OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Committee on Oversight and Government Reform

U.S. House of Representatives

"Transparency at TSA"

Homeland Security

March 2, 2017
10:00 AM

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me here today to discuss issues relating to transparency at the Transportation Security Administration (TSA).

The Importance of Transparency to the Work of the Office of the Inspector General (OIG)

The Value of Independent Oversight in Improving Government Operations

Oversight fosters positive change and makes government better. The critical and skeptical review of programs and operations, both by the Inspectors General and by congressional oversight committees, conducted in full view of the public, acts as the "disinfectant of sunlight" to ensure improved transparency, accountability, and efficiency in government. It also facilitates the efforts of Inspectors General to keep Congress fully and currently informed about problems and deficiencies within government programs and operations, in compliance with their obligations under the *Inspector General Act*.

TSA is an excellent example of an agency that has had to confront the necessity of changing the manner in which it does business. Our covert testing program, which revealed dramatic and troubling shortfalls, as well as other OIG reports about deficiencies in TSA's judgment of risk in relation to expedited screening, vetting airport employees, and managing the access badge program, all served as important catalysts for change.[1] It was only through our public oversight, and public oversight by this and other congressional committees, and TSA's then-new leadership strongly embracing the message, that TSA at last acknowledged the need for change and started the long road to becoming a more effective organization.

The OIG Policy Regarding Transparency in our Reports

However, the effectiveness of our oversight depends on our ability to issue detailed, balanced and public reports that accurately describe our findings and include recommendations to resolve them. The *Inspector General Act* requires that we inform the DHS Secretary, Congress, and the public about any problems and deficiencies we identify through our work.

[1] *Vulnerabilities Exist in TSA's Checked Baggage Screening Operations*, OIG-14-142 (September 2014); *Security Enhancements Needed to the TSA PreCheck Initiative*, OIG-15-29 (January 2015); *TSA Can Improve Aviation Worker Vetting*, OIG-15-98 (June 2015); *Use of Risk Assessment within Secure Flight*, OIG-14-153 (June 2015); *Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints*, OIG-15-150 (September 2015); *TWIC Background Checks Not as Reliable as They Could Be*, OIG-16-128 (September 2016); *TSA Could Improve Its Oversight of Airport Controls over Access Media Badges*, OIG-17-04 (October 2016).

In 2014, I became concerned that the Department's procedures for redacting OIG reports during component reviews reflected neither the letter nor the spirit of the *Inspector General Act* and significantly impeded the OIG's effectiveness. I found that, during sensitivity reviews, components often requested redactions based solely on the fact that reports were marked "For Official Use Only" or "Law Enforcement Sensitive." Component officials requesting these redactions appeared not to have the background or context needed to balance speculative sensitivity concerns against the very real need to inform Congress and the public about important government programs.

Accordingly, I instituted a new policy in June 2014 that limited redactions except in three narrow circumstances: (1) disclosure of the information is specifically prohibited by law; (2) an Executive Order specifically requires the information to be protected from disclosure in the interest of national defense, national security, or in the conduct of foreign affairs; and (3) the information is part of an ongoing criminal investigation. The new policy leaves open the possibility for other discretionary redactions — *e.g.*, in the event disclosure could cause significant harm to DHS programs and operations — but rested that discretion solely with the OIG. When considering whether to approve discretionary redactions, I require a component seeking the redactions to articulate the *specific*, *actual* harm that could result from disclosure.

