5) Scientific, technological, or economic matters relating to national security;
6) Federal programs for safeguarding nuclear materials or facilities;
7) Vulnerabilities or capabilities of national security systems; or
8) Weapons of mass destruction.[10]

Classified information is classified as "Top Secret" if its unauthorized disclosure could reasonably be expected to cause "exceptionally grave damage" to national security.[11] The standard for "Secret" information is downgraded to include information which if released would do "serious damage" to national security, and "Confidential" information is defined as information which if released would pose "damage" to national security.[12] The Counterintelligence and Security Enhancement Act of 1994 established procedures governing the

---

[6] JENNIFER K. ELSEA, CONG. RESEARCH SERV., RS 21900, THE PROTECTION OF CLASSIFIED INFORMATION: THE LEGAL FRAMEWORK (2013).
[7] DHS, Transportation Security Administration (TSA) Sensitive Security Information (SSI) Program: SSI Training for Air Cargo Stakeholders, http://www.tsa.gov/sites/default/files/assets/pdf/ssi/ssi_training_air_cargo.pdf (last visited May 1, 2014).
[8] *Id.*
[9] Executive Order 13526, Classified National Security Information, at § 1.2 (Dec. 29, 2009), http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information.
[10] *Id.* § 1.4
[11] *Id.* § 1.2
[12] *Id.*

access to classified material so that no person can gain such access without having undergone a background check.[13] Only personnel with the proper security clearances are permitted access to classified information.

Criminal and civil penalties apply to unauthorized disclosure of classified information, the severity of which depends on the type of information and the manner of disclosure. Federal law allows for a prison sentence of no more than one year and/or a $1,000 fine for officers and employees of the federal government who knowingly remove classified material without the authority to do so and with the intention of keeping that material at an unauthorized location.[14] Further, fines of up to $10,000 and imprisonment for up to 10 years can be imposed on a federal employee who transmits classified information to anyone who the employee has reason to believe is an agent of a foreign government.[15]

A fine and a 10-year prison term may be imposed on anyone, government employee or not, who publishes, makes available to an unauthorized person, or otherwise uses to the United States' detriment classified information regarding codes, cryptography, and communication intelligence used by the United States or a foreign government.[16] Lastly, the disclosure of confidential information identifying a covert agent, when done intentionally by a person with authorized access to such information, is punishable by imprisonment for up to 15 years.[17] In addition, an agency may employ administrative measures to deter unauthorized disclosures by government personnel.[18] Such measures may include the ability to impose disciplinary action or revoke a person's security clearance.[19]

SSI is not classified national security information and therefore not afforded the same protections as classified information. SSI is defined in the Homeland Security Act of 2002 as information obtained or developed during security activities, "if the Under Secretary decides that disclosing the information would (A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information, or (C) be detrimental to the security of transportation."[20] In order for information to be SSI, it must be related to transportation security, and it must fall under one of the 16 categories of SSI as defined in the SSI regulation.[21]

Although SSI is not subject to the handling requirements governing classified national security information, it is subject to the handling procedures required by TSA's SSI regulation.[22] Restrictions on access to SSI and penalties for unauthorized disclosure of SSI are much less

---

[13] Counterintelligence and Security Enhancement Act of 1994, Title VII of P.L. 103-359 (codified at 50 U.S.C. § 435 *et seq.*).
[14] ELSEA, *supra* note 6.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] PUB. L. 107-296.
[21] 49 C.F.R. § 1520.5(b).
[22] *Id.* § 1520.

severe.[23] A security clearance is not required to gain access to SSI, and criminal penalties may not be imposed in the event of unauthorized disclosure of SSI.[24] Unauthorized disclosure of SSI may, however, result in civil penalties and/or other enforcement or corrective actions.[25]

B. The Origins of SSI

FINDING:	Problems with TSA's application of the SSI designation date back to 2004, including inconsistent application of the designation.

The concept behind the SSI designation dates back to the early 1970s.[26] A 1970 terrorist hijacking that resulted in the explosions of four airliners "convinced the White House that stronger [security] steps were needed," including installing federal air marshals and screening passengers and their carry-on luggage.[27] Although the air marshal and screening programs provided additional security, continued airliner attacks demonstrated the need for further security directives to prevent the exploitation of airline vulnerabilities.[28]

On January 4, 1973, after authorities discovered bombs on three airplanes, among other security breaches,[29] Senator Howard W. Cannon of Nevada, then-Chairman of the Subcommittee on Aviation of the Senate Commerce Committee, introduced legislation which eventually became the Air Transportation Security Act of 1974 (ATSA).[30] ATSA authorized the FAA to issue regulations that, notwithstanding the Freedom of Information Act, prohibited the disclosure of any information, if such disclosure "would be detrimental to the safety of persons traveling in air transportation."[31]

Pursuant to the authority granted by ATSA, the FAA promulgated regulations that created a "category of sensitive but unclassified information known as Sensitive Security Information (SSI)."[32] Originally, SSI included, but was not limited to: hijacker profiles, baggage screening protocols, airport or air carrier security programs, explosive detection devices, security plans, security communications equipment and procedures, and any threats of sabotage, terrorism and air piracy.[33]

In 1988, nearly 15 years after ATSA's passage, the bombing of Pan Am Flight 103 over Lockerbie, Scotland prompted significant reform in aviation security. In 1989, the President's Commission on Aviation Security and Terrorism recommended improvements to the FAA

---

[23] *Id.* § 1520.17.
[24] *Id.*
[25] *Id.*
[26] TSA History, *supra* note 1.
[27] Judy Rumerman, *Aviation Security*, U.S. Centennial of Flight Comm'n, ¶ 7, (2004), https://www.hsdl.org/?view&did=447844 (last accessed May 1, 2014).
[28] *Id.*
[29] *Id.*
[30] Pub. L. 93-366, 88 Stat. 415 (Aug. 5, 1974).
[31] H.R. Rep. No. 93-1194, at 9 (1974).
[32] TSA History, *supra* note 1.
[33] Withholding Security Information from Disclosure under the Air Transportation Security Act of 1974, 41 Fed. Reg. 26579 (June 28, 1976).

security bulletin process.[34] As a result, Security Directives and Information Circulars were created, and in 1997, those products became SSI-protected.[35]

In 1997, the FAA published its final SSI rule, which strengthened the existing regulations.[36] The rule states:

> Much of the effectiveness of the programs **depends on strictly limiting access to such information to those persons who have a need-to-know**. Unauthorized disclosure of the specific provisions of the air carrier and airport security programs or other aviation security information would allow potential attackers of civil aviation to devise methods to circumvent or otherwise defeat the security provisions. It would also discount the deterrent effect inherently providing in prohibiting disclosure of security measures that may or may not be in place.
>
> There are sophisticated criminal elements who actively seek information on what seemingly are minor security points, with a view to accumulating a larger picture of the entire security program. Therefore, it is imperative that the entire security program be protected.[37]

Modifications to the regulations also expanded SSI coverage to include, among other things, "[a]ny information that the [FAA] Administrator has determined may reveal a systemic vulnerability of the aviation system, or a vulnerability of aviation facilities to attack," including but not limited to "details of inspections, investigations, and alleged violations and findings of violations . . . ."[38]

Tragically, the September 11, 2001 terrorist attacks drastically altered the landscape concerning the definition of classified and unclassified information. Just two months after the attacks, Congress passed a law that established TSA and delegated it the authority to designate information as SSI.[39] TSA regulations implementing the law included new information categories.[40]

Even before TSA issued its final rules, controversies erupted over whether the rules went too far. For example, a Congressional Research Service (CRS) report noted that the SSI regulations "raised a number of concerns," including whether they were being applied to withhold information."[41] Before TSA issued its final rules, the *Washington Post* reported that, TSA was "muzzling debate by labeling too many of the agency's policies and reports as too sensitive for public dissemination, according to pilots, flight attendants and consumer

---

[34] TSA History, *supra* note 32.
[35] *Id.*
[36] *Id.*
[37] 14 C.F.R. § 107 (1997).
[38] 14 C.F.R. § 191.7 (1997).
[39] *See* Aviation & Transp. Security Act of 2001, 49 U.S.C. § 40101 (2001); TSA History, *supra* note 1.
[40] *See* 49 C.F.R. § 1520 (2002).
[41] MITCHEL A. SOLLENBERGER, CONG. RES. SERV., SENSITIVE SECURITY INFO. (SSI) & TRANSP. SECURITY: BACKGROUND & CONTROVERSIES, at 3 (2004).

advocates."[42] Notwithstanding the tumult, TSA issued its final SSI rules on May 18, 2004, expanding covered information to include all lists of critical infrastructure developed by state and local governments "because their release to the public would increase the risk of attack on critical transportation assets."[43]

