

**The TSA SSI Program  
Office's Identification and  
Redaction of Sensitive  
Security Information**





# DHS OIG HIGHLIGHTS

## *The TSA SSI Program Office's Identification and Redaction of Sensitive Security Information*

February 8, 2018

### Why We Did This Inspection

Protecting Sensitive Security Information (SSI), which can pose a risk to transportation security if released, must be balanced with ensuring transparency. Our objective was to determine whether the Transportation Security Administration (TSA) SSI Program office appropriately reviews and redacts SSI.

### What We Recommend

We made three recommendations to improve the TSA SSI Program office's review of SSI.

#### **For Further Information:**

Contact our Office of Public Affairs at (202) 254-4100, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)

### What We Found

The TSA SSI Program office has policies and procedures to identify and redact SSI. In addition, the office uses SSI Identification (ID) guides to help TSA and Department of Homeland Security personnel identify SSI. Yet, several ID guides are outdated, which could lead to improperly identifying and marking SSI. We examined 80 reviews processed by the SSI Program office and determined that the office follows policies and procedures, but the existing controls are not always effective. We identified errors in marking information for redaction. The SSI Program office resolves most challenges by stakeholders to its redactions through informal, program-level discussions, but we did not observe documentation verifying resolution of these challenges. Further, because the office does not consistently track them, the total number of challenges to redactions is unknown. TSA could improve its review and redaction process by updating the ID guides, documenting justifications for changing redactions, and tracking challenges to redactions.

### TSA Response

TSA officials concurred with all three recommendations. TSA proposed steps to update guidance, develop a tracking mechanism for redaction challenges, and document changes in position on SSI and make those changes accessible to TSA personnel. TSA also provided documentation and requested closure for Recommendation 1.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / [www.oig.dhs.gov](http://www.oig.dhs.gov)

February 8, 2018

MEMORANDUM FOR: The Honorable David Pekoske  
Administrator  
Transportation Security Administration

FROM: John V. Kelly   
Acting Inspector General

SUBJECT: *The TSA SSI Program Office's Identification and  
Redaction of Sensitive Security Information*

For your action is our final report, *The TSA SSI Program Office's Identification and Redaction of Sensitive Security Information*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving the TSA SSI Program. Your office concurred with all three recommendations. Based on information provided in your responses to the draft report, we are closing Recommendation 1. Recommendations 2 and 3 remain open and resolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response to include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendations. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions.

Please send your response or closure request to  
[OIGInspectionsFollowup@oig.dhs.gov](mailto:OIGInspectionsFollowup@oig.dhs.gov).

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Jennifer L. Costello, Assistant Inspector General for Inspections and Evaluations or Erika Lang, Chief Inspector, at (202) 254-4100.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### Background

Sensitive Security Information (SSI) is defined as information obtained or developed in conducting security activities, which if disclosed, would (1) constitute an unwarranted invasion of privacy; (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to transportation security.<sup>1</sup> There are 16 categories of SSI related to transportation security, including security programs, vulnerability assessments, threat information, security screening information, and systems security information.<sup>2</sup> The Transportation Security Administration's (TSA) SSI Program office examines material submitted by TSA program offices, Department of Homeland Security components, the Government Accountability Office (GAO), Congress, and other external entities to assess whether it contains SSI and should therefore be protected from public disclosure.

In July 2011, because of concerns about TSA's use and potential misuse of the SSI designation, the House Committee on Oversight and Government Reform began investigating how TSA identified and protected SSI. In a May 2014 report,<sup>3</sup> the committee criticized TSA's past mismanagement and alleged attempts to abuse SSI redactions, but also concluded that, following the investigation, TSA had made significant improvements to its SSI process.

