OFFICE OF INSPECTOR GENERAL

Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports (Redacted)

Homeland Security

December 30, 2016

OIG-17-14

DHS OIG Highlights

Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports

December 30, 2016

Why We Did This Audit

We previously reported on deficiencies regarding security controls for the Transportation Security Administration's (TSA) information technology (IT) systems at airports. This report summarizes the previous reports and analyzes the effectiveness of TSA's actions to implement improved IT security policies at these critical sites.

What We Recommend

We are making two recommendations to improve security controls for TSA's IT systems at airports.

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

What We Found

Our previous reports identified numerous deficiencies in security controls for TSA's IT systems and equipment at airports. These deficiencies included inadequate physical security for TSA server rooms at airports, unpatched software, missing security documentation, and incomplete reporting of IT costs. TSA has undertaken various actions to address the recommendations we made in these reports. Based on our review of the corrective actions taken as of May 2016, we consider most of the recommendations resolved and closed.

However, TSA has not yet resolved recommendations we made in two key areas. TSA officials indicate it will take time, money, and contract changes to include security requirements in the Security Technology Integrated Program, a data management system that connects airport screening equipment to servers. TSA also disagrees that closed-circuit televisions, including cameras, at airports constitute IT equipment and that TSA is responsible for maintaining them.

Further, as a result of our analysis to compile this report, we are making two new recommendations to improve security controls for TSA's IT systems at airports. Specifically, TSA needs to assess the risk of not having redundant data communications capability to sustain operations at airports in case of circuit outages. Additionally, while TSA has undertaken reviews of security controls for its IT systems at airports, it would benefit from establishing a plan to conduct the reviews on a recurring basis nationwide.

Agency Response

TSA concurred with both our recommendations. These two recommendations are considered resolved and open.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

December 30, 2016

MEMORANDUM FOR: The Honorable Peter Neffenger
Administrator
Transportation Security Administration

FROM: John Roth
Inspector General

SUBJECT: *Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports*

Attached for your information is our final report, *Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports.* This report contains findings and recommendations for improving management and security controls for Transportation Security Administration's (TSA) information technology systems at airports.

I must lodge an objection regarding the way that TSA has handled information in the report it considered Sensitive Security Information (SSI). Specifically, we issued the draft report, *Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports,* to the Department on September 16, 2016. Pursuant to the *Department of Homeland Security Directive 077-01, Follow-Up and Resolution for Office of Inspector General Report Recommendations,* we asked for agency comments, including a sensitivity review, within 30 days of receipt of the draft. On October 7, 2016, the Chief of the SSI Program provided the results of its sensitivity review, marking as SSI various passages in the report.

The redactions are unjustifiable and redact information that had been publicly disclosed in previous Office of Inspector General (OIG) reports. I am challenging TSA's proposed redactions to our summary report based on the following:

- On page 5 of the Dallas Ft. Worth audit report, *Audit of Security Controls for DHS Information Technology Systems at Dallas/Ft.*

Worth International Airport (OIG-14-132, September 5, 2014), we reported that 12 server rooms we reviewed showed warning lights signaling that batteries needed to be replaced or were being bypassed. On page 7 of the same report, we listed the temperature and humidity readings for the 12 server rooms. TSA did not mark this information as SSI in the Dallas/Ft. Worth audit report, but has opted to redact this same information on page 8 of our draft summary report.

- In our report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*, (OIG-15-18, January 7, 2015), we discussed TSA's fire protection systems in airport server rooms. A table on page 9 of the report listed the server rooms by name and terminal location. Again, TSA did not redact this information in the John F. Kennedy audit report, but has marked this same information as SSI on page 9 of our draft summary report.

- On page 21 of our draft summary report, TSA has requested redacting average high vulnerabilities we reported at San Francisco International Airport, based on a vulnerability assessment scan that we performed on servers at the airport. However, in the prior report, *Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport*, (OIG-15-88, May 7, 2015) we listed on page 21, table 5, the servers and number of high vulnerabilities, as well as the number of critical high vulnerabilities. TSA did not redact this information in the prior report.

- TSA is requesting that the words "TSA is Not Scanning STIP Servers" on page 24 of the draft summary report be classified as SSI for three specific airports. However, TSA is not requesting the same redactions for the John F. Kennedy, San Francisco, and Orlando airports listed on the same page. Moreover, we previously publicly reported that TSA was not scanning STIP servers for technical vulnerabilities, without TSA's objection.[1]

- TSA is requesting that the number of deficiencies identified on pages 8 and 9 of our draft summary report regarding server and telecommunications rooms at Dallas Ft. Worth, John F.

[1] *IT Management Challenges Continue in TSA's Security Technology Integrated Program*, OIG-16-87 (May 9, 2016).

Kennedy, San Francisco, and Orlando airports be classified as SSI. However TSA is not requesting that similar information be redacted for the Washington Dulles, Ronald Reagan, Los Angeles, Chicago O'Hare, and Hartsfield-Jackson Atlanta airports on the same pages.

- On page 52 of our draft summary report, TSA is requesting that we redact information on whether technical control issues existed at the John F. Kennedy, San Francisco, and Orlando airports. However, TSA is not requesting that comparable information be redacted for all of the other airports listed in the same table.