In September 2004, two House Appropriations Committee Members asked the Government Accountability Office (GAO) to review how TSA used its SSI authority to withhold transportation security information from the public.[44] In making their request, Representatives David Obey (D-Wis.) and Martin Olav Sabo (D-Minn.) stated that TSA provided written responses to questions that were designated SSI, "but did not treat the same information as sensitive a month earlier."[45] They also noted that TSA claimed information relating to electronic baggage screening was SSI, despite the same information having "already been reported in the public domain."[46]

In 2005, as a result of its review, GAO found TSA had promulgated no guidance or procedures "for determining what constitutes SSI or who can make the designation," no policies on accounting for or tracking SSI documents, and no systematic reviews for determining if and when an SSI designation should be removed.[47] GAO also found TSA "lack[ed] adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA."[48]

GAO noted that TSA's Internal Security Policy Board recognized that handling and identifying SSI had become problematic.[49] A memo from the Board stated that, "[i]dentification of SSI has often appeared to be ad-hoc, marked by confusion and disagreement depending upon the viewpoint, experience, and training of the [particular TSA employee]."[50] As a result of the complaints concerning TSA's handling of SSI, the Department of Homeland Security Appropriations Act of 2006 required DHS to include timely reviews of SSI requests, and that all information designated SSI, more than three years old, be released upon request, unless the DHS Secretary makes a written determination that the information must remain SSI.[51]

---

[42] Sara Kehaulani Goo, *TSA Faulted for Restricting Information*, WASH. POST, Oct. 10, 2003, at A11.
[43] 49 C.F.R. § 1520, at 28072.
[44] Christ Strohm, *Lawmakers Question Policy on Transp. Security Info.*, GOV'T EXEC., Sept. 15, 2004, http://www.govexec.com/federal-news/2004/09/lawmakers-question-policy-on-transportation-security-information/17599/.
[45] *Id.*
[46] *Id.*
[47] GAO, *TSA: Clear Policies & Oversight Needed for Designation of Sensitive Security Info.*, GAO-05-677 (2005).
[48] *Id.*
[49] *Id.*
[50] *Id.* at 5.
[51] TSA History, *supra* note 32; DHS Approps. Act of 2006, P.L. 109-295, § 525(a)(1)(A), 120 Stat. 1355, 1381-1382 (2006).

V. Origin of Investigation

The Committee's investigation into how DHS identifies and protects SSI began in July 2011. On July 13, 2011, the Subcommittee on National Security, Homeland Defense, and Foreign Operations held a hearing on airport perimeter security.[52] In preparation for this hearing, Subcommittee Chairman Jason Chaffetz requested information relating to airport incidents involving security breaches. In response, DHS provided a PowerPoint presentation entitled "Information Requested by Chairman Chaffetz," outlining such security breaches.[53] Chairman Chaffetz disclosed portions of this presentation publicly both before and during the hearing.

Following the hearing, DHS Deputy General Counsel Joseph Maher sent Chairman Chaffetz a letter accusing him of unlawfully releasing this non-classified information, because it was designated SSI.[54] Maher stated that "[u]nder applicable regulations, SSI may be disclosed only to covered persons as defined in 49 C.F.R. § 1520.7 who have a 'need to know.'"[55] In response, Chairman Issa wrote to then-Homeland Security Secretary Janet Napolitano, explaining that Congress is not covered by the regulation governing SSI protection.[56] Members of Congress are constitutionally protected if they disclose either SSI or classified information.[57] Additionally, 40 C.F.R. § 1520.15(c) specifically entitles Congress to access to SSI documents.[58] Based on the plain language of the regulation and relevant case law, Chairman Issa concluded that the Department's position was without merit.[59]

Further, consistent with Title 49 of the U.S. Code, documents designated SSI for the purpose of "conceal[ing] a violation of law, inefficiency, or administrative error" or "prevent[ing] embarrassment" are deemed improperly designated.[60] Former SSI Office Director Andrew Colsky, an SSI expert, reviewed the PowerPoint presentation in question and concluded

---

[52] *TSA Oversight Part 2: Airport Perimeter Security: Hearing before the H. Comm. on Oversight & Gov't Reform, Subcomm. on Nat'l Security, Homeland Defense, & Foreign Ops.* 112th Cong. (July 13, 2011).

[53] Inspection & Enforcement Analysis, Info. Requested by Chairman Chaffetz: *U.S. Airport Security Breach & Access Control Incidents November 19, 2001-April 30, 2011*, TSA Office of Security Ops. Compliance Programs (May 12, 2011).

[54] Letter from Joseph B. Maher, Dep. Gen. Counsel, DHS, to Rep. Jason Chaffetz, Chairman, Subcomm. on Nat. Security, Homeland Defense, & Foreign Ops. (July 13, 2011).

[55] *Id.*

[56] Letter from Rep. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform, to Hon. Janet Napolitano, Sec'y, DHS (July 22, 2011); 49 C.F.R. § 1520.

[57] Gravel v. United States, 408 U.S. 606, 628-29 (1972).

[58] 49 C.F.R. § 1520.15(c) (2012) ("*Disclosures to committees of Congress and the General Accounting Office.* Nothing in this part precludes TSA or the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.").

[59] For clear guidance on this issue, see Frederick M. Kaiser et al., CONG. RES. SERVICE, *Cong. Oversight Manual*, No. RL30240, at 66 (2011) ("[T]he SSI regulations also appear to insulate congressional committees and their staffs from any sanctions or penalty from the receipt and disclosure of SSI. Specifically, the SSI regulations contain a provision defining those persons who are 'covered persons' and, thus, subject to the regulations. A close reading of the definition of 'covered person' indicates that it does not include members of Congress, committees, or congressional staff.").[60] 49 U.S.C. § 40119(b).

[60] 49 U.S.C. § 40119(b).

it may have been improperly designated SSI because it was (1) not sufficiently marked, and (2) comprised of cumulative figures of no value to our enemies and other publicly-available information.[61] Colsky's expert opinion raised questions about TSA's use of the SSI designation.

The dialogue between the Committee and DHS about TSA's application of the SSI designation captured the attention of former SSI Office Director Colsky, who expressed his concerns about DHS's management of the SSI program. Further, as part of its investigation, the Committee conducted a series of transcribed interviews with current and former staff of the TSA office that manages SSI designations.

Witness testimony and documents obtained by the Committee showed significant problems with TSA's application of the SSI designation. Specifically, TSA officials were inconsistent in the application of the designation—sometimes choosing to release information the SSI Office determined to be sensitive security information while in other instances refusing to release potentially embarrassing information the SSI Office did not consider to merit the SSI designation.

VI. Inappropriate Use of the SSI Designation to Prevent FOIA Releases

FINDING: TSA improperly designated certain information as SSI in order to avoid its public release.

Witnesses interviewed by the Committee testified about instances in which TSA inappropriately withheld documents from FOIA requesters because it was deemed SSI. Former SSI Office Director Andrew Colsky testified that TSA used the SSI designation to prevent the release of documents to FOIA requesters related to Whole Body Imagers (WBIs). He stated:

> There's certain public interest groups out there that do a lot of FOIA requests over these types of things, and one of them did a FOIA request about information related to those scanners, I guess, and their ability to store images or not store images or whatever. And now this is being—you know, coming secondhand, but from a significant number of highly reliable sources, and -- I don't want to say anything to get anybody in trouble -- and things that I personally overheard where there was information in the responsive documents that was not by any stretch of the imagination at all SSI, but was either embarrassing or was something that they just didn't want the other side to know. And there was **extreme pressure** from again I'll use the term 'front office' to mark it as SSI.[62]

Colsky also discussed other ways that TSA may be withholding information from disclosure under FOIA. He stated:

[61] Transcribed Interview of Andrew Colsky, at 110-111 (Nov. 9, 2011) (emphasis added) [hereinafter Colsky Tr.]
[62] Colsky Tr. at 56.