In May 2016, the House Committee on Homeland Security requested that the OIG review TSA's use of the SSI designation, citing concerns that TSA was using the designation to withhold information from public scrutiny. More specifically, the committee had previously received at least two documents that were incorrectly labeled as SSI. In a December 2016 report, the DHS Inspector General expressed similar concerns to TSA about "abusing its stewardship" of the SSI Program.<sup>4</sup> In particular, he noted that TSA's redactions in the report were unjustifiable, in part because the information had already been publicly disclosed in previous Office of Inspector General (OIG) reports. The Inspector General reiterated this concern to Congress in March 2017.<sup>5</sup>

In light of these ongoing concerns, we reviewed whether the TSA SSI Program office is appropriately reviewing and redacting SSI. In this report, we examine

---

<sup>1</sup> 49 Code of Federal Regulation (CFR) § 1520.5(a)

<sup>2</sup> 49 CFR § 1520.5(b)

<sup>3</sup> *Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information (SSI) Designation*, May 29, 2014

<sup>4</sup> *Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports*, OIG-17-14, December 30, 2016

<sup>5</sup> Testimony of Inspector General John Roth Before the Committee on Oversight and Government Reform, U.S. House of Representatives, "Transparency at TSA," March 2, 2017  
[www.oig.dhs.gov](http://www.oig.dhs.gov)



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

(1) whether the TSA SSI Program office has adequate policies and procedures to identify SSI; (2) whether existing controls prevent the misidentification of SSI; and (3) challenges made to TSA's redactions and the process used to resolve such challenges.

### **Results of Inspection**

The TSA SSI Program office has policies and procedures to identify and redact SSI. In addition, the office uses SSI Identification (ID) guides to help TSA and DHS personnel identify SSI. Yet, several ID guides are outdated, which could lead to improperly identifying and marking SSI. We examined 80 reviews processed by the SSI Program office and determined that the office follows policies and procedures, but the existing controls are not always effective. We identified errors in marking information for redaction. The SSI Program office resolves most challenges by stakeholders to its redactions through informal, program-level discussions, but we did not observe documentation verifying resolution of these challenges. Further, because the office does not consistently track them, the total number of challenges to redactions is unknown. TSA could improve its review and redaction process by updating the ID guides, documenting justifications for changing redactions, and tracking challenges to redactions.

### **SSI Program Office Has Adequate Policies and Procedures But Key Guidance Is Outdated**

The SSI Program office has a number of management directives, policies, and procedures to guide employees in determining what constitutes SSI, but some critical guidance on identifying SSI needs to be updated.

Both DHS and TSA have Management Directives (MD) that broadly define TSA's responsibilities for maintaining, safeguarding, and assessing SSI.<sup>6</sup> TSA personnel are permitted to mark<sup>7</sup> material as containing SSI without submitting it to the SSI Program office. If TSA personnel wish to disclose information outside of TSA and are uncertain whether the material they wish to disclose contains SSI, they are to submit the material to the TSA SSI Program office.

For day-to-day operations, the SSI Program office has a handbook and standard operating procedures to guide its work:

---

<sup>6</sup> DHS MD 11056.1, *Sensitive Security Information* (DHS MD) and TSA Management Directive (TSA MD) 2810.1, *SSI Program*

<sup>7</sup> DHS MD 11056.1 defines mark/markings as the application of the SSI protective marking and distribution limitation statement to records containing SSI.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

- The *SSI Policies and Procedures Handbook* (SSI handbook) explains how to properly identify, mark, and protect SSI. According to the SSI handbook, when identifying information for redaction, SSI Program office personnel are to, among other actions, release as much information publicly as possible without compromising transportation security. The SSI handbook also instructs SSI Program office personnel to strive for consistency in SSI redactions, unless changes in identification guidance, security measures, technology, or other factors make it necessary to redact the record differently.
- The *Internal SSI Program Consolidated Standard Operating Procedures on Intake and Reviews* (standard operating procedures) provides detailed instructions for assessing material to determine whether it contains SSI and reviewing material to identify and redact SSI. The standard operating procedures describe collaborating with subject matter experts (SME) and reviewing previously redacted documents as essential to assessing material for SSI.

In addition to the handbook and standard operating procedures, the Chief of the SSI Program office, in coordination with the Office of Chief Counsel and the appropriate program SME, creates and updates SSI ID guides. SSI ID guides are designed to help the SSI Program office, other TSA program offices, and DHS personnel determine whether information associated with a particular TSA program office subject area is SSI. According to TSA's Enterprise Risk Management Team, these guides are "crucial in the sharing of program information across and outside [TSA]."