I can only conclude that TSA is abusing its stewardship of the SSI program. None of these redactions will make us safer and simply highlight the inconsistent and arbitrary nature of decisions that TSA makes regarding SSI information. This episode is more evidence that TSA cannot be trusted to administer the program in a reasonable manner.

This problem is well-documented. In addition to my previous objection to the handling of one of our reports,[2] the House Committee on Oversight and Government Reform in 2014 issued a bipartisan staff report finding that TSA had engaged in a pattern of improperly designating certain information as SSI in order to avoid its public release because of agency embarrassment and hostility to Congressional oversight.[3] As recently as a hearing held this summer, Chairman Katko of the Committee on Homeland Security, Subcommittee on Transportation Security, stated 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."[4] In response to a request from House Homeland Security Committee Chairman McCaul, Transportation Security Subcommittee Chairman Katko, and Oversight and Management Efficiency Subcommittee Chairman Perry, the OIG has

---

[2] *Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport*, OIG-15-18 (January 2015).
[3] 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).
[4] Hearing, *How Pervasive is Misconduct at TSA: Examining Findings from a Joint Subcommittee Investigation.* July 7, 2016.

initiated a review of TSA's management and use of the SSI designation. We expect to issue our final report in the summer of 2017.

Inconsistently and inappropriately marking information in our reports as SSI impedes our ability to issue reports to the public that are transparent without unduly restricting information, which is key to accomplishing our mission and required under the *Inspector General Act*. In order to meet our timeliness requirements, we are publishing this report with the redactions as requested. However, this letter serves as our formal direct appeal to the Administrator of TSA to remove the above-listed redactions.

We have incorporated in our final report TSA's formal comments. The report contains two recommendations aimed at improving security controls for TSA's information technology systems at airports. Your office concurred with both recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolution for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Based on information provided in your response to the draft report, we consider both recommendations resolved and open. Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered open.

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

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4100.

Attachment

Table of Contents

Background 3

Results of Audits 5

TSA's Operational Controls for IT Systems 6

TSA's Technical Controls for IT Systems 19

TSA's Management Controls for IT Systems 28

Summary and Status of Prior OIG Recommendations to TSA.....39

Recommendations.....41

Appendixes

Appendix A: Objective, Scope, and Methodology 43
Appendix B: Agency Comments to the Draft Report 45
Appendix C: Previous Audit Reports on Security Controls of TSA's IT Systems at Airports 47
Appendix D: TSA IT Systems at Selected U.S. Airports 49
Appendix E: TSA Operational Controls Issues 51
Appendix F: TSA Technical Controls Issues.....52
Appendix G: TSA Management Controls Issues 53
Appendix H: April 15, 2016 Memo to TSA Administrator 54
Appendix I: Open TSA Airport IT Security Recommendations 60
Appendix J: Office of IT Audits Contributors to This Report 69
Appendix K: Report Distribution 70

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

Abbreviations

ATL	Hartsfield-Jackson Atlanta International Airport
BIA	business impact analysis
CCTV	closed-circuit television
CIO	Chief Information Officer
CPIC	capital planning and investment control
DCA	Ronald Reagan Washington National Airport
DC1	Data Center 1
DC2	Data Center 2
DFW	Dallas/Fort Worth International Airport
EUC	Enterprise User Computing
FAMSNET	Federal Air Marshall Services Network
ICS	Infrastructure Core Services
IAD	Washington Dulles International Airport
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
IT	information technology
JFK	John F. Kennedy International Airport
LAX	Los Angeles International Airport
MCO	Orlando International Airport
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORD	Chicago O'Hare International Airport
OSC	Office of Security Capabilities
POA&M	plan of action and milestones
SFO	San Francisco International Airport
SOC	security operations center
SOO	Statement of Objective
STIP	Security Technology Integrated Program
TSA	Transportation Security Administration
TSANet	TSA Network
TSE	transportation security equipment
UPS	uninterruptible power supply

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Background

In the aftermath of the 9/11 attacks, the Transportation Security Administration (TSA) was created to address the need to strengthen the security of the Nation's transportation systems. TSA provides the resources and capabilities needed to ensure security across all transportation modes, screen all commercial airline passengers and baggage, and support the freedom of movement of people and commerce. TSA security operations are ongoing 365 days a year across roughly 440 federally-regulated airports. On any given day, TSA and its industry partners secure about 1.8 million passengers, 1.2 million checked bags, 3 million carry-on bags, and 8.4 million pounds of cargo on approximately 25,000 flights.

TSA interacts with various stakeholders as partners in aviation security and recognizes the impact its decisions can have on them. These stakeholders typically have a variety of competing priorities that must be balanced to achieve maximum efficiency and effectiveness. Stakeholders include:

- Passengers: Technology acquisitions must balance security considerations against passenger experience and operational efficiency. For example, checkpoint security, which utilizes a combination of technologies to screen passengers and their carry-on baggage, contributes to the overall passenger experience and is often the primary factor influencing public perception of TSA.
- Airports: Because TSA does not own airport infrastructure, TSA considers both airport footprint and installation requirements when analyzing transportation security equipment (TSE) for acquisition and deployment. Specifically, TSA must coordinate with airports and assess the impact, across varying physical layouts, of planned changes to checkpoint and checked baggage technologies.
- Airline Groups and Air Carriers: TSA's actions affect the customer's flying experience and perception, as well as airline operations.