> [C]urrently I sit in the Freedom of Information Act office. And one of the first things I was told when I got there from both attorneys and FOIA processors was, oh, yeah, don't worry about it, because **if you come across embarrassing information or whatever, [the Chief Counsel] will just hide it and come up with an exemption**; because if you cover it with a FOIA exemption, it's so hard for the other person to challenge it, and it will be costly and difficult for them to challenge it, and they're probably never going to see it anyway, so you just get away with it. That's the way it's done.[63]

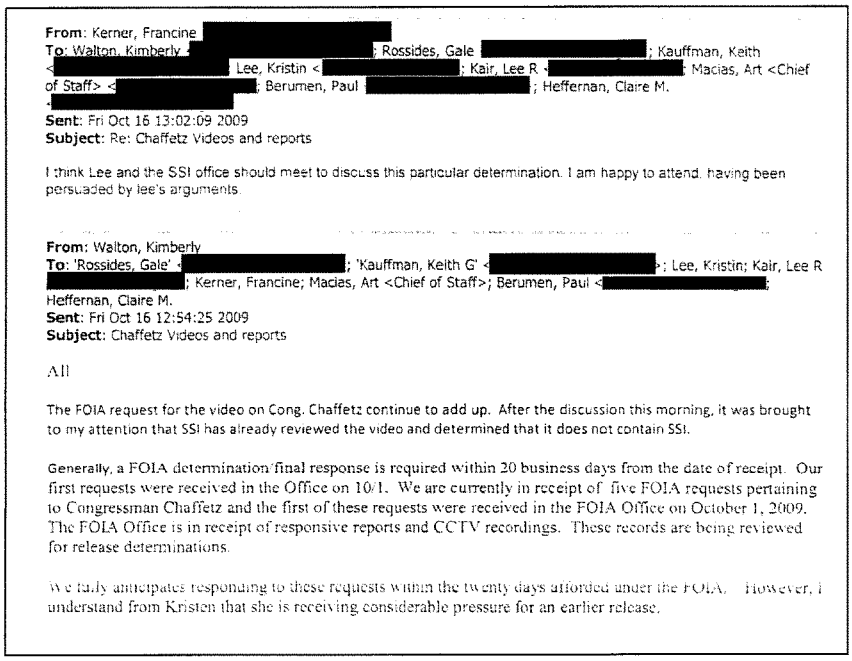
Pursuant to a FOIA request, the SSI Office was asked to review a video documenting Chairman Chaffetz passing through a TSA screening checkpoint. Multiple news outlets made requests for the video under FOIA. Colsky stated the SSI Office determined the video did not contain any SSI, but other TSA officials intervened to censor the part of the video showing Chairman Chaffetz receiving a "pat down." Colsky stated:

> A. Congressman Chaffetz had gone through the screening at—I forget which airport it was . . . But I remember that the video of that screening or that incident had been requested by multiple news sources. And so, again, in good old TSA fashion, I see this commotion down in Office of Public Affairs, because my office at the time was right next to them, and, you know, all this scuffling. You've got general counsel there, you've got all these members of Public Affairs and some people from the front office, I guess. I can't remember who. There was a whole group of people that are all looking at this video. At first we had been asked to review the video for SSI. We reviewed it, and we said there's no SSI in it based on all the guidance that we had at the time. And video was something that we spent a lot of time defining.
>
> But then I believe it was Lee Kair decided that he had concerns about the video being shown. And I don't know—I was not privy to the conversations, so I don't know what the concerns were or whatever.
>
> Q. Who is Lee?
>
> A. Lee Kair was the Assistant Administrator over the Office of Security Operations. Those are the people that deal with the airport security stuff.
>
> Q. Okay.
>
> A. And so someone, I don't know who, I'm going to assume [General Counsel] Francine Kerner and Gale Rossides, I believe, made the

[63] *Id.* at 64.

> decision that they wanted to block out information as SSI, and they proceeded to, you know, put like the fuzzy image over certain parts of the image. And I was left out of the process. I happened to come over, so I was sort of brought into the discussion. And there's several instances like that.[64]

After the SSI Office determined there was no SSI in the video, Assistant Administrator Lee Kair disagreed with the SSI Office's decision, and TSA General Counsel Francine Kerner intervened to revisit it. By e-mail, TSA Special Counselor Kimberly Walton alerted Kair and Kerner to the fact that TSA had received several FOIA requests for the video, and that the SSI Office had determined the video did not contain SSI.[65] Kerner wrote: "I think Lee and the SSI office should meet to discuss this particular determination. I am happy to attend having been persuaded by lee's [sic] arguments."[66]



From: Kerner, Francine [redacted]
To: Walton, Kimberly [redacted]; Rossides, Gale [redacted]; Kauffman, Keith [redacted]; Lee, Kristin [redacted]; Kair, Lee R [redacted]; Macias, Art <Chief of Staff> [redacted]; Berumen, Paul [redacted]; Heffernan, Claire M. [redacted]
Sent: Fri Oct 16 13:02:09 2009
Subject: Re: Chaffetz Videos and reports

I think Lee and the SSI office should meet to discuss this particular determination. I am happy to attend. having been persuaded by lee's arguments.

From: Walton, Kimberly
To: 'Rossides, Gale' [redacted]; 'Kauffman, Keith G' [redacted]; Lee, Kristin; Kair, Lee R [redacted]; Kerner, Francine; Macias, Art <Chief of Staff>; Berumen, Paul [redacted]; Heffernan, Claire M.
Sent: Fri Oct 16 12:54:25 2009
Subject: Chaffetz Videos and reports

All

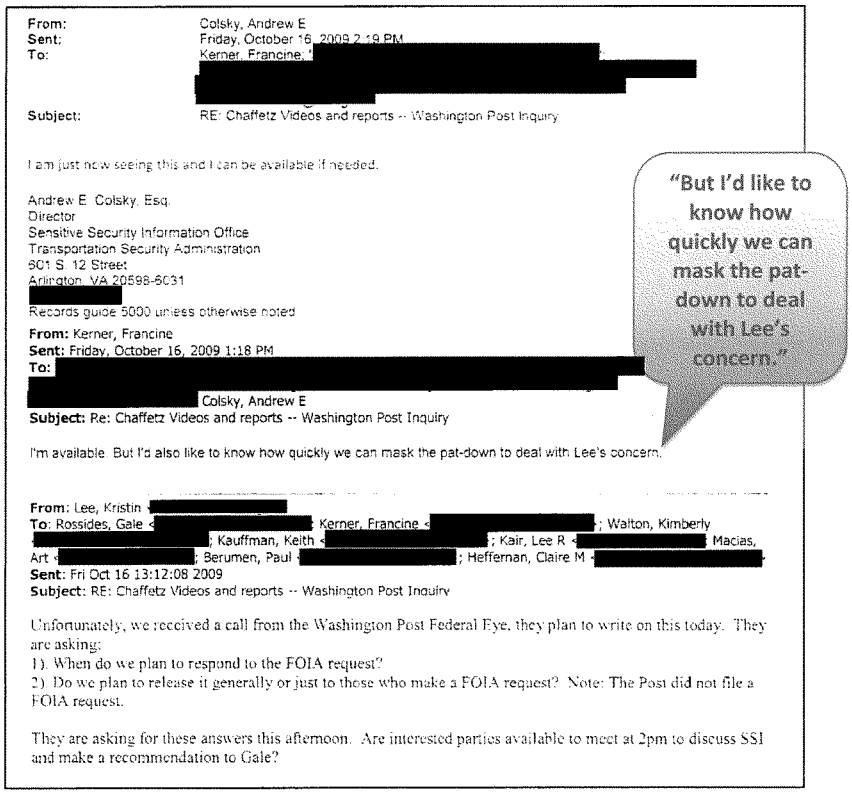
The FOIA request for the video on Cong. Chaffetz continue to add up. After the discussion this morning, it was brought to my attention that SSI has already reviewed the video and determined that it does not contain SSI.

Generally, a FOIA determination/final response is required within 20 business days from the date of receipt. Our first requests were received in the Office on 10/1. We are currently in receipt of five FOIA requests pertaining to Congressman Chaffetz and the first of these requests were received in the FOIA Office on October 1, 2009. The FOIA Office is in receipt of responsive reports and CCTV recordings. These records are being reviewed for release determinations.

We fully anticipates responding to these requests within the twenty days afforded under the FOIA. However, I understand from Kristen that she is receiving considerable pressure for an earlier release.

[64] *Id.* at 53-54.
[65] E-mail to from Kimberly Walton, Ass't Adm'r, Office of Special Counselor, to Lee Kair, Ass't Adm'r, Office of Sec. Operations, & Francine Kerner, Chief Counsel, TSA, et al. (Oct. 16, 2009, 12:54 p.m.).
[66] E-mail from Francine Kerner, Chief Counsel, TSA, to Kimberly Walton, Ass't Adm'r, Office of Special Counselor, et al. (Oct. 16, 2009, 1:02 p.m.).

Even as TSA General Counsel Francine Kerner was suggesting a meeting with the SSI Office to discuss overruling the SSI Office's determination, Kerner was planning how to "mask the pat down" in the video.[67]



From: Colsky, Andrew E
Sent: Friday, October 16, 2009 2:19 PM
To: Kerner, Francine; [redacted]
Subject: RE: Chaffetz Videos and reports -- Washington Post Inquiry

I am just now seeing this and I can be available if needed.