Concerns About the TSA Sensitive Security Information System

TSA has a history of taking an aggressive approach to applying redactions, particularly with respect to a category of information known as Sensitive Security Information, commonly known by its acronym, SSI. This problem is well-documented. For instance, in our latest report on airport-based IT systems, published in December 2016, TSA demanded redaction of information that previously had been freely published without objection, and which my IT security experts believe poses no threat to aviation security.[2] We encountered a similar issue in 2015, when TSA insisted on applying the SSI designation to information in an audit report concerning the IT operations at John F. Kennedy airport that previously had been published in two prior OIG reports.[3]

Entities outside the OIG have made similar findings, and I believe that the problem is deeply rooted and systemic. For instance, as far back as 2005, GAO issued a report finding that TSA did not have adequate policies and procedures to determine what constitutes SSI or who was authorized to make the

[2] *Summary Report on Audits of Security Controls for TSA information Technology Systems at Airports*, OIG-17-14 (December 2016).
[3] *Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport*, OIG 15-18 (January 2015).

designation.[4] GAO found that TSA's lack of internal controls left TSA unable to provide reasonable assurance that those within TSA making SSI designations were applying the designation properly.[5] Nearly 10 years later, this Committee reached a similar conclusion in a bipartisan staff report it issued in 2014.[6] And in 2016, the House Committee on Homeland Security, Subcommittee on Transportation Security, objected to TSA's management and use of the SSI designation, noting that the improper invocation of SSI "raised the specter that we've heard again and again about TSA conveniently using the security classifications to avoid having public discussions about certain things that may be unpleasant for them to discuss in public."[7]

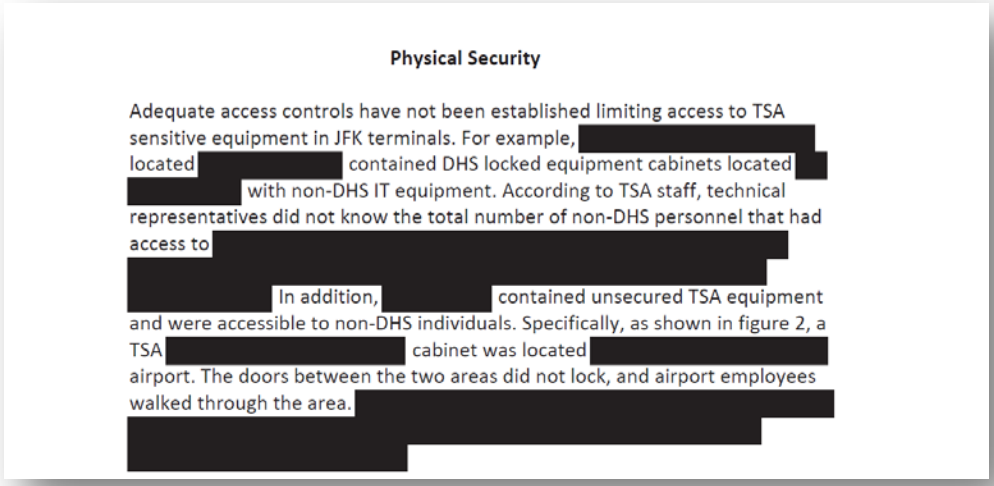
Impact of Misapplication of SSI on Whistleblowing

TSA's misapplication of the SSI designation can have far-reaching consequences. For instance, SSI designations have been used as a basis for challenging the disclosure of information by whistleblowers, which may have a chilling effect on future whistleblowers. The various categories of SSI are vague in nature, inviting differing interpretations about what qualifies as SSI and making it difficult for whistleblowers to determine whether the information may properly be disclosed. Moreover, TSA has designated information as SSI years after a disclosure to punish whistleblowers who, at the time of disclosure, had no reason to believe the information was SSI.

Illustrations of the Misapplication of SSI

The issues we have encountered with TSA's inconsistent or improper application of SSI can be easily illustrated. For instance, in our report discussing physical security issues in TSA's space at JFK airport, TSA's SSI Program Office marked much of the information as SSI:[8]