Since 2007, we have conducted a series of audits of the security controls for IT systems supporting homeland security operations of the following DHS components at selected major U.S. airports: Management Directorate, TSA, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the United States Coast Guard. The nine airports audited were Dulles International Airport (IAD), Ronald Reagan Washington International Airport (DCA), Chicago O'Hare International Airport (ORD), Hartsfield-Jackson International Airport (ATL), Dallas-Fort Worth International Airport (DFW), John F. Kennedy International Airport (JFK), Los Angeles

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

International Airport (LAX), San Francisco International Airport (SFO), and Orlando International Airport (MCO).[1] We audited IAD twice, producing two separate reports. See appendix C for a list of the total 10 reports resulting from our security control audits of component systems at these airports.

During our audits of IT systems used at the airports, we examined three security control areas:

- Operational Controls – Mechanisms primarily implemented and executed by people. For example, operational controls include physical access controls that restrict the entry and exit of personnel from an area, such as an office building, data center, or room, where sensitive information is accessed, stored, or processed.

- Technical Controls – Security controls executed by information systems. These controls provide automated protection from unauthorized access, facilitate detection of security violations, and support information technology (IT) applications and data security requirements. Technical controls include system passwords and protection against malware.

- Management Controls – Strategies for managing system security controls and system risk. Management controls include performing risk assessments, developing rules of behavior, ensuring that security is an integral part of both system development and IT procurement processes, as well as conducting capital planning and investment control (CPIC).

In the 10 reports resulting from this prior work, we included recommendations for improvement addressed to the various components.

We are issuing this summary report to highlight significant issues and trends that we have found over the years regarding security controls for IT systems at the selected airports. Although we examined security controls for IT systems of multiple DHS components, we focused this summary report on TSA controls alone. We justify this approach given TSA's overarching responsibility for transportation security, as well as the prevalence and nature of the TSA security control deficiencies we identified in our individual audits. See appendix D for details on the IT systems used by TSA at the airports reviewed.

The objective of this summary project was to determine whether reported

[1] We audited MCO as part of our cross-cutting assessment and report on TSA's Security Technology Integrated Program, a data management system that connects airport screening equipment to servers.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

operational, management, and technical security control vulnerabilities for TSA's IT systems have increased or decreased over time. We also sought to determine whether TSA's actions to resolve the reported deficiencies have been effective and addressed underlying causes. Based on our summary analysis, we are making additional recommendations for improvement to the TSA Administrator.

Results of Audits

Our previous reports identified numerous deficiencies in security controls for TSA's IT systems and equipment at airports. These deficiencies included inadequate physical security for TSA server rooms at airports, unpatched software, missing security documentation, and incomplete reporting of IT costs. TSA has undertaken various actions to address the recommendations we made in these reports. Based on our review of the corrective actions taken as of May 2016, we consider most of the recommendations resolved and closed.

However, TSA has not yet resolved recommendations we made in two key areas. TSA officials indicate it will take time, money, and contract changes to include security requirements in the Security Technology Integrated Program (STIP), a data management system that connects airport screening equipment to servers. TSA also disagrees that closed-circuit televisions, including cameras, at airports constitute IT equipment and that TSA is responsible for maintaining them.

Further, as a result of our analysis to compile this report, we are making two new recommendations to improve security controls for TSA's IT systems at airports. Specifically, TSA needs to assess the risk of not having redundant data communications capability to sustain operations at airports in case of circuit outages. Additionally, while TSA has undertaken reviews of security controls for its IT systems at airports, it would benefit from establishing a plan to conduct the reviews on a recurring basis nationwide.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

TSA's Operational Controls for IT Systems

We previously reported on six types of operational control deficiencies at TSA server rooms and communications closets containing IT equipment at airports and nearby TSA and Federal Air Marshal Service facilities.

- inadequate physical security controls,
- inadequate environmental controls,
- inadequate housekeeping,
- inadequate fire protection,
- deficiencies in uninterruptible power supply (UPS) capabilities, and
- a lack of redundant data circuits.

Appendix E provides a matrix summarizing operational control deficiencies identified across the airports reviewed.

In summary, TSA has taken several actions to resolve the various operational control deficiencies identified. For example, TSA has performed technical vulnerability audits at selected airports around the country. In calendar year 2011, TSA performed these internal audits at 21 airports. The objective of these internal TSA audits was to validate the existing IT security controls and determine their effectiveness and compliance with TSA and DHS policies and mandates. These TSA internal audits also resulted in reports containing recommendations for improving operational control deficiencies. Specifically, identified vulnerabilities and corresponding Plans of Action and Milestones (POA&Ms) with an "Open" status have been submitted to TSA's Continuous Diagnostic and Mitigation Team and associated Information System Security Officers for remediation and awareness.