Andrew E. Colsky, Esq.
Director
Sensitive Security Information Office
Transportation Security Administration
601 S. 12 Street
Arlington, VA 20598-6031
[redacted]
Records guide 5000 unless otherwise noted

From: Kerner, Francine
Sent: Friday, October 16, 2009 1:18 PM
To: [redacted] Colsky, Andrew E
Subject: Re: Chaffetz Videos and reports -- Washington Post Inquiry

I'm available. But I'd also like to know how quickly we can mask the pat-down to deal with Lee's concern.

"But I'd like to know how quickly we can mask the pat-down to deal with Lee's concern."

From: Lee, Kristin [redacted]
To: Rossides, Gale [redacted]; Kerner, Francine [redacted]; Walton, Kimberly [redacted]; Kauffman, Keith [redacted]; Kair, Lee R [redacted]; Macias, Art [redacted]; Berumen, Paul [redacted]; Heffernan, Claire M [redacted]
Sent: Fri Oct 16 13:12:08 2009
Subject: RE: Chaffetz Videos and reports -- Washington Post Inquiry

Unfortunately, we received a call from the Washington Post Federal Eye, they plan to write on this today. They are asking:
1). When do we plan to respond to the FOIA request?
2). Do we plan to release it generally or just to those who make a FOIA request? Note: The Post did not file a FOIA request.

They are asking for these answers this afternoon. Are interested parties available to meet at 2pm to discuss SSI and make a recommendation to Gale?

Colsky sent a follow up e-mail to the SSI Office that stated:

> Note, I expressed that the SSI regulation and the SSI Office guidance, along with [former Deputy Director of the SSI Office] Rob Metzler's review and my own review did not reveal anything about the blurred portion of the image that would cause me to believe it was SSI. Showing

[67] E-mail from Andrew Colsky to Francine Kerner, et al. (Oct. 16, 2009, 2:19 p.m.).

> the capabilities of all of the cameras for that area, however, was worth considering.[68]

Colsky, the head of the SSI Office, stated he felt he was left out of the SSI determination process.[69] Ultimately, the video was released with the pat down of Chairman Chaffetz masked.[70]

VII. The Release of Information against the Advice of the SSI Office

FINDING:	TSA repeatedly released information to the public against the advice of the SSI Office and without proper documentation to explain the release.

TSA's Office of Public Affairs (OPA) repeatedly released information to the public against the advice of career staff within the SSI Office.

A. SSI Related to Federal Air Marshals

Both the former Director and Deputy Director of the SSI Office provided examples in which agency officials released information related to the presence of Federal Air Marshals (FAMs) on domestic flights. According to both Colsky and former SSI Office Deputy Director Robert Metzler, information about the deployment of air marshals was to be protected as SSI. Metzler stated:

> The Federal Air Marshal Service has always expressed to our office a desire to always be very protective of the flights on which their marshals can—the flights on which they have air marshals. And as much as possible we have always attempted to protect it.[71]

Metzler described two examples of incidents in which TSA's OPA released specific information about the presence of an air marshal on a flight. In one example, Metzler said an OPA official issued a press release that a plane that had to make an emergency landing had an air marshal on board. According to Metzler, "[i]n our office we saw absolutely no reason why you would release that information."[72] Metzler also described an incident in which individuals were smuggling weapons into the United States and TSA issued a statement stating "something along the lines that though nobody was in danger, there were Federal Air Marshals on that flight."[73]

Former Director Andrew Colsky also stated:

---

[68] E-mail from Andrew Colsky to Doug Blair & Robert Metzler (Oct. 16, 2009, 4:48 p.m.).
[69] Colsky Tr. at 62.
[70] Nicole Gonzales, *TSA Releases Reports Detailing Incident with Utah Congressman*, KSL.COM, Nov. 5, 2009, http://www.ksl.com/?nid=148&sid=8568676.
[71] Transcribed Interview of Harry Robert Metzler, Jr., Transcript at 96 (Dec. 15, 2011) [hereinafter Metzler Tr.].
[72] *Id.* at 97.
[73] *Id.* at 98.

> Consistently and regularly, whenever there were any events that were newsworthy and dealt with an airline, Public Affairs would be in touch with the news media and couldn't wait to tell them—whether it was true or not, I don't know—there were air marshals aboard you know or this is a regular route that air marshals fly or air marshals you know never travel alone.[74]

In one particular case, the TSA Administrator authorized the public release of information about FAMs without consulting the SSI Office. Colsky said in his interview he was unaware OPA had released the information until he saw it in the news.[75] Former Administrator Kip Hawley explained his decision in an e-mail. Hawley stated:

> I authorized the release of information related to that specific incident. There are real and timely security benefits from public disclosure of the FAM action on that flight for that reason. It is my understanding that I have the authority to make such a decision, and I did so in the best interests of securing passenger air travel. As you know, there is a substantial body of classified information to support this decision.[76]

TSA's release of information related to FAMs is particularly ironic given the agency's treatment of whistleblower and former air marshal Robert MacLean. In 2003, MacLean blew the whistle on TSA's plans to cancel FAM coverage on flights despite the threat of an imminent Al Qaeda hijacking plot.[77] Numerous Members of Congress raised concerns, and DHS retracted the order to cancel FAM coverage, calling it "a mistake."[78] Three years later, TSA retroactively labeled the information that MacLean had disclosed as SSI and fired MacLean for his disclosure.[79]

MacLean challenged his dismissal under the Whistleblower Protection Act (WPA). The government argued that MacLean's disclosures were not protected under the WPA because TSA's SSI regulations prohibit disclosure. On March 19, 2012, Representatives Elijah Cummings, Dennis Kucinich, and Carolyn Maloney filed an amicus brief arguing that only Congress, through statutory authority, or the President through Executive Order, can restrict the public free speech rights of government employees to disclose information protected under the WPA.[80] In April 2013, the U.S. Court of Appeals for the Federal Circuit sided with MacLean, holding that agency regulations, such as TSA's SSI regulations, do not trump a federal employee's protections under the WPA.[81] On May 19, 2014, the U.S. Supreme Court granted

---

[74] Colsky Tr. at 36-37.
[75] *Id.* at 69-70.
[76] E-mail from Adm'r Kip Hawley to Ellen Howe (June 20, 2008, 5:16 p.m.).
[77] *What TSA Whistleblower Robert McLean Tells Us About Post-9/11 Security*, MOTHER JONES, May 9, 2013, http://www.motherjones.com/politics/2013/05/tsa-whistleblower-maclean-security.
[78] *Air Marshals Back to Long Flights*, USA TODAY, July 30, 2003, http://usatoday30.usatoday.com/news/washington/2003-07-30-air-marshal_x.htm.
[79] Government Accountability Project, *GAP Hails Court Ruling Reaffirming Whistleblower Victory* (Sept. 3, 2013).
[80] Brief for Representatives Cummings, Kucinich, & Maloney as Amici Curiae Supporting Reversal, MacLean v. Dep't of Homeland Sec., 714 F.3d 1301 (2013).
[81] Robert J. MacLean v. Dep't of Homeland Security, 714 F.3d 1301 (Fed. Cir. 2013).

DHS's certiorari petition, agreeing to hear the Administration's appeal of the Federal Circuit's decision during the Court's next term.[82]

The lack of communication between OPA and the SSI Office regarding approved releases of information made it very difficult for the SSI Office to do its job. Colsky explained this in an e-mail to Office of Chief Counsel officials. He wrote: "I also cannot sign my name to court documents confirming SSI decisions because I may find the very same information on the news the same day."[83]

From:	Colsky, Andrew E
Sent:	Friday, June 20, 2008 10:21 AM
To:	Newhouse, Victoria <TSA OCC>; Johnson, Robert S <TSA OCC>; Walton, Kimberly; Plofker, Howard <TSA OCC>
Cc:	Osler, Bonnie <TSA OCC>; Ruggeri, Amy <TSA OCC>; 'Riggs, Ronald <TSA OCC>'; Bester, Margot <TSA OCC>
Subject:	RE: SSI Breach
Follow Up Flag:	Follow up
Flag Status:	Flagged

I have received confirmation from Ellen that Kip did in fact authorize this release. He has the authority to do so and that is his choice. We do, however, have a process problem here in that OPA does not share this information with the SSI Office despite repeated requests.

I am very uncomfortable in that I have personally given a deposition under oath in a very similar case supporting the fact that this is SSI and a man lost his job over it. I am unable to assist OCC with any testimony in future cases as I don't know what to honestly call SSI anymore. I also cannot sign my name to court documents confirming SSI decisions because I may find the very same information on the news the same day.

I think SSI and OCC need to sit down together and decide how to move forward. Perhaps we need to de-SSI portions of the regulation? I cannot have my staff continue to protect images and FAM information, etc. I am also unclear on how to proceed with marking of GAO reports for Congress especially related to covert testing.

I will send out a meeting invite to those people on this email and allow you to invite any others you feel may need to attend.