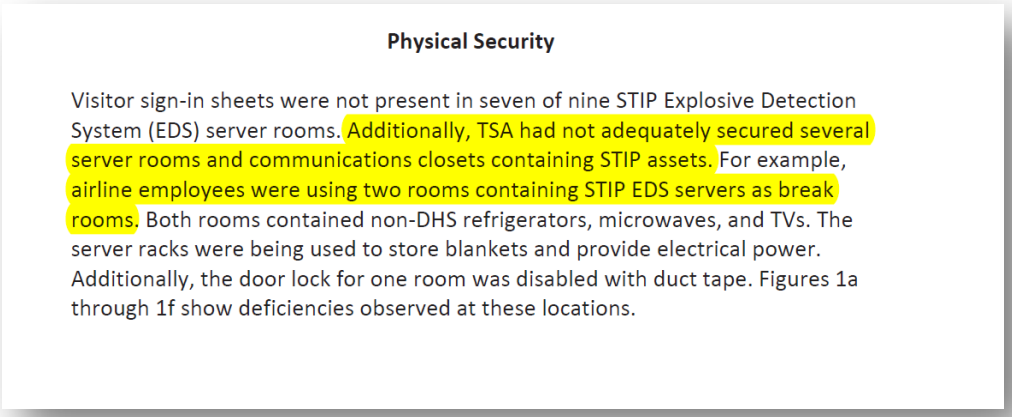
[4] *Clear Policies and Oversight Needed for Designation of Sensitive Security Information*, GAO-05-677 (June 2005).
[5] *Id*.
[6] *Joint Staff Report, Committee on Oversight and Government Reform, Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information (SSI) Designation*, May 29, 2014. (Retrieved from https://oversight.house.gov/wp-content/uploads/2014/05/Pseudo-Classification-Report-FINAL-5-28-2014-5.pdf).
[7] Hearing, How Pervasive is Misconduct at TSA: Examining Findings from a Joint Subcommittee Investigation. July 7, 2016.
[8] *Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport*, OIG 15-18 (January 2015).



Physical Security

Adequate access controls have not been established limiting access to TSA sensitive equipment in JFK terminals. For example, [redacted] located [redacted] contained DHS locked equipment cabinets located [redacted] with non-DHS IT equipment. According to TSA staff, technical representatives did not know the total number of non-DHS personnel that had access to [redacted] In addition, [redacted] contained unsecured TSA equipment and were accessible to non-DHS individuals. Specifically, as shown in figure 2, a TSA [redacted] cabinet was located [redacted] airport. The doors between the two areas did not lock, and airport employees walked through the area. [redacted]

However, we published similar information about security measures and potential vulnerabilities identified at Dallas-Fort Worth airport without redaction:[9]



Physical Security

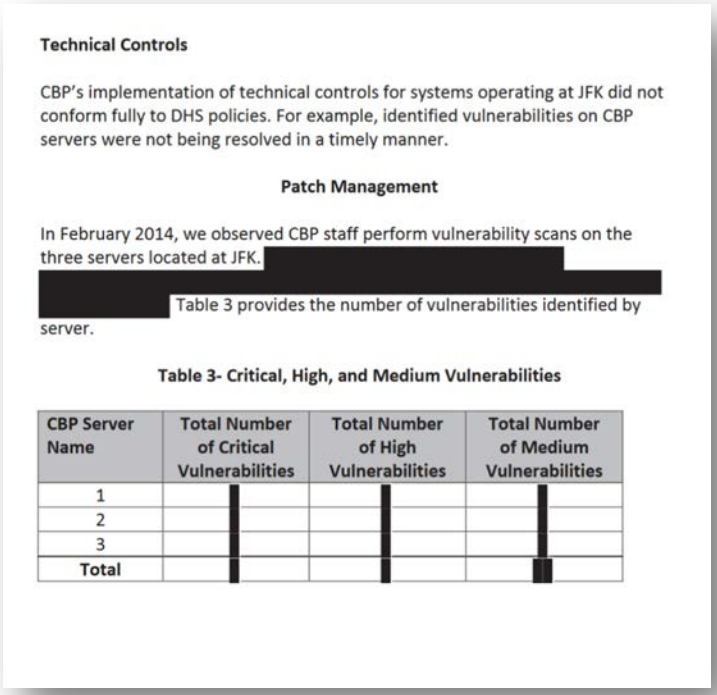
Visitor sign-in sheets were not present in seven of nine STIP Explosive Detection System (EDS) server rooms. Additionally, TSA had not adequately secured several server rooms and communications closets containing STIP assets. For example, airline employees were using two rooms containing STIP EDS servers as break rooms. Both rooms contained non-DHS refrigerators, microwaves, and TVs. The server racks were being used to store blankets and provide electrical power. Additionally, the door lock for one room was disabled with duct tape. Figures 1a through 1f show deficiencies observed at these locations.