TSA's technical vulnerability audits focused on locations associated with the Transportation Security Administration Network (TSANet), Infrastructure Core Services (ICS), and End User Computing (EUC) systems. As such, they did not evaluate controls at airport locations involving STIP and Federal Air Marshall Services Network (FAMSNet) servers and switches.[2]

[2] The STIP program, a joint effort co-funded by the Passenger Screening Program and Electronic Baggage Screening Program, is a TSA-wide enterprise system that delivers data from passenger and baggage screening security technologies (in a common format) to facilitate data interchange/exchange through a single network for effective communication and metrics reporting.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

According to TSA staff, the local TSA Federal Security Directors assign a local point of contact the responsibility for ensuring the environment and physical security controls for TSANet and FAMSNet areas are compliant with the DHS guidance. Additionally, in response to our audit of operational controls at MCO (OIG-15-88), TSA plans to perform an inventory of all airport locations where STIP IT equipment is located to ensure they have adequate physical and environmental controls.

Although TSA actions have adequately resolved and closed most of our operational control recommendations, we still have concerns in two areas. Our primary concern is that TSA has not completely addressed operational control deficiencies in airport areas containing STIP IT equipment. Additionally, we are concerned that TSA has accepted the increased risk of a loss of system availability at some airports without a complete understanding of the service disruption impact on its operations.

The following subsections provide a recap of our findings in the six operational control areas for IT systems at the airports reviewed.

Physical Security Controls

Unauthorized access and storage can create manifold problems in rooms designated solely for IT equipment operations. According to the *DHS Sensitive System Policy Directive 4300A*, v12.01, issued February 2016:

> Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.

We identified physical security deficiencies from 8 of our 10 audits of security controls for TSA's IT systems at airports. Table 1 provides examples of physical security deficiencies we identified at each airport audited.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Table 1. Physical Security Deficiencies

Airport	OIG Report	Physical Security Deficiencies
IAD	OIG-07-25, January 2007	• Deficiencies were identified in 2 of 8 (25%) server and telecommunications rooms evaluated. • TSA data communications assets were in a shared space accessible to other tenants in the building. • No TSA visitor log was maintained in the shared communications room. • No TSA camera was in place to monitor one entrance to its server room.
DCA	OIG-07-44, May 2007	• Deficiencies were identified in 4 of 6 (67%) server and telecommunications rooms evaluated. • Cabinets were not locked to prevent unauthorized access to TSA routers.
LAX	OIG-09-01, October 2008	• Deficiencies were identified in 2 of 6 (33%) server and telecommunications rooms evaluated. • A switch and a server in the TSA telecommunications room were not secured in a locked cabinet. • A TSA switch in another room was not secured in a locked cabinet.
IAD	OIG-09-66, May 2009	• Deficiencies were identified in 3 of 12 (25%) server and telecommunications rooms evaluated. • Telecommunications equipment in the basement of a commercial office building was not secured in a locked cabinet and therefore was accessible to anyone entering the building. • The door to the telecommunications room was held open with a trash can. • A workstation adjacent to a TSA passenger screening exit area was not properly secured.
ORD	OIG-12-45, March 2012	• No deficiencies were identified among the 25 server and telecommunications rooms evaluated.
ATL	OIG-13-104, July 2013	• No deficiencies were identified among the 19 server and telecommunications rooms evaluated.
DFW	OIG-14-132, September 2014	• Deficiencies were identified in [redacted] server and telecommunications rooms evaluated. • Two STIP server rooms were used as airline employee break rooms and contained non-DHS refrigerators, microwaves, and TVs. • Server racks were used to store blankets and provide electrical power. • One room door lock was disabled with duct tape.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Airport	OIG Report	Physical Security Deficiencies
JFK	OIG-15-18, January 2015	• Deficiencies were identified in [redacted] server and telecommunications rooms evaluated. • [redacted] TSA telecommunications rooms contained locked DHS equipment cabinets in a shared room with non-DHS IT equipment. • TSA was unable to change door locks to 12 of the 21 (57%) telecommunications rooms. • Some rooms contained unsecured TSA equipment accessible to non-DHS individuals. • A door to a secure room was propped open to vent a portable air conditioning unit. • No visitor logs were maintained in TSA's telecommunications rooms.
SFO	OIG-15-88, May 2015	• Deficiencies were identified in [redacted] server and telecommunications rooms evaluated. • Some TSA telecommunications racks were not completely enclosed. • Non-TSA equipment was located in some TSA racks.
MCO	OIG-16-87, May 2016	• Deficiencies were identified in [redacted] server and telecommunications rooms evaluated. • Some STIP switches in a shared space were not secured in a locked cabinet.

Source: Office of Inspector General (OIG)-compiled based on data from previous reports

Physical security vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data. For example, unauthorized access to TSA server rooms may result in the loss of IT processing capability to screen passengers and baggage for departing flights.

TSA has resolved our eight report recommendations concerning physical security deficiencies at specific airports. TSA's scheduled internal audits to identify physical security deficiencies at 19 of 440 (4 percent) airport locations containing TSANet, ICS, EUC, and STIP IT assets help address our concerns in this area. Except for one resolved but open recommendation from our recently published MCO report, we consider our other seven recommendations in this area to be resolved and closed.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Environmental Controls

DHS 4300A Sensitive Systems Handbook specifies temperature and humidity ranges allowed in rooms containing IT equipment. We reported environmental control issues related to server room temperature and humidity levels for TSA IT systems at 8 of the 9 (89 percent) locations audited. We identified these environmental control deficiencies based on the temperature and humidity ranges in effect at the time of the individual audits. Specifically, according to *DHS 4300A Sensitive Systems Handbook,* v 9.1, temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit while humidity levels should remain between 35 percent and 65 percent. Table 2 provides examples of the environmental control deficiencies we identified at airport locations audited.