Colsky testified that he believed these strategic releases were "security theater" meant to convince the public that the nation's transportation systems were secure. Colsky testified:

> TSA is an organization, sadly, that focuses—you know, the term 'security theater' has been used, and unfortunately it's true. Let's do whatever we need to do to change the public perception. Let's not worry about the real issues behind the scenes. And that's all it was. If we needed—if they felt **they needed to do something to get it in the press to change the public**

[82] U.S. Supreme Court, Dep't of Homeland Security v. MacLean, No. 13-894, Petition for Writ of Certiorari Granted May 19, 2014, http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/13-894.htm (last visited May 27, 2014).

[83] E-mail from Andrew Colsky to Victoria Newhouse, et al. (June 20, 2008, 10:21 a.m.).

> **perception, that was more important than the security concerns involved**. Period.[84]

Colsky said that the release of SSI by the Office of Public Affairs decreased when the personnel changed in 2009 as part of the new Administration[85]

B. SSI Related to Whole Body Imagers

The implementation of the controversial Whole Body Imager ("WBI") machines generated significant press attention for TSA. In response, OPA granted media access to TSA's WBIs. Some employees in the SSI Office considered images created by the machines and other related information to be SSI because the release of such materials could adversely affect national security.[86] SSI Office staff were concerned that terrorists could use the published images to determine the device's vulnerabilities. Colsky informed the Committee that in 2009, after TSA's chief scientist implored him to find a way to stop TSA from releasing WBI images, Colksy approached OPA.[87] Despite Colsky's warnings, TSA made the images available to the media. Former SSI Office Deputy Director Metzler testified:

> [TSA decided to] allow the press to have some level of access to the images, which technically under the [SSI regulation], where it was very specific and said this is SSI, the decision was made that we have to release some level of images because the public has such concern, we have to respond to these public concerns, we need to share this information.[88]

Following a meeting with the SSI Office in which the SSI Office designated the images as SSI—OPA defied the designation and released the images publicly.[89] Colsky testified: "[The images] were designated SSI, and **it was just ignored by the Public Affairs Office**."[90] An attorney from TSA's Office of Chief Counsel expressed surprise about the release after seeing those images posted on TSA's website. In an e-mail to Metzler, Howard Plofker wrote: "Public Affairs is stating that these images are EXACTLY what TSOs see. If correct, wouldn't the images be SSI? "[91]

---

[84] Colsky Tr. at 21 (emphasis added).
[85] *Id.* at 86-87.
[86] *Id.* at 21-23.
[87] *Id.* at 25-26.
[88] Metzler Tr. at 62.
[89] E-mail from Howard Plofker to Robert Metzler & Andrew Colsky (May 12, 2008, 10:02 a.m.).
[90] Colsky Tr. at 23 (emphasis added).
[91] See E-mail from Plofker, *supra* note 89.

From: Plofker, Howard <TSA OCC>
Sent: Monday, May 12, 2008 10:02 AM
To: Metzler, Robert
Cc: Colsky, Andrew E
Subject: FW: Blog Post on Friday containing frontal images of MMV
Importance: High

Rob,

Would you review this post? Public Affairs is stating that these images are EXACTLY what TSOs see. If correct, wouldn't the images be SSI?

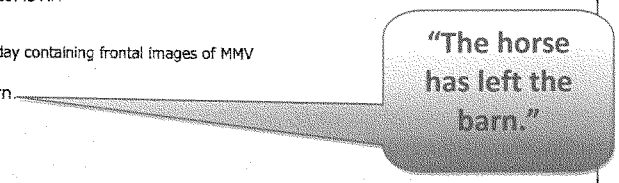
BTW, the checkpoint technologies guide doesn't discuss mm wave.

Howard Plofker
Office of Chief Counsel
Transportation Security Administration

In response, Metzler replied, "[t]hanks for bringing this to our attention, we are responding but the images are probably going to be staying up."[92] Because OPA had already posted the images on its blog, TSA counsel, Howard Plofker, acknowledged that it would not be helpful to remove the images from the website. He stated in an e-mail to Metzler, "The horse has left the barn."[93]

From: Plofker, Howard <TSA OCC>
Sent: Monday, May 12, 2008 10:45 AM
To: Metzler, Robert
Cc: Colsky, Andrew E
Subject: RE: Blog Post on Friday containing frontal images of MMV

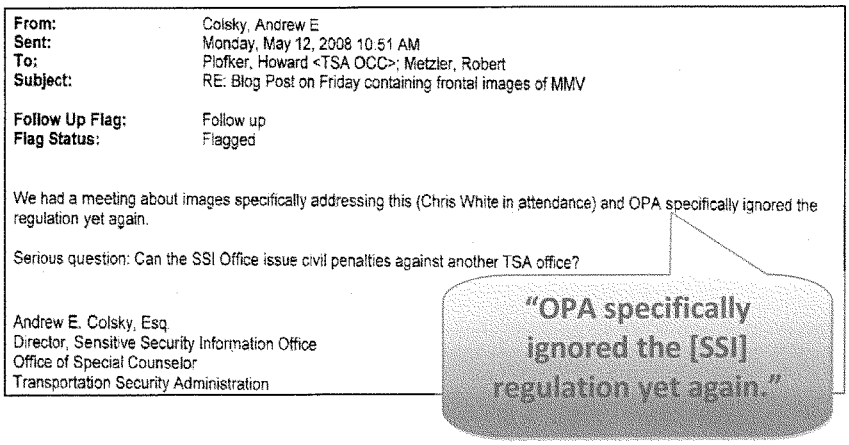
The horse has left the barn.



Howard Plofker
Office of Chief Counsel
Transportation Security Administration

Considering the sensitivity of the information and the internal disagreement about its release, Colsky was frustrated. He was especially distressed because a meeting had been held concerning the images. He wrote: "OPA specifically ignored the regulation yet again."[94]

[92] E-mail from Robert Metzler to Howard Plofker & Andrew Colsky (May 12, 2008, 10:42 a.m.).
[93] E-mail from Howard Plofker to Robert Metzler & Andrew Colsky (May 12, 2008, 10:45 a.m.).
[94] E-mail from Andrew Colsky to Howard Plofker & Robert Metzler (May 12, 2008, 10:51 a.m.).



Despite the fact OPA made these images available to the public on the TSA blog, similar full body millimeter wave images continued to be withheld from FOIA requesters.[95] Such actions illustrate the dichotomy in the treatment of such similar information. For example, in July 2009, through a FOIA request, the Electronic Privacy Information Center (EPIC) sought uncensored images from Advanced Imaging Technology (AIT) scanners, contracts relating to the use and manufacture of AIT, and complaints to TSA about the use of AIT. In response, DHS withheld 2,000 images produced by the body scanners and 376 pages of TSA training materials.[96] Further, the Committee was only allowed limited access to these images through an *in camera* review because the DHS officials considered them to be sensitive.

This is not the first time the Committee explored the inconsistent treatment and release of SSI information. In February 2008, Chairman Henry Waxman and Ranking Member Tom Davis inquired about a TSA Administrator's CNN interview during which he divulged sensitive information about covert testing. Waxman and Davis noted the paradox – that while TSA imposed strict standards on the Committee to prevent release of SSI during a congressional hearing on a GAO covert testing report, the TSA Administrator revealed related SSI on the same subject to the general public on national television.[97]

[95] *See* Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec. (*EPIC I*), 750 F. Supp. 2d 4, 7-8 (D.D.C. 2011), *mot. for relief from judgment denied*, 653 F.3d 1 (D.C. Cir. 2011).
[96] *EPIC I*, 760 F. Supp. 2d at 8.
[97] Letter from Rep. Henry A. Waxman, Chairman, & Rep. Tom Davis, Ranking Mem., H. Comm. on Oversight & Gov't Reform, to Hon. Edmund Hawley, Adm'r, TSA (Feb. 22, 2008).

VIII. Inter-Office Rift Causes Inconsistent Application of the SSI Regulations

Witnesses testified that many problems surrounding the SSI designation process emanate from inconsistent implementation of the SSI regulation. The Administrator is a political appointee, and the regulation is subject to interpretation by the Administrator. Thus, the Administrator has significant latitude in making SSI determinations. This power, combined with the seemingly arbitrary manner in which SSI is labeled, makes it easy for Administrators to play politics with sensitive information. In fact, such inappropriate handling of this information was confirmed by multiple witnesses, who testified that TSA's Office of Chief Counsel, OPA, and the TSA Administrator repeatedly neglected to consult with the SSI Office when making SSI determinations. This rendered the SSI Office powerless and has made the SSI decision-making process appear biased.