The SSI Program Office's standard operating procedures require SSI ID guides to be updated periodically as information and programs change; some TSA staff stated that updating them every 12 to 18 months is reasonable. However, we identified multiple SSI ID guides that have not been updated in many years. Specifically, of the 15 guides we reviewed, 10 were published between 2007 and 2014, and as of May 30, 2017, had not been updated. Of the remaining five guides, one was in draft, one was published in 2016, and three were updated between 2014 and 2016. Outdated ID guides could lead personnel to improperly identify and mark information as SSI. Appendix B contains a complete list of the SSI ID guides we reviewed.

In the absence of updated guides, TSA should at a minimum document the justification for changing its position on redactions. According to one TSA official, documenting justifications for redacting information could improve communications between TSA and its stakeholders. TSA could also use the documentation for internal use to explain SSI decisions. For example, if there is a change in the sensitivity of certain cargo screening information, the TSA



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

cargo screening program office should document the justification for its change in position. Documenting the justification for changing redactions would clarify TSA program offices' decisions and, later, foster open communication with stakeholders to alleviate confusion about redactions.

### **The SSI Program Office Follows Policies and Procedures But Existing Controls Are Not Always Effective**

The SSI Program Office's standard operating procedures include a review mechanism designed to prevent both overprotecting and improperly releasing SSI. As part of this internal control process, reviewers are to justify and explain why information should be redacted or not redacted. Although the SSI Program office generally follows this process, we identified errors in marking information for redaction.

The SSI Program Office has implemented a three-level review process to ensure the proper application of SSI redactions. First-level reviewers have the least experience, and when identifying SSI, are to describe in comments why information should be redacted. Second-level reviewers have more experience and are usually senior program analysts; they review first-level reviewers' redactions, commenting, correcting, and making additional redactions as necessary. Third-level reviewers, usually the Chief or Deputy Chief of the SSI Program office, make final decisions about whether information is SSI and should be redacted. As previously noted, reviewers collaborate with SMEs and review previously redacted information before marking documents for redaction. The reviewers also consider various factors, including the length of time since the information was first marked as SSI and the current threat environment. (Appendix C contains detailed information on these factors.)

We identified 379 reviews processed by the SSI Program office between fiscal year 2016 and February 28, 2017. We randomly selected 80 reviews and found that the reviewers generally follow this process. Specifically, we observed evidence of all three levels of review in eReview, the database used by the office as a document management system. Nevertheless, we found that the process is not always effective. Of the 80 reviews we examined, 38 reviews (comprising 56 documents) contained SSI; the remaining 42 reviews did not contain SSI. We identified errors in 8 of these 80 reviews — a 10 percent error rate.

The kinds of errors we identified can be attributed to simple human error. TSA officials acknowledge SSI personnel make mistakes. For example, in one instance an analyst redacted specific names on one page but did not redact those same names on a different page. In another example, an analyst redacted more text than necessary because the information in question was already publicly available and easily accessible through an internet search. Although



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

we did not find evidence of any attempt to hide embarrassing information through the redaction process, we would expect a lower error rate given the three levels of review.

### **The SSI Program Office Does Not Consistently Track SSI Challenges and the Total Number of Challenges Is Unknown**

The SSI Program office generally relies on an informal process to resolve most challenges from stakeholders on SSI decisions or redactions. However, the office does not have a mechanism to officially track and document challenges from initiation to resolution.

Stakeholders can challenge the TSA SSI Program office's redactions informally or formally if they believe information has been improperly or erroneously redacted. According to the SSI Program office, they resolve most challenges from stakeholders on SSI decisions and redactions through informal discussions by email, phone, or in person. The officials we spoke with reported they were satisfied with the responsiveness, professionalism, and knowledge of the SSI Program office. However, other than some email communication, the SSI Program office does not officially track or document informal discussions or resolution of challenges. If there are changes to redactions, the SSI Program office's standard is to simply update the new redactions to the document in eReview.

After informal challenge discussions, if stakeholders still disagree with the final decision of the Chief of the SSI Program office about a redaction, they may use the formal challenge process in the SSI handbook and provide a written justification for challenging the decision. These formal challenges are rare — since 2008 the SSI Program office has received only five and, according to office staff, all five were resolved. However, similar to the informal challenges, we did not find documentation to verify resolution of these formal challenges.

We did obtain internal SSI Program office tracking documents related to informal and formal challenges on reports from two entities outside of TSA that the office reviewed. The documentation was not consistent; did not identify additional challenges from other TSA stakeholders; and did not include initiation and resolution dates, the reason for the challenge, or the resolution.