Table 2. Environmental Control Deficiencies Reported

Airport	OIG Report	Environmental Control Deficiencies
IAD	OIG-07-25, January 2007	• No temperature sensor found in the server room evaluated. • Temperature readings were not recorded.
DCA	OIG-07-44, May 2007	• No temperature sensor found in the server room evaluated. • Temperature readings were not recorded.
LAX	OIG-09-01, October 2008	• Temperature of 76.7° Fahrenheit in 1 of 2 (50%) server rooms evaluated exceeded DHS standards.
IAD	OIG-09-66, May 2009	• Despite a temperature sensor located in the server room evaluated, temperature readings were not recorded.
ORD	OIG-12-45, March 2012	• Average relative humidity reading of 25.8% in all seven server rooms evaluated was noncompliant with DHS guidance. • Average temperature reading of 73.5° Fahrenheit in 6 of 7 (86%) server rooms evaluated was noncompliant with DHS guidance.
ATL	OIG-13-104, July 2013	• No humidity sensor found in the server room evaluated.
DFW	OIG-14-132, September 2014	• Temperature readings were noncompliant with DHS guidance in all 12 server rooms evaluated.
JFK	OIG-15-18, January 2015	• 13 of 21 (62%) server and telecommunications rooms evaluated did not contain temperature sensors. • 2 of 8 (25%) server and telecommunications rooms evaluated that had temperature sensors with temperature readings greater than the accepted DHS range.
SFO	OIG-15-88, May 2015	• Temperature readings exceeded DHS guidance in 6 of 8 (75%) server rooms evaluated. • The average temperature in the 6 server rooms evaluated was 73.1° Fahrenheit.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

MCO	OIG-16-87, May 2016	• We identified no environmental control deficiencies at MCO.

Source: OIG-compiled based on data from previous reports

However, version 12 of *DHS 4300A Sensitive Systems Handbook*, dated November 2015, reset the environmental requirements to higher levels. Based on the updated requirements, the dry bulb temperature range became 64.4 to 80.6 degrees Fahrenheit.[3] The dewpoint range became 41.9 degrees Fahrenheit to 60 percent relative humidity and dewpoint 59 degrees Fahrenheit in server rooms. Based on this updated guidance, only 1 of the 28 (3.6 percent) server rooms would have been noncompliant.

According to the *DHS 4300A Sensitive Systems Handbook*, v12.0:

> While many systems will continue to function when temperatures and humidity are beyond this range, the associated risk to data is increased.
>
> Humidity levels below those recommended may result in static; high temperatures may damage sensitive system elements.

TSA has resolved our five report recommendations concerning environmental control deficiencies at specific airports. Additionally, TSA's audits to identify environmental control deficiencies at airport locations containing TSANet, ICS, and EUC IT assets help address this issue. We consider the five recommendations in this area to be resolved and closed.

Housekeeping Deficiencies

Housekeeping is another important area to monitor. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, section 4.2.1.9, housekeeping considerations include weekly dusting of hardware and vacuuming of work areas and trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware. Further, cleaning supplies may include hazardous and potentially explosive substances that should not be stored inside of computer rooms.

We identified various housekeeping issues related to housing TSA IT equipment at over half (6 of 10) of the airport locations that we audited. Table 3 provides

[3] According to the *DHS 4300A Sensitive Systems Handbook,* v12.0, the ranges are specified in terms of ambient temperature, registered by a dry bulb thermometer, which is identical to the temperature of the air. The dew point is the temperature at which a parcel of air becomes saturated when cooled at constant pressure and constant water-vapor content.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

examples of the housekeeping deficiencies we reported from these audits.

Table 3. Housekeeping Deficiencies Reported

Airport	OIG Report	Housekeeping Deficiencies
IAD	OIG-07-25, January 2007	• No deficiencies were identified among the 9 server and telecommunications rooms evaluated.
DCA	OIG-07-44, May 2007	• Deficiencies were identified in 1 of 6 (17%) server and telecommunications rooms evaluated. • An area by one telecommunications cabinet was used for general storage.
LAX	OIG-09-01, October 2008	• Deficiencies were identified in 1 of 7 (14%) server and telecommunications rooms evaluated. • A server room was used to store new equipment, as well as old equipment prior to disposal.
IAD	OIG-09-66, May 2009	• Deficiencies were identified in 1 of 12 rooms (8%) server and telecommunications rooms evaluated. • A local area network room contained excess IT equipment and boxes.
ORD	OIG-12-45, March 2012	• No deficiencies were identified among the 25 server and telecommunications rooms evaluated.
ATL	OIG-13-104, July 2013	• Deficiencies were identified in 1 of 19 (5%) server and telecommunications rooms evaluated. • A server room contained excess storage items.
DFW	OIG-14-132, September 2014	• Deficiencies were identified in 21 of 29 (72%) server and telecommunications rooms evaluated. • Server and telecommunications rooms contained excess storage items, paint, cleaning supplies, trash, and dust.
JFK	OIG-15-18, January 2015	• Deficiencies were identified in 4 of 21 (19%) server and telecommunications rooms evaluated. • Server and telecommunications rooms contained excess storage items, dust, and cleaning supplies.
SFO	OIG-15-88, May 2015	• No deficiencies were identified among the 28 server and telecommunications rooms evaluated.
MCO	OIG-16-87, May 2016	• No deficiencies were identified among the 5 server and telecommunications rooms evaluated.