Regulations authorize TSA to make a conditional disclosure of specific records or information that constitute SSI, "upon the written determination by TSA that disclosure of such records or information ... would not be detrimental to transportation security."[98] The former SSI Office Director and the Deputy Director informed the Committee that documentation of an authorized disclosure is typically completed through the issuance of a memorandum. They stated that a memo explaining a decision to release SSI is important to ensure consistency in future SSI determinations. Yet, the SSI Office received very little guidance regarding the treatment of certain information. Former SSI Office Deputy Director Metzler testified:

> Q. The other thing we talked about is sort of the importance of memorializing this information at the beginning of the process . . . early on, so that it is clear . . . what information is being released. So, again, it sounds like there was a significant amount of time that passed between the beginning when these pictures were first released, and later on when the memo was actually written.
>
> Can you talk maybe just for a moment about . . . what importance might have been for the SSI office of having that memo written before the images were actually released or at the beginning of that process?
>
> A. For example, when we were seeing images released, we didn't know what that meant for PowerPoint presentations where we would have individuals that were going to conferences and those conferences might have AIT images present in them. So does that mean that I protect the images when they are trying—I don't know what—you have seen those images. It is hard to tell if it is the

[98] 49 C.F.R. § 1520.15(e) (stating that TSA may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by TSA that disclosure of such records or information, subject to such limitations and restrictions as TSA may prescribe, would not be detrimental to transportation security).

> same image that might be a template or not. It is sometimes difficult for the untrained eye to make that decision.
>
> So am I supposed to protect it if it is going to this conference, or am I not? If I have training documents related to AIT screening, do I protect the images in those training documents that might be subject to litigation or might be subject to FOIA? I know decisions were made to release those images. Even though the reg[ulation] specifically says all images, how do I apply the senior leadership team's decision that this is not detrimental; what are the parameters of that; how much do I protect related to other images; how much do I not?
>
> So that would make it difficult for us to decide what to protect. And once you have opened up that door to those types of images, even though the reg[ulation] makes no distinction, am I supposed to alter the way I protect X ray images or EDS images? Did someone make the decision that we no longer need to protect any images?
>
> We didn't know what the decisions were. So the way we treated it at the time was without any additional guidance, we were still very protective of all of the other images until we received some kind of guidance as to what should or should not be protected.[99]

Witnesses reported that in some cases, a determination memo would be submitted to the SSI office **retroactively**. Metzler stated that failure to follow the protocols and such little guidance on designations substantially increased the likelihood of inconsistencies in TSA's SSI designations. Metzler explained:

> Q. So that could lead to some inconsistencies, then?
>
> A. Yes.
>
> Q. So is it fair to say . . . if you had been in the room or someone from the SSI had been in the room, a couple of things they would have pointed out might have been . . . the importance of . . . making a clear determination about what is being released and about writing that information down in a memorandum so that it was clear for everyone who is handling SSI material?
>
> A. Yes.

[99] Metzler Tr. at 73-74.

> Q. And is that, again, to your understanding, to the best of your understanding, is it required the SSI office to be involved in that conversation, or at least under the policies of the Department?
>
> A. Or have the decision relayed to us with some formality so that we could be confident that the decision actually was made by somebody with the appropriate authority to make that decision. It was I think never our position that that was a decision that they could not make. It was that the decision had not been relayed to us and we didn't know how to respond to the--it was like trying to read tea leaves; you don't know what is intended there. You can read into it any number of different things.[100]

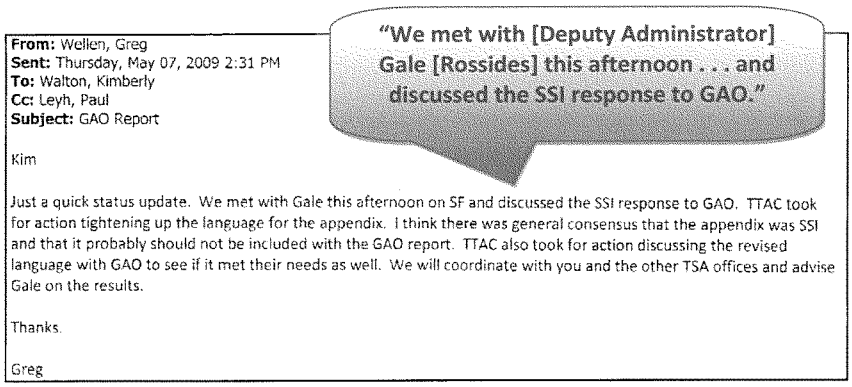
Witnesses also described that senior TSA officials repeatedly excluded the SSI Office from discussions about SSI determinations, even though TSA's Management Directive (MD) requires collaboration with the SSI Office. Metzler stated:

> Q. And so under your understanding of the management directive, the current one, not the draft one--could that person, the Assistant Administrator for Public Affairs, make that determination without consulting someone above them in the chain of command?
>
> A. My understanding of the regulatory requirements is that **if something is specifically identified as SSI, either in the regulation or in our written guidance, that needs some formal discussion with the SSI office before that information is released**. If the head of the Office of Public Affairs were to receive a document from some program office related to their program, they are in a position to know not every word in there is going to be SSI and they can, under their authority and responsibility, make decisions on particular information that should be shared. And if they include information that they then release that TSA has otherwise protected, from my reading of the reg and the MD, is that that would constitute a breach that needs to be addressed formally.[101]

An e-mail exchange between Office of Chief Counsel officials and Andrew Colsky illustrates an instance in which TSA officials made an SSI determination without the input or agreement of the SSI Office. In the following e-mail, senior TSA officials discussed proposed responses to potential SSI in a GAO report.[102] The e-mail shows that a consensus was reached, but it does not mention whether the SSI Office was included in the consensus.[103]

---

[100] Metzler Tr. at 74-75.
[101] *Id.* at 76.
[102] E-mail from Greg Wellen to Kimberly Walton & Paul Leyh (May 7, 2009, 2:31 p.m.).
[103] *Id.*



From: Wellen, Greg
Sent: Thursday, May 07, 2009 2:31 PM
To: Walton, Kimberly
Cc: Leyh, Paul
Subject: GAO Report

Kim

Just a quick status update. We met with Gale this afternoon on SF and discussed the SSI response to GAO. TTAC took for action tightening up the language for the appendix. I think there was general consensus that the appendix was SSI and that it probably should not be included with the GAO report. TTAC also took for action discussing the revised language with GAO to see if it met their needs as well. We will coordinate with you and the other TSA offices and advise Gale on the results.

Thanks.

Greg

In the next e-mail, Paul Leyh, Director of the "TSA Secure Flight" program, states, "I'm working on the language and will forward a draft when completed."[104] The director of another program—not the SSI Office—prepared the draft response on the SSI issue. Shortly thereafter, Leyh sent an e-mail with the draft language attached. He wrote:[105]

From: Leyh, Paul
Sent: Thursday, May 07, 2009 5:39 PM
To: Leyh, Paul; Thompson, Mardi <TSA OCC>; Smith, Courtney <TSA OCC>; Colsky, Andrew E; Schamberger, Steven
Cc: Wellen, Greg; [redacted]
Subject: GAO Report

All,

As a follow up to previous emails and discussion with Gale earlier today attached is the draft of the language that supports the direction requested for the GAO SF report. Please review and let me know if there are any changes, updates, etc.. I'd appreciate any feedback by tomorrow morning so that we can get this issue closed out tomorrow. Current PW applies.

In response, another TSA employee, Steven Schamberger, responded that he would defer to the SSI Office on what was to be considered SSI.[106]

[104] E-mail from Paul Leyh to Mardi Thompson, et al. (May 7, 2009, 3:27 p.m.).
[105] E-mail from Paul Leyh to Mardi Thompson, et al. (May 7, 2009, 5:39 p.m.).
[106] E-mail from Steven Schamberger to Paul Leyh, et al. (May 7, 2009 5:48 p.m.).

From: Schamberger, Steven
Sent: Thursday, May 07, 2009 5:48 PM
To: Leyh, Paul; Thompson, Mardi <TSA OCC>; Smith, Courtney <TSA OCC>; Colsky, Andrew E
Cc: Wellen, Greg; [redacted]
Subject: RE: GAO Report

Paul,
I defer to the SSI office as to whether the added material is in fact SSI. But if it is GAO will not accept this. They want to produce a public report and only a public report. They are not producing a companion SSI version of the report.

"I defer to the SSI office as to whether the added material is in fact SSI."

Shortly after Schamberger's e-mail, Colsky expressed his concern. He wrote, "I am very uncomfortable and somewhat shocked with the way this process has been handled."[107]

From:	Colsky, Andrew E
Sent:	Thursday, May 07, 2009 5:56 PM
To:	Leyh, Paul; Thompson, Mardi <TSA OCC>; Smith, Courtney <TSA OCC>; Schamberger, Steven
Cc:	Wellen, Greg; [redacted] Metzler, Robert; Blair, Doug E.
Subject:	RE: GAO Report
Follow Up Flag:	Follow up
Flag Status:	Flagged

All:

I am very uncomfortable and somewhat shocked with the way this process has been handled. I cannot comment on the product of a process in which my office has not been appropriately involved. I suggest we discuss SSI issues with the SSI office at the table, not as an afterthought.