Similarly, TSA redacted information about patch management issues at JFK in one of our reports, but did not redact similar wording used in two previously published reports regarding other airports:[10]

[9] *Audit of Security Controls for DHS Information Technology Systems at Dallas/Ft. Worth International Airport*, OIG-13-132 (September 2014)

[10] *Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport*, OIG 15-18 (January 2015); *Audit of Security Controls for DHS Information Technology Systems at Dallas/Ft. Worth International Airport*, OIG-13-132 (September 2014); *Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport*, OIG-13-104 (July 2013).

JFK Airport Report (pg. 21)



Technical Controls

CBP's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on CBP servers were not being resolved in a timely manner.

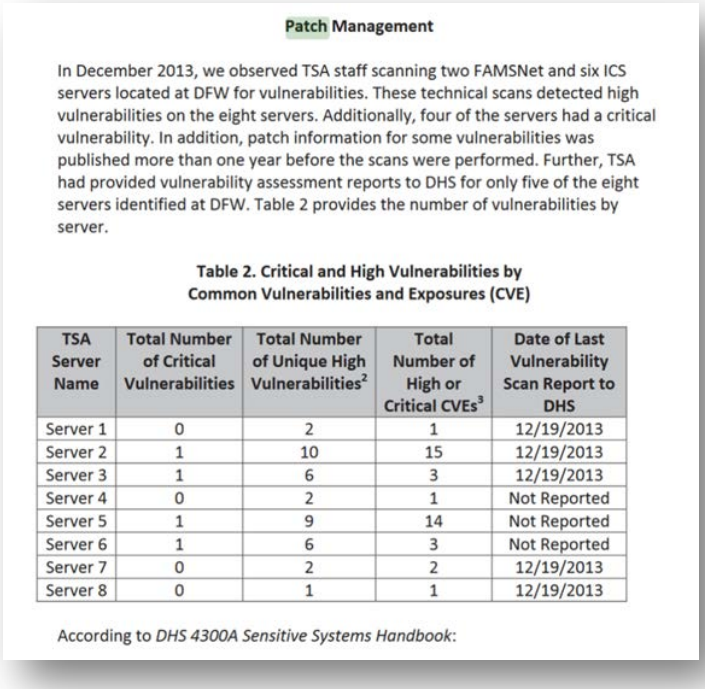
Patch Management

In February 2014, we observed CBP staff perform vulnerability scans on the three servers located at JFK. [redacted] Table 3 provides the number of vulnerabilities identified by server.

Table 3- Critical, High, and Medium Vulnerabilities

CBP Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]

Dallas-Fort Worth Airport Report (pg. 10)



Patch Management

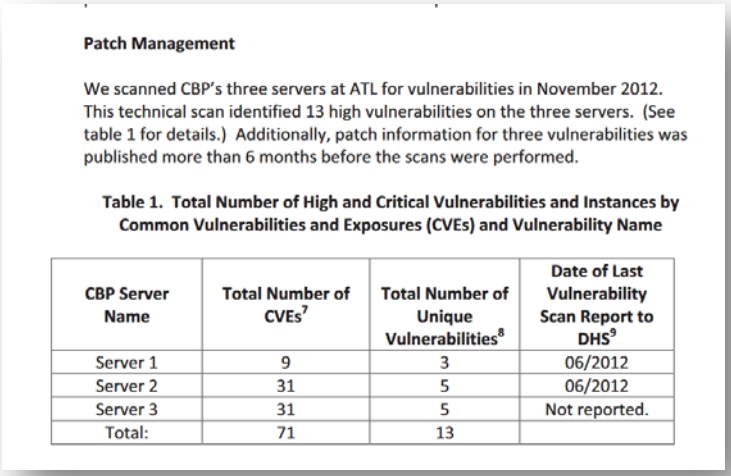
In December 2013, we observed TSA staff scanning two FAMSNet and six ICS servers located at DFW for vulnerabilities. These technical scans detected high vulnerabilities on the eight servers. Additionally, four of the servers had a critical vulnerability. In addition, patch information for some vulnerabilities was published more than one year before the scans were performed. Further, TSA had provided vulnerability assessment reports to DHS for only five of the eight servers identified at DFW. Table 2 provides the number of vulnerabilities by server.