Source: OIG-compiled based on data from previous reports

Housekeeping and storage vulnerabilities that are not mitigated may pose risks to the availability of TSA data. For example, computer hardware damaged by dust and debris may not be available to support TSA's passenger and baggage screening processes.

In response to our six report recommendations, TSA officials resolved identified housekeeping deficiencies and provided photographic documentation

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

supporting their actions. We now consider all of our recommendations in this area to be resolved and closed.

Fire Protection

Fire can have far-reaching consequences for computer networks and equipment. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, section 4.2.1.5, *Environmental Controls*, facility managers and security administrators must ensure that environmental controls are established, documented, and implemented to provide fire protection, detection, and suppression. Section 4.2.1.6, *Fire Protection*, of the handbook states that when a centralized fire suppression system is not available, fire extinguishers should be readily available. Specifically, facilities should make available/provide Class C fire extinguishers (which are designed for use with electrical fire and other types of fire). The fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve one.

Fire protection issues we reported from our security controls audits related to a lack of fire extinguishers or smoke detectors at TSA IT locations at airports. Inadequate fire suppression systems place TSA's IT assets at risk of possible loss, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters. Four of our 10 airport security controls reports discussed fire protection issues. Table 4 provides examples of the fire protection deficiencies we identified across the various airport locations.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Table 4. Fire Protection Deficiencies

Airport	OIG Report	Fire Protection Deficiencies
IAD	OIG-07-25, January 2007	• No deficiencies were identified among the 9 server and telecommunications rooms evaluated.
DCA	OIG-07-44, May 2007	• No smoke detectors were identified in 3 of 5 (60%) server and telecommunications rooms evaluated.
LAX	OIG-09-01, October 2008	• No fire suppression was identified in 4 of 7 (57%) server and telecommunications rooms evaluated.
IAD	OIG-09-66, May 2009	• No deficiencies were identified among the 12 server and telecommunications rooms evaluated.
ORD	OIG-12-45, March 2012	• No deficiencies were identified among the 25 server and telecommunications rooms evaluated.
ATL	OIG-13-104, July 2013	• No smoke detector was identified in 1 of 19 (5%) server and telecommunications rooms evaluated.
DFW	OIG-14-132, September 2014	• No deficiencies were identified among 29 server and telecommunications rooms evaluated.
JFK	OIG-15-18, January 2015	• Deficiencies, no fire extinguishers, were identified in 14 of 21 (67%) server and telecommunications rooms evaluated. • Deficiencies, no fire suppression, were identified in 8 of 21 (38%) server and telecommunications rooms evaluated. • Deficiencies, no smoke detectors, were identified in 14 of 21 (67%) server and telecommunications rooms evaluated.
SFO	OIG-15-88, May 2015	• No deficiencies were identified among 28 server and telecommunications rooms evaluated.
MCO	OIG-16-87, May 2016	• No deficiencies were identified among 5 server and telecommunications rooms evaluated.

Source: OIG-compiled based on data from previous reports

TSA resolved the identified fire protection deficiencies. For example, as a compensating control, TSA deployed fire extinguishers at LAX. We therefore consider all of our fire protection recommendations resolved and closed.

Uninterruptable Power Supply

Electrical backup is a key ingredient to sustaining equipment operations in the event of power disruption. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, section 4.2.1.7, *Electronic Power Supply Protection*, electrical power must be filtered through a UPS system for all servers and critical workstations and surge suppressing power strips used to protect all other computer equipment from power surges.

Four of the 10 TSA IT locations at airports we audited had UPS issues. The issues we reported were related to UPS devices that were lacking or needed to

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

be replaced. Table 5 provides examples of the UPS deficiencies we identified.

Table 5. Uninterruptable Power Supply Deficiencies Reported

Airport	OIG Report	Uninterruptable Power Supply Deficiencies
IAD	OIG-07-25, January 2007	• A UPS battery needed replacing in 1 of 9 (11%) server and telecommunications rooms evaluated.
DCA	OIG-07-44, May 2007	• UPS devices were lacking at 4 of 5 (80%) server and telecommunications rooms evaluated.
LAX	OIG-09-01, October 2008	• No deficiencies were identified among 7 server and telecommunications rooms evaluated.
IAD	OIG-09-66, May 2009	• No deficiencies were identified among 12 server and telecommunications rooms evaluated.
ORD	OIG-12-45, March 2012	• No deficiencies were identified among 25 server and telecommunications rooms evaluated.
ATL	OIG-13-104, July 2013	• No deficiencies were identified among 19 server and telecommunications rooms evaluated.
DFW	OIG-14-132, September 2014	• In 4 of 12 (33%) server and telecommunications rooms evaluated, the UPS warning light signals indicated that batteries needed to be replaced.
JFK	OIG-15-18, January 2015	• Inoperable UPS were identified in 3 of 21 (14%) server and telecommunications rooms evaluated.
SFO	OIG-15-88, May 2015	• No deficiencies were identified among 28 server and telecommunications rooms evaluated.
MCO	OIG-16-87, May 2016	• No deficiencies were identified among 5 server and telecommunications rooms evaluated.