In the following e-mail, TSA Assistant Administrator Greg Wellen appears to completely disregard Colsky's documented frustration.[108] Wellen does not address Colsky's e-mail when he writes that he would set up a teleconference with GAO to discuss the SSI issue with three other TSA employees, none of whom were from the SSI Office.[109]

[107] E-mail from Andrew Colsky to Paul Leyh, et al. (May 7, 2009, 5:56 p.m.).
[108] E-mail from Greg Wellen to Paul Leyh, et al. (May 8, 2009, 9:53 a.m.).
[109] *Id.*

From: Welon, Greg
Sent: Friday, May 08, 2009 9:53 AM
To: Schamberger, Steven; Leyh, Paul; Thompson, Mardi <TSA OCC>; Smith, Courtney <TSA OCC>; Colsky, Andrew E
Cc: [redacted]; Williams, Alison; Webb, Matthew <TSA OCC>
Subject: RE: GAO Report

Steve

Appreciate the update. Paul and I will set up a teleconference with Penny to address the SSI issue. We will make sure Matt and Mardi are also included. Will advise DC of the results

Thanks

Greg

Shortly thereafter, Colsky sent a subsequent e-mail requesting a meeting with Schamberger and the Special Counselor for TSA. The purpose of the meeting was, in Colsky's words, to "get back on track."[110] It is unclear whether that meeting took place. What is clear is excluding the SSI Office from decisions to determine whether information qualifies as SSI can lead to inconsistent application of the SSI regulations.

IX. SSI Office Structure and Position within TSA

FINDING:	**The structure and position of the SSI office within TSA has contributed to the difficulties the office has encountered in carrying out its mission. TSA has moved the office within the agency's organizational structure several times. One official stated the office moves have effectively relegated it a "throwaway office."**

TSA moved the SSI Office within the agency hierarchy several times. Originally, the SSI Office reported directly to the Chief of Staff to the TSA Administrator. The Office was then moved under the supervision of the Assistant Chief Administrator. It remained there until it was again relocated to the Business Management Office within the Office of Intelligence.[111] Later, the SSI Office was placed under the authority of the Federal Air Marshal Service. According to Colsky, this move only further marginalized the office. Colsky testified:

> Q. How so does moving it into the Federal Air Marshal Service marginalize it further?
>
> A. Because they've been moved so far down the organization, they don't have access to anything. They don't have access to decision

[110] E-mail from Andrew Colsky to Kimberly Walton (May 8, 2009, 10:30 a.m).
[111] Colsky Tr. at 99-100.

> makers. They don't have access to the budget and stuff that they would normally have. **It's just a throwaway office now.**[112]

TSA informed the Committee that the agency moved the SSI Office as part of an Office of Intelligence initiative. A review determined that the functions of the SSI Office were more closely aligned with the mission and responsibilities of the Federal Air Marshal Service's Chief Security Officer, also charged with managing TSA's classified information program. Considering the importance of the SSI designation process, TSA should give the SSI Office a more prominent position in the TSA hierarchy to enable effective communication with OPA and TSA leadership.

X. TSA's Efforts to Address the Problems

FINDING: TSA made significant improvements to its SSI designation process following the Committee's investigation.

On September 15, 2008, TSA issued Management Directive 2810.1, aimed at providing "policy and procedures for the issuance of sensitive security information (SSI) guidance, and the training of personnel on the procedures for recognizing, identifying, safeguarding, and sharing SSI."[113] In April 2012, TSA Administrator John Pistole issued a new SSI handbook applicable to all TSA personnel creating standard operating procedures for SSI. The handbook consolidated numerous stand-alone policies on SSI, streamlining the information to provide clearer guidance. New policies include a template for the revocation of SSI, a system for reporting SSI breaches, and an improved employee training program that is customized to each TSA office.

In late September 2013, the Committee received a briefing from the Division Director for the Office of Security Services and Assessments, who provided an update on the SSI program.[114] According to the Division Director, TSA has made improvements to employee training and SSI reporting.

The Committee's investigation found incidents in which OPA released SSI without following the proper procedures. It is not clear whether OPA released this type of information inadvertently or in spite of the regulation. Better knowledge of and respect for the SSI process are necessary. Online SSI training is now provided to all TSA employees, including those in OPA. Requiring OPA to complete SSI training is a step in the right direction. SSI training is tailored to the specific work of each TSA office. Through the training, employees learn how to report a breach and the process for revoking an SSI determination.

Additionally, an online program called "I-Share" is now used for all SSI incident reporting. Use of I-Share allows any TSA employee to report an SSI breach. Once a report is

---

[112] *Id.* at 100 (emphasis added).
[113] TSA, Office of the Special Counselor, Management Directive No. 2810.1, SSI Program (Sept. 15, 2008), http://www.tsa.gov/video/pdfs/mds/TSA_MD_2810_1_FINAL_080915.pdf.
[114] Briefing of Div. Dir., Office of Sec. Servs. & Assessments, TSA, to Committee Staff (Sept. 27, 2013).

submitted, it is sent to the SSI Office for resolution. By exposing problems related to the inconsistent labeling of SSI, the Committee's investigation has been successful in engaging TSA to reassess its SSI policies. What these policy changes do not address, however, is the ease with which political appointees can circumvent the process. Thus, changes to the SSI regulation itself are warranted to clarify the procedures that must be followed to designate information as SSI or to remove an SSI designation.

XI. Conclusion

The examples set forth in this report raise valid concerns as to whether TSA consistently uses the SSI designation appropriately. While the agency has made some improvements to the program, additional steps may be necessary in order to insulate the integrity of the SSI process.

TSA must ensure consistent and appropriate application of the SSI designation. TSA officials should always consult the SSI Office when making decisions either to designate information as SSI or to release information that has been or could be designated SSI. Documentation authorizing the release of SSI must be issued prior to the release, rather than after the fact. Further, the TSA Administrator should consider the location of the SSI Office within TSA's organizational structure so that it can perform its work free from political interference.

More broadly, Congress must strongly encourage agencies to curb the use of pseudo-classification of information. The proliferation of the use of unclassified designations in Executive Branch departments and agencies has a profound impact on public access. Strict enforcement of rules governing the use of such designations is necessary to prevent abuse and to maximize public access to government information. Agencies must make greater efforts to track and report the use of such labels on information, as it has become clear that consistency is lacking and better controls are needed. By focusing on the use of SSI at TSA, the Committee hopes to promote transparency and better information security across the Executive Branch.

Follow-Up Questions for Annmarie Lontz (TSA)

1. How many total FOIA requests has TSA received each year, for the last five fiscal years? For each fiscal year, please specify the number of SSI Review Requests, and the total corresponding number of pages.

2. Of the SSI Review requests TSA received over the last five fiscal years, what percentage did TSA redact or deny altogether?

3. DHS Deputy General Counsel Joseph Maher accused Subcommittee Chairman Jason Chaffetz of unlawfully releasing portions of a DHS PowerPoint Presentation during a National Security, Homeland Defense, and Foreign Operations Subcommittee hearing on July 13, 2011.

   In light of Executive Order 13556, "Controlled Unclassified Information," TSA's 2012 SSI Handbook and TSA's existing SSI designation training regime—isn't TSA's position on this matter erroneous?

4. FOIA requesters sought the video footage from TSA of Congressman Chaffetz's passing through a TSA checkpoint in November 2009. The SSI Office determined that the video did not contain any SSI. However, TSA officials including Assistant Administrator Lee Kair and TSA General Counsel, Francine Kerner, intervened to mask the part of the video which showed TSA agents administering Congressman Chaffetz a "pat down."

   This incident shows a lack of coordination among the TSA Administrator, the Office of Public Affairs, and the SSI Office. What efforts has TSA made to improve coordination among these offices?

5. Do you believe that TSA's new SSI training protocols and handbook improve the agency's ability to apply the SSI designation consistently, and in doing so, to protect sensitive information pursuant to Executive Order 13556?

Question#:	1
Topic:	FOIA 1
Hearing:	Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: How many total FOIA requests has TSA received each year, for the last five fiscal years? For each fiscal year, please specify the number of SSI Review Requests, and the total corresponding number of pages.

Response: The table below contains data derived from the inventories of both the Transportation Security Administration's (TSA) Freedom of Information Act (FOIA) Branch and the Sensitive Security Information (SSI) Program. Recognizing the need to improve the tracking mechanism for SSI reviews, in 2011, the SSI Program implemented a new SSI Reviews database which now closely tracks SSI reviews and the number of pages associated with each review. Accurate data prior to the implementation of the database is not available.