Because neither the informal nor formal process is documented, we could not determine the actual number of challenges, nor assess how well the process is working. In addition, the lack of documentation related to challenges prevents the SSI Program office from analyzing its own process for lessons learned and trends.





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

### Conclusion

Overall, within the scope of this review, we did not identify any unjustifiable redactions. The TSA SSI Program office strives to consistently identify and redact SSI by following policies and procedures. Updating guidance, documenting changes in position for SSI redactions, and tracking challenges to SSI redactions are essential to strengthening the TSA SSI Program office's review and redaction process.

### Recommendations

We recommend that the SSI Program, with the oversight of the TSA Assistant Administrator for the Office of Law Enforcement/Federal Air Marshal Service:

**Recommendation 1:** Develop and implement a schedule to regularly review and update, as necessary, TSA Sensitive Security Information Identification Guides.

**Recommendation 2:** Develop a tracking mechanism for all Sensitive Security Information redaction challenges.

We recommend that the TSA Assistant Administrators assist the SSI Program to:

**Recommendation 3:** Document justifications for changes in position on Sensitive Security Information and make the changes accessible to TSA personnel for use with stakeholders as necessary.

### Management Comments and OIG Analysis

TSA concurred with all recommendations. A summary of TSA's response and our analysis follows. Appendix A contains a copy of the management comments in their entirety. TSA also provided technical comments, which we incorporated as appropriate.

**TSA Response to Recommendation 1:** TSA concurred with the recommendation. The TSA SSI Program currently has 15 SSI ID guides to assist both the program and TSA personnel in applying appropriate and consistent protections to information. TSA acknowledged that its outdated SSI ID guides may reduce clarity of current SSI designations, making TSA less efficient in its identification and review of potential SSI.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

In its formal response, TSA indicated it would identify impacted programs for all SSI ID guides and review and update guides on a 3-year cycle, pursuant to Section 525(a) of the *Department of Homeland Security Appropriations Act of 2007*, which requires periodic review of SSI determinations. On February 2, 2018, TSA provided an *SSI IDG Publication and Update Schedule*, as well as a new SSI ID guide for incidents.

**OIG Analysis:** We consider TSA's actions responsive to the intent of the recommendation. Based on our review of the information, we are closing this recommendation. No further reporting is required for this recommendation.

**TSA Response to Recommendation 2:** TSA concurred with the recommendation. The SSI Program uses a management database to manage review requests and structure controls as the SSI Program office conducts reviews for SSI. Tracking informal and formal appeals of SSI determinations will be integrated into current office operational tracking mechanisms. The SSI Program will initiate an efficiency review to determine how best to capture data elements required for long-term reporting and will include these changes in internal program procedures guidance. The estimated completion date is May 31, 2018.

**OIG Analysis:** We consider TSA's proposed actions responsive to the intent of the recommendation, which is open and resolved. We will close the recommendation pending completion of the proposed corrective actions and submission of adequate supporting documentation demonstrating TSA's long-term tracking mechanisms for informal and formal appeals.

**TSA Response to Recommendation 3:** TSA concurred with the recommendation. Currently, the SSI ID guide coordination process requires final review by the impacted Assistant Administrators and Office of Chief Counsel prior to issuance and publication. In the event of a substantial change in SSI determination prior to the scheduled review of an SSI ID guide, the SSI Program will coordinate the change with the impacted Assistant Administrators, document the justification for the change, and publish an interim update to the relevant SSI ID guide. In addition, the SSI Program will distribute the substance of the decision to TSA through a structured and consistent communications plan, conveying changes to TSA personnel through its intranet website and the SSI Coordinator network. The estimated completion date is May 31, 2018.

**OIG Analysis:** We consider TSA's proposed actions responsive to the intent of the recommendation, which is open and resolved. We will close the recommendation pending completion of the proposed corrective actions and



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

submission of adequate supporting documentation verifying TSA's communications plan for conveying changes to TSA personnel.

### **Objective, Scope, and Methodology**

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

The objective of the inspection was to determine whether the TSA SSI Program office appropriately reviews and redacts SSI.