Source: OIG-compiled based on data from previous reports

Electrical power supply vulnerabilities that are not mitigated pose risks to the availability of TSA data. For example, TSA servers that are not connected to a working UPS may not be operational following a power outage. Data may be lost or access delayed to support mission operations. To illustrate, in Phoenix, AZ, on May 12, 2016, at approximately 6:30 a.m., a UPS failed, causing the servers supporting the baggage scanning systems at three airport terminals to fail. This failure resulted in more than 3,000 bags being left in 90-degree heat on a secured airport parking lot and missing flights. TSA brought in additional screeners to process the bags by hand; some airlines transported bags to nearby airports, including San Diego and Los Angeles, to be screened and then flown to their destinations. The outage was resolved that night and baggage screening operations were restarted the next day, May 13, 2016. As a result of this outage, TSA included Phoenix in its inventory of airport locations being evaluated to ensure they have adequate operational controls for STIP IT equipment.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

In response to our report recommendations, TSA resolved all UPS deficiencies we identified. For example, TSA reported that 22 failing UPS devices were replaced at DFW. As such, we consider all of our UPS-related recommendations to be resolved and closed.

Redundant Data Communications Circuits

Redundant communications circuits are also vital to continued service for users in the event of disruption. According to *DHS 4300A Sensitive Systems Handbook*, Attachment M: *Tailoring the NIST SP 800-53 Security Controls*, a risk-based management decision must be made regarding requirements for telecommunications services. The availability requirements for the system will define the time period within which the system connections must be available. If continuous availability is required, redundant telecommunications services may be an option. Once a decision is made regarding requirements for telecommunications services, agreements must be established between the appropriate officials.

We reported data communications redundancy issues for TSA IT in 4 of our 10 airport security audit reports. Table 6 lists the data communication circuit deficiencies at the various airport locations.

Table 6. Data Communications Circuit Deficiencies Reported

Airport	OIG Report	Data Communications Circuit Deficiencies
IAD	OIG-07-25, January 2007	• No deficiencies were identified.
DCA	OIG-07-44, May 2007	• No deficiencies were identified.
LAX	OIG-09-01, October 2008	• No deficiencies were identified.
IAD	OIG-09-66, May 2009	• No deficiencies were identified.
ORD	OIG-12-45, March 2012	• Redundant telecommunications services had not been established and only one telecommunications circuit was available to service users at 4 ORD terminals and its Rosemont office.

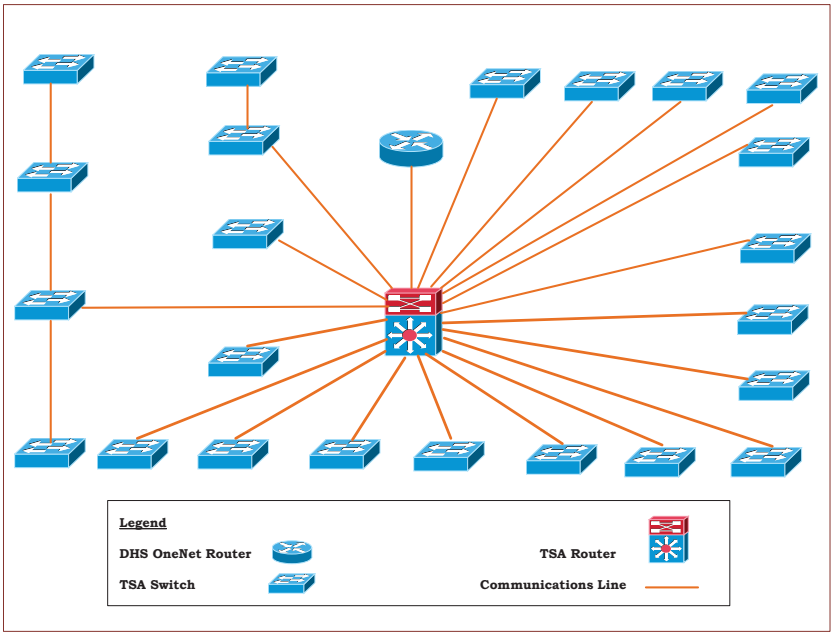
~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Airport	OIG Report	Data Communications Circuit Deficiencies
ATL	OIG-13-104, July 2013	• Only 1 data telecommunications circuit was identified to service TSA users in the North, South, and International Terminals.
DFW	OIG-14-132, September 2014	• Circuits had not been configured to provide redundancy for each DFW terminal and for each server room at the Coppell facility.
JFK	OIG-15-18, January 2015	• No deficiencies were identified.
SFO	OIG-15-88, May 2015	• One telecommunications device represented a single point failure for 23 switches.
MCO	OIG-16-87, May 2016	• No deficiencies were identified.

Source: OIG-compiled based on data from previous reports

As illustrated, TSA IT equipment at three airport locations did not include redundant data communications circuits to ensure system connectivity in the event of a hardware failure. One telecommunications router represented a single point of failure for 23 other switches at SFO. This means that if this one router experienced a hardware failure, TSA staff at SFO would not have remote access to other TSA IT resources. See figure 1 for details.