The 759 unique FOIA-initiated SSI Reviews for Fiscal Years (FY) 2011-2014 (to date) represented in the table below correspond to approximately 108,000 pages, according to data derived from the SSI Reviews database, which tracks the number of pages associated with each unique review.

	FY09	FY10	FY11	FY12	FY13	FY14 (to date)	Total
TSA FOIA REQUESTS	849	716	926	861	909	*Data Not Yet Available*	4,261
FOIA-INITIATED SSI REVIEWS (SUBSET OF TSA FOIA REQUESTS)	*Data Not Available*	*Data Not Available*	258	178	208	115	759
NUMBER OF PAGES (APPROX.)	*Data Not Available*	*Data Not Available*	30,000	30,000	28,000	20,000	108,000

Question#:	2
Topic:	SSI Review
Hearing:	Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Of the SSI Review requests TSA received over the last five fiscal years, what percentage did TSA redact or deny altogether?

Response: In 2011, the Transportation Security Administration's Sensitive Security Information (SSI) Program implemented a new SSI Reviews database, which now closely tracks SSI reviews and the number of pages associated with each review. Prior to 2011, there are no reliable data. Since 2011, the SSI Program has undertaken approximately 759 unique SSI Reviews at the request of the Freedom of Information Act (FOIA) office. Of those, approximately 19 reviews contained materials determined to be SSI in their entirety, accounting for 2.5 percent of SSI Reviews referred from the FOIA office.

For all SSI Reviews and assessments, regardless of source (FOIA, litigation, etc.), over the same period fewer than 50 of over 5,480 reviews were found to contain materials determined to be SSI in their entirety. This accounts for less than 1 percent of all SSI Reviews.

With regard to FOIA-initiated SSI Reviews for fiscal years 2011-2013 to which any SSI redaction was applied, the table below shows that SSI was redacted in whole or in part in 334 of 644 SSI Review referrals. This amounts to approximately 52 percent of FOIA-initiated SSI Reviews during this period.

	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014 (to date)
FOIA-INITIATED SSI REVIEWS	*Data Not Available*	*Data Not Available*	258	178	208	115
SSI REDACTED FROM RESPONSIVE RECORDS	104	76	100	101	133	*Data Not Yet Available*

Question#:	3
Topic:	Controlled Unclassified Information
Hearing:	Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: DHS Deputy General Counsel Joseph Maher accused Subcommittee Chairman Jason Chaffetz of unlawfully releasing portions of a DHS PowerPoint Presentation during a National Security, Homeland Defense, and Foreign Operations Subcommittee hearing on July 13, 2011.

In light of Executive Order 13556, "Controlled Unclassified Information," TSA's 2012 SSI Handbook and TSA's existing SSI designation training regime—isn't TSA's position on this matter erroneous?

Response: No, it is not erroneous. In a letter dated July 13, 2011, the Department notified Chairman Chaffetz that it had obtained information indicating that sensitive security information provided to the Subcommittee by TSA was inappropriately disclosed. The disclosure that this letter addressed was not a disclosure made during a congressional hearing. As noted in correspondence with the Committee, the sensitive security information was scanned into a PDF file by a copy machine at the Committee Offices and then disseminated to an unauthorized recipient who later forwarded the document to the Department. After learning of this breach of security, the Department sent a letter to Chairman Chaffetz expressing concern about this disclosure and sought to engage in a discussion to reach an understanding about how sensitive materials would be handled by the Subcommittee in the future.

Sensitive Security Information (SSI) is a category of sensitive but unclassified information that must be protected because it is information that, if publicly released, would be detrimental to the security of transportation. The Department's authority to protect this information was granted by Congress, and is codified at 49 U.S.C. § 114(r). The Transportation Security Administration's (TSA) SSI regulations, 49 C.F.R. 1520.7, prohibit the disclosure of SSI to persons other than covered persons who "have a need to know." SSI provided by the TSA to Chairman Chaffetz's subcommittee was in turn publicly disclosed. Neither Executive Order 13556, "Controlled Unclassified Information," TSA's 2012 SSI Handbook, nor TSA's existing SSI designation training regime negate the regulatory requirement for covered persons to take reasonable steps to safeguard SSI against unauthorized disclosure. Both the TSA *SSI Policies & Procedures Handbook* and the TSA SSI training regime instruct TSA personnel that SSI may not be released to the public.

Question#:	4
Topic:	FOIA 2
Hearing:	Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: FOIA requesters sought the video footage from TSA of Congressman Chaffetz's passing through a TSA checkpoint in November 2009. The SSI Office determined that the video did not contain any SSI. However, TSA officials including Assistant Administrator Lee Kair and TSA General Counsel, Francine Kerner, intervened to mask the part of the video which showed TSA agents administering Congressman Chaffetz a "pat down."

This incident shows a lack of coordination among the TSA Administrator, the Office of Public Affairs, and the SSI Office. What efforts has TSA made to improve coordination among these offices?

Response: The Transportation Security Administration (TSA) has implemented significant changes to its policies, training, and management of Sensitive Security Information (SSI) to ensure, among other objectives, proper coordination and collaboration in the designation of information as SSI. An updated Management Directive (MD) on SSI, issued in April 2012, specifically charges senior TSA officials with the responsibility to coordinate with the SSI Program to ensure information within their programs is identified as SSI appropriately. The Handbook accompanying the MD, also issued in April 2012, provides detail on the SSI review and assessment processes beyond that which was documented in November 2009. The guidance issued by TSA makes clear that coordination between TSA offices and the SSI Program is paramount to the identification of SSI.

Furthermore, the TSA SSI Program has developed and deployed tools and aids to assist personnel throughout TSA in engagement of the SSI Program. These include: an automated SSI Review and SSI Assessment request function that resides on the TSA Intranet, a standard process to request the TSA Administrator's revocation of an SSI designation in the interest of public safety or transportation security, and the deployment of an improved database for tracking SSI Reviews.

In the incident cited above, TSA adopted a consultative, collaborative and deliberative approach among its program offices. After review by the SSI Office, the Assistant Administrator for the Office of Security Operations (OSO) – the TSA office in charge of airport security – expressed concern at that time about releasing footage that could be studied in detail to learn how a TSA pat-down was conducted. The video footage was reviewed together by the Assistant Administrator for the Office of Civil Rights and Liberties, the Deputy Assistant Administrator for OSO, the Director of the SSI Office, the Chief Counsel, the Special Assistant to the TSA Chief of Staff, and staff from the Office

Question#:	4
Topic:	FOIA 2
Hearing:	Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

of Legislative Affairs and the Office of Public Affairs. Taking into consideration the security concerns voiced by OSO, the video was altered to blur the pat-down. This action was cleared by the TSA Acting Administrator and the video was then posted in TSA's Electronic Reading Room.

Question#:	5
Topic:	SSI training
Hearing:	Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation
Primary:	The Honorable John L. Mica
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Do you believe that TSA's new SSI training protocols and handbook improve the agency's ability to apply the SSI designation consistently, and in doing so, to protect sensitive information pursuant to Executive Order 13556?

Response: Yes. The Transportation Security Administration's (TSA) abilities to apply the Sensitive Security Information (SSI) designation consistently and protect SSI accordingly have been improved by the updated training protocols and Handbook issued by the Agency. With respect to training, all TSA personnel are required to complete Basic SSI training every year, reviewing principles of identifying, marking, safeguarding, disclosing, and destroying SSI. Also, every TSA office and field location is required to have at least two persons who have completed the Advanced SSI Training and Certification Course. This means that these individuals have participated in detailed SSI training, have passed the SSI Certification Examination, and continue to maintain a high level of proficiency through annual participation in Continuing Education in SSI. These personnel are authorized to provide expertise in the identification of SSI, and they maintain awareness on developments in SSI affecting TSA personnel.

The updated Handbook provides a single, comprehensive resource for personnel to consult regarding their responsibilities concerning SSI. It replaced a previously-issued series of discrete, independent, and less-detailed SSI policies. It was extensively coordinated and provides guidance and assistance in a user-friendly format. It is organized by subject matter and covers SSI topics including identifying, marking, safeguarding, disclosing and destroying SSI, along with overviews of SSI training and awareness programs and instructions for the reporting and adjudication of SSI that is lost, stolen, or subject to unauthorized disclosure. Lastly, it is readily available to all TSA personnel on the TSA intranet.

Pursuant to Executive order 13556, SSI has been approved as a subcategory of Controlled Unclassified Information. TSA's updated training protocols and Handbook, along with the improved coordination and collaboration regarding SSI matters, significantly enhance TSA's ability to protect SSI consistent with the requirements of the Executive order.