To achieve our objective, we reviewed TSA's SSI regulations, Department of Transportation regulations, TSA and DHS Management Directives, policies, and procedures. We also reviewed:

- OIG and GAO reports;
- *Freedom of Information Act* documents;
- Responses to congressional requests;
- 15 SSI ID guides;
- 80 randomly selected reviews from the TSA SSI Program office's eReview database, analyzing redactions in each document; and
- Four fiscal years of SSI Program office document review data from FY 2014 through FY 2017 (up to February 28, 2017).

We interviewed various officials from TSA Headquarters, U.S. Customs and Border Protection, U.S. Coast Guard, Federal Emergency Management Agency, DHS GAO-OIG Liaison office, GAO, and the Department of Transportation.

We conducted this review between January and June 2017 under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

The Office of Inspections and Evaluations' major contributors to this report are Erika Lang, Chief Inspector; LaDana Crowell, Lead Inspector; Anthony Crawford, Intelligence Officer; Ryan Nelson, Senior Inspector, Kimberley Crabbe, Inspector; Adam Robinson, Inspector; Samuel Tunstall, Inspector; Kelly Herberger, Communications and Policy Analyst; and Stephanie Christian, Independent Referencer.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Appendix A**  
**TSA Comments to the Draft Report**

U.S. Department of Homeland Security  
601 South 12th Street  
Arlington, VA 20598



**Transportation  
Security  
Administration**

JAN 18 2018

MEMORANDUM FOR: John V. Kelly  
Acting Inspector General  
U.S. Department of Homeland Security

FROM: David P. Pekoske  
Administrator  
Transportation Security Administration

SUBJECT: Management's Response to DHS OIG Draft Report:  
*"The TSA SSI Program Office's Identification and  
Redaction of Sensitive Security Information,"* Project No. 17-011-  
ISP-TSA

Thank you for the opportunity to review and comment on the subject draft report. The Transportation Security Administration (TSA) appreciates the efforts of the Department of Homeland Security (DHS) Office of Inspector General (OIG) in planning and conducting this review, and issuing this report.

The TSA Sensitive Security Information (SSI) Program serves as the principal point of contact for DHS to implement all laws and regulations regarding the development, maintenance, safeguarding, and disclosure of SSI. In order for TSA to effectively execute its security mission, information is shared with industry partners and stakeholders, with appropriate safeguards in place. TSA takes the identification and protection of SSI very seriously, as protecting critical information is essential to our Nation's transportation systems.

The core mission of the SSI Program is to properly protect SSI and guard against over or under protection. The SSI Program manages this task through training and outreach programs to communicate program requirements and updates to TSA employees and stakeholders. To that end, the SSI Program has trained and certified over 1,000 SSI Coordinators over the past 9 years, and currently supports over 450 SSI Coordinators throughout TSA and SSI Program Managers at other DHS Components. With the help of this substantial network, TSA's 12-member SSI Program staff supports the entire Department and stakeholder community in the consistent identification and protection of sensitive information in the interest of transportation security. Notably, the SSI Program is relied upon to review more than 500,000 pages in over 1,200 review requests annually, supporting Freedom of Information Act (FOIA), litigation, and other operational needs for TSA, DHS, and the larger stakeholder community. The Agency has further controls in place to ensure accuracy, to include Office of Chief Counsel review of FOIA or litigation redactions before release.



# OFFICE OF INSPECTOR GENERAL

## Department of Homeland Security

---

## Appendix A

### TSA Comments to the Draft Report

#### Background

In his cover letter to a report issued in December 2016 (OIG-17-14, “Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports”), then-Inspector General John Roth raised concerns about TSA’s application of the SSI Regulation and specifically about TSA’s redactions. However, during the course of this most recent review, the OIG reported it “did not find evidence of any attempt to hide embarrassing information through the redaction process” and the “office strives to consistently identify and redact SSI by following policies and procedures.”