Table 2. Critical and High Vulnerabilities by Common Vulnerabilities and Exposures (CVE)

TSA Server Name	Total Number of Critical Vulnerabilities	Total Number of Unique High Vulnerabilities[2]	Total Number of High or Critical CVEs[3]	Date of Last Vulnerability Scan Report to DHS
Server 1	0	2	1	12/19/2013
Server 2	1	10	15	12/19/2013
Server 3	1	6	3	12/19/2013
Server 4	0	2	1	Not Reported
Server 5	1	9	14	Not Reported
Server 6	1	6	3	Not Reported
Server 7	0	2	2	12/19/2013
Server 8	0	1	1	12/19/2013

According to *DHS 4300A Sensitive Systems Handbook*:

Atlanta Airport Report (Pg. 10)



Patch Management

We scanned CBP's three servers at ATL for vulnerabilities in November 2012. This technical scan identified 13 high vulnerabilities on the three servers. (See table 1 for details.) Additionally, patch information for three vulnerabilities was published more than 6 months before the scans were performed.

Table 1. Total Number of High and Critical Vulnerabilities and Instances by Common Vulnerabilities and Exposures (CVEs) and Vulnerability Name

CBP Server Name	Total Number of CVEs[7]	Total Number of Unique Vulnerabilities[8]	Date of Last Vulnerability Scan Report to DHS[9]
Server 1	9	3	06/2012
Server 2	31	5	06/2012
Server 3	31	5	Not reported.
Total:	71	13	

In addition to these inconsistent SSI designations, we have encountered instances in which TSA redacted information so widely known that redaction bordered on the absurd. For instance, TSA redacted the following statement in one of our draft reports relating to expedited screening procedures because it claimed it contained SSI: "Passengers are not required to remove shoes, belts, laptops, liquids, or gels." After showing TSA that this information is publicly available on its website, TSA agreed that the information was not SSI and should not be redacted.

Similarly, TSA asked that we redact from another draft report the bolded language in the statement below:

> The program compares **self-reported** traveler information **provided to TSA from air carrier reservations, such as name, date of birth, and gender**, to lists of low risk travelers, the Terrorist Screening Database (TSDB) and Selectee Lists, as well as to other intelligence-based data systems maintained by TSA and other Federal Government Agencies.

The bolded information, however, was obtained by the OIG from the *Privacy Impact Assessment Update for Secure Flight*, dated September 4, 2013, which the Department makes publicly available.[11] The specter of TSA attempting to block the OIG from publishing information that TSA itself has made public is troubling and highlights the incoherent nature of the program.

[11] *Privacy Impart Assessment Updated for Secure Flight*, DHS/TSA/PIA-18(f) (September 2013).

These examples raise serious concerns about whether TSA can be trusted to make reasonable, appropriate, and consistent SSI designations.

TSA's Delays in Resolving Redaction Issues

We issue draft reports to the DHS components we review, including TSA, to allow for component comment prior to the publication of a final report. We find that this iterative process improves the final work product by ensuring that component concerns are considered and, if appropriate, addressed in advance of publication. For this process to succeed, however, we rely on timely responses from the components.

We often find ourselves questioning TSA's purported SSI redactions during the sensitivity review process. In such cases, we typically request that the Administrator of TSA review the SSI designations, which are made in the first instance by TSA's SSI Program Office, and make an independent assessment as to whether the designations are appropriate. The length of time it takes to get a resolution from TSA is troubling. In many cases, while awaiting resolution, we have been compelled to publish redacted reports containing SSI markings with which we disagree to meet our reporting requirements.