In this report, OIG found that the SSI Program has policies and procedures to identify and redact SSI and SSI Identification (ID) guides to help TSA and DHS personnel identify SSI. OIG determined that the SSI Program office follows policies and procedures, but the existing controls are not always effective and a number of ID guides are outdated, which could lead to improperly identifying and marking SSI. OIG identified an unqualified and unquantified number of errors in marking information for redaction within eight of the 56 documents it reviewed containing SSI markings. Additionally, the SSI Program office resolves most challenges by stakeholders to its redactions through informal, program-level discussions, but OIG did not observe documentation verifying resolution of these challenges. Further, because the office does not have a structured process to track them, the total number of challenges to redactions is unknown. TSA could improve its review and redaction process by updating the ID guides, documenting justifications for changing position on SSI determinations, and tracking challenges to redactions. To address these findings, OIG made three recommendations and TSA concurred on all three.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

## **Appendix A**

### **TSA Comments to the Draft Report**

#### **TSA's Response to OIG Recommendations**

TSA concurs with all three OIG recommendations and will implement each in a timely fashion. The SSI Program welcomes these recommendations as an opportunity to improve the service it provides and reaffirm its responsibility to uphold the public trust. Below is TSA's response to each recommendation in the OIG draft report.

**Recommendation 1:** We recommend that the TSA Assistant Administrator for the Office of Law Enforcement/Federal Air Marshal Service develop and implement a schedule to regularly review and update, as necessary, TSA Sensitive Security Information Identification Guides.

**Response: Concur.** As noted in the report, the SSI Program currently has 15 SSI Identification (ID) Guides to assist both the program and TSA personnel in applying appropriate and consistent protections to information. These SSI ID Guides govern many programs across TSA and a number of the guides apply to multiple TSA programs. The inspection team made reference to outdated SSI ID Guides. TSA acknowledges the outdated guidance may reduce clarity of current SSI designations, making the Agency less efficient in its identification and review of potential SSI.

The Agency has begun to identify impacted programs for all SSI ID Guides, and will memorialize the review and update of guides on a three-year cycle, pursuant to Section 525(a) of the Department of Homeland Security Appropriations Act, 2007, as reenacted, which requires periodic review of SSI determinations. Four SSI ID Guides are in the late stages of development and approval, including: revisions to the National Explosives Detection Canine Team Program, Prescreening Procedures, and Airport Security Cameras guides, and a new guide addressing Incidents.

The estimated completion date (ECD) is January 31, 2018.

**Recommendation 2:** We recommend that the TSA Assistant Administrator for the Office of Law Enforcement/Federal Air Marshal Service develop a tracking mechanism for all Sensitive Security Information redaction challenges.

**Response: Concur.** The SSI Program currently has a robust workflow management database to manage review requests and structure controls as they conduct reviews for SSI. Tracking informal and formal appeals of SSI determinations will be integrated into current office operational tracking mechanisms. The SSI Program will initiate an efficiency review to determine how best to capture data elements required for long-term reporting and will include these changes in internal program procedures guidance.

The ECD is May 31, 2018.

**Recommendation 3:** We recommend that the TSA Assistant Administrators document justifications for changes in position on Sensitive Security Information and make the changes accessible to TSA personnel for use with stakeholders as necessary.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### Appendix A

### TSA Comments to the Draft Report

**Response: Concur.** Currently, the SSI ID Guide coordination process requires final review by the impacted Assistant Administrators and Office of Chief Counsel prior to issuance and publication. In the event of a substantial change in SSI determination prior to the scheduled review of an SSI ID Guide, the SSI Program will coordinate the change with the impacted Assistant Administrators, document the justification for the change, and publish an interim update to the relevant SSI ID Guide. In addition, the SSI Program will distribute the substance of the decision to TSA through a structured and consistent communications plan, conveying changes to TSA personnel through its Intranet website and the SSI Coordinator network.

The ECD is May 31, 2018.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Appendix B**  
**Fifteen SSI Identification Guides**

<b>SSI Program Identifications Guide</b>	<b>Date of Initial Publication</b>	<b>Date of Change/ Updates</b>
<b>TSA Cargo Security</b> <i>SSIIDG 0050 Version 1.0</i>	<b>May 2007</b>	No further update as of May 30, 2017
<b>Foreign Airport Assessment Program and Other International Transportation Security</b> <i>SSIIDG 0073 Version 1.0</i>	<b>June 21, 2012</b>	No further update as of May 30, 2017
<b>Screening Passengers by Observational Techniques</b> <i>SSIIDG 0057A Version 3.0</i>	<b>April 11, 2011</b>	No further update as of May 30, 2017
<b>Vetting and Credentialing</b> <i>SSIIDG 0056 Version 1.0</i>	<b>March 1, 2007</b>	No further update as of May 30, 2017
<b>TSO Certification and Testing</b> <i>SSIDG 12-01 Version 1.0</i>	<b>November 3, 2011</b>	No further update as of May 30, 2017
<b>National Explosives Detection Canine Team</b> <i>SSIDG 0009 Version 1.1</i>	<b>June 3, 2011</b>	No further update as of May 30, 2017
<b>Prescreening Procedures</b> <i>SSIIDG 0055 Version 1.5</i>	<b>August 14, 2008</b>	No further update as of May 30, 2017
<b>Access Control</b> <i>SSIIDG 009 Version 2.0</i>	<b>September 5, 2007</b>	<b>February 9, 2016 (Version 2.0)</b>
<b>Aircraft Operator and Crew Security Program</b> <i>SSIIDG 005 Version 2.0</i>	<b>May 2007</b>	<b>January 30, 2015 (Version 2.0)</b>
<b>Airport Security Cameras</b> <i>SSIIDG 13-004 Version 1.0</i>	<b>April 16, 2013</b>	No further update as of May 30, 2017
<b>Checkpoint and Checked Baggage Screening</b> <i>SSIIDG 0010 Version 1.0</i>	<b>September 28, 2016</b>	No further update as of May 30, 2017
<b>FAMS AIR and Grounds-Based Mission</b> <i>SSIIDG 13-001 Version 1.0</i>	<b>June 10, 2013</b>	No further update as of May 30, 2017
<b>Pipeline Security Program</b> <i>SSIIDG 002 Version 1.0</i>	<b>April 30, 2014</b>	No further update as of May 30, 2017
<b>Transportation Sector Security Risk Assessment</b> <i>SSIIDG 003 Version 1.1</i>	<b>April 16, 2013</b>	<b>April 30, 2014 (Version 1.1)</b>
<b>Incidents</b> <i>SSIIDG 008 Version 1.0 (Draft)</i>	<b>February TBD, 2016</b>	No further update as of May 30, 2017





## **Appendix C**

### **Examples of Factors Impacting SSI Redactions**

#### **Three Year Rule**

According to the TSA MD and DHS MD, SSI that is 3 years old or older shall be released upon request unless the information meets specific criteria. For example, information that was once considered SSI several years ago may now be public knowledge. Therefore, TSA has no reason to continue protecting the information and will release it unless there are reasons to continue protection.

#### **Comparison Information**

Comparison information identifies common deficiencies at multiple locations that reveal vulnerability, leading an adversary to choose one location over another. If this is the case, the SSI Program office may identify the comparison information as SSI. For example, a document may show that location A has seven broken doors and location B has two. Separately, either piece of information may not be SSI, but when comparing the same deficiency at both locations, the information shows location A is more vulnerable than location B. The TSA SSI Program office may redact the number of broken doors for both locations because of one location's vulnerability over another.

#### **Aggregate Information**

The release of aggregate information regardless of individual content may reveal systemic vulnerabilities. If an adversary were to employ analytic techniques to compile information, they could exploit potential weaknesses within critical locations. One TSA official said that because there are multiple layers of security, a deficiency in one layer may not reveal vulnerability, but more than one deficiency could. For example, the door to the computer room in location A is broken, and security guards patrol location A from 8:00 a.m. to 5:00 p.m. — by combining the information, an adversary could attempt to access the computer room at location A after 5:00 p.m.

#### **Threat Environment**

SSI Program officials conduct risk based assessments of the current threat environment and may choose to protect different information at different times. These changes may be due to advancements in technology, threats to cybersecurity, and updates to transportation security systems. If released, this information exposes TSA program vulnerabilities.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Appendix D**  
**Report Distribution**

**Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chiefs of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
Under Secretary for Management  
Office of the Chief Security Officer  
TSA Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

**External**

Office of the Secretary of Transportation

## **Additional Information and Copies**

To view this and any of our other reports, please visit our website at:  
[www.oig.dhs.gov](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General  
Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov).  
Follow us on Twitter at: @dhsoig.



### **OIG Hotline**

To report fraud, waste, or abuse, visit our website at [www.oig.dhs.gov](http://www.oig.dhs.gov) and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security  
Office of Inspector General, Mail Stop 0305  
Attention: Hotline  
245 Murray Drive, SW  
Washington, DC 20528-0305