Our audit report concerning the information technology operations at John F. Kennedy airport is illustrative. It took nearly 6 months to get a response from TSA, as reflected in the timeline below:

- **July 22, 2014**: OIG provides draft report to the Department's Chief Information Officer with a response date of August 22, 2014.
- **August 22, 2014**: No response.
- **August 27, 2014**: DHS Chief of Staff requests an extension; extension granted until September 17, 2014.
- **September 17, 2014**: No response.
- **October 20, 2014**: TSA returns a draft of the report with several passages marked as SSI.
- **November 19, 2014**: OIG sends a formal challenge memo to TSA Administrator John Pistole contesting the SSI markings.
- **December 16, 2014**: Having received no response, the Inspector General writes to Administrator Pistole a second time to request that TSA remove the SSI designations in the report; the OIG never receives a response.

- **January 13, 2015**: The TSA SSI Program Office, which made the original SSI designations in the draft report, contacts the OIG and refuses to remove the markings, in essence affirming its own designations.

We encountered other issues with TSA more recently in connection with our airport IT capping report:

- **September 16, 2016**: OIG provides draft report to the Department's Chief Information Officer requesting agency comments, including a sensitivity review, by October 17, 2016.

- **October 11, 2016**: TSA sends its request for redactions.

- **October 14, 2016**: TSA requests an extension until October 21, 2016, to provide management comments to the draft report.

- **October 17, 2016**: OIG notifies TSA that certain of the proposed redactions relate to information that has been published in prior OIG reports; TSA responds that information regarding deficiencies over 3 years old need not be redacted.

- **October 18, 2016**: OIG sends TSA a detailed analysis of the requested redactions and requests that TSA reconsider its request for all redactions of information previously published in OIG reports (*i.e.*, not just redactions relating to deficiencies greater than 3 years old).

- **October 25, 2016**: TSA provides management comments to the draft report, which do not mention the requested redactions.

- **October 27, 2016**: TSA sends revised redactions, eliminating some, but not all, of the redactions pertaining to information previously published in OIG reports.

TSA's refusal to remove unsupportable SSI designations — including designations pertaining to previously published information — raises serious questions about its stewardship of the SSI program. None of these redactions will make us safer, and they serve to highlight the inconsistent and often arbitrary nature of TSA's SSI designations. Furthermore, improperly applied SSI designations impede my ability to keep Congress and the public "fully and currently informed," which is required under the *Inspector General Act* and key to accomplishing the OIG's critical mission.

TSA Appeals Process

Under DHS policy, any authorized holder of SSI who believes an SSI designation is improper or erroneous is encouraged to challenge the marking. Challenges can be made informally or formally. An informal challenge is made directly to the person that applied the SSI marking, who is supposed to reevaluate the SSI markings against certain criteria.[12] A formal challenge must be made in writing to the person who applied the SSI marking, or to the TSA SSI Office. Further appeals must be made first to the Director of the TSA SSI Office, and then to the TSA Assistant Secretary, whose decision is final.[13]

This appeals process is structured to ratify TSA's SSI designations and prevent review of such designations by independent, external entities. The appeals process is foreordained and fails to properly balance the public's right to information against non-speculative threats to aviation security, and it is vulnerable to abuse.

OIG Upcoming Work

We are currently in the fieldwork stage of a comprehensive review of TSA's management of its SSI program and its use of the SSI designation. . We expect to issue a final report by July 2017 and will provide a copy of the report to this Committee when it is published.

Additionally, we will continue to review and publish public reports on TSA's programs and operations. To the extent we continue to observe the abuse of the SSI designation, we will continue to highlight it.

Mr. Chairman, this concludes my testimony. I am happy to answer any questions you or other members of the committee may have.

[12] *Sensitive Security Information (SSI)*, MD Number 11065.1 (issued 11/03/2006).
[13] *Id.*