Figure 1. TSA Data Telecommunications Network at SFO



Source: OIG-compiled based on data obtained from TSA

During our onsite visit at SFO, we observed that this single-point-of-failure

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

router was located in a room with a temperature exceeding the recommended range. The high temperature increased the potential for telecommunications equipment failure. According to TSA officials, they have since corrected the temperature deficiency in this room.

We recommended that TSA determine whether it is necessary and cost-effective to establish redundant data telecommunications services at SFO airport. In response, TSA has accepted the risk to its communications capability and refuted the need for action. Specifically, TSA management said:

> TSA has determined it is not necessary to install redundant data circuits for each of the individual circuits already at SFO. An in-depth review identified that current enterprise telecommunication circuits and associated operations and maintenance costs are approximately $30 million annually. TSA determined it is not cost-effective to install redundant circuits considering the multiple communications and connectivity capabilities already available.

As TSA responded that it was not cost effective to provide redundant circuits, we considered the associated recommendations resolved and closed.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

TSA's Technical Controls for IT Systems

Technical controls provide automated protection from unauthorized access, facilitate detection of security violations, and support IT applications and data security requirements. Technical controls include system passwords and protection against malware. We previously reported on six types of technical control deficiencies for TSA IT equipment at selected airports and other pertinent TSA and Federal Air Marshal Service facilities. These deficiencies included:

- technical vulnerabilities on servers,
- out-of-date software,
- not scanning for vulnerabilities,
- not reporting server scans to the DHS Office of the Chief Information Security Officer,
- not reporting STIP information security incidences to the TSA Security Operations Center, and
- Information Systems Security Officers (ISSO) not receiving real-time security alerts concerning computer security incidences and not performing weekly monitoring of system audit logs.

Appendix F provides a matrix summarizing technical control deficiencies identified across the airports reviewed. TSA has taken several key actions to address these technical control deficiencies in response to our various report recommendations. Specifically—

- TSA now complies with Office of Management and Budget (OMB) guidance for continuous monitoring of IT security risk by having its Information Assurance Division perform vulnerability scans of ICS servers each month and providing the resulting vulnerability reports to the Department for in-depth analysis.[4]
- STIP servers located at TSA data centers have been placed within the boundaries of TSA's ICS to ensure they have the latest software patches and operating systems.
- Information Assurance Division has also been tasked with validating the security controls of airport transportation security equipment (TSE) before they are re-attached to TSA's network.

[4] OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, provides agencies with guidance for managing information security risk on a continuous basis and builds upon efforts towards achieving the cybersecurity Cross Agency Priority goal.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

While TSA's actions have adequately resolved and closed most of the technical control recommendations, TSA has not completely addressed technical control deficiencies associated with STIP IT equipment. For example, we recommended in our MCO report that TSA update the operating systems on STIP servers to a vendor-supported version that can be patched to address emerging vulnerabilities.[5] TSA provided us with action plans for addressing these STIP-related recommendations in our MCO report. Based on our review of the corrective actions outlined in these plans, we consider most of the recommendations resolved but open pending completion of all actions. However, TSA's action plan for recommendation 5 did not provide the steps to obtain and change administrator passwords for STIP servers at airports. This recommendation is unresolved and will remain open until TSA provides supporting documentation that all corrective actions are completed.

Technical Vulnerabilities

Routine patch management to address emerging vulnerabilities is essential to an effective information security program. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, maintaining software that is vendor-supported and routinely updated with patches to address new vulnerabilities as they emerge is critical to IT security.

We reported on technical vulnerability issues related to TSA servers in 9 of our 10 airport security audit reports. High vulnerabilities reported from these audits included vulnerabilities that could be exploited for denial of service or code execution attacks.[6]

Table 7 provides examples of technical control deficiencies we identified from our audits.

[5] Open STIP-related recommendations are listed in appendix I.
[6] The scanning software used for our audits scores vulnerabilities on a scale of 0 to 10, which is based on the Forum of Incident Response and Security Teams' Common Vulnerability Scoring System. Within this system, the more easily a vulnerability can be exploited, the higher the vulnerability score. For this report, vulnerabilities scored over 6.9 are considered to be 'high.'

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Table 7. Technical Vulnerabilities Deficiencies Reported

Airport	OIG Report	Technical Vulnerabilities Deficiencies
IAD	OIG-07-25, January 2007	• Deficiencies, 2 missing patches, were identified on 1 of 2 servers scanned. • Deficiencies were identified for remote logins allowing 'null' sessions and guest accounts that can be exploited.
DCA	OIG-07-44, May 2007	• Deficiencies, updates needed to avoid execution of arbitrary code, were identified on 3 routers scanned.
LAX	OIG-09-01, October 2008	• Deficiencies were identified on 2 servers. The Lightweight Directory Access Protocol was configured to allow anonymous access and the Windows built-in user group "EVERYONE" was configured to allow full control and access to shared data. • Deficiencies were identified on 1 communications switch that we scanned. The switch allowed the Telnet and File Transfer Protocol communications services to transmit login and password credentials in clear text, which may allow an attacker to capture login credentials.
IAD	OIG-09-66, May 2009	• Deficiencies, including vulnerabilities of guest accounts, null sessions, and remote desktop protocol server, were identified on 3 servers scanned.
ORD	OIG-12-45, March 2012	• No servers or switches were scanned as part of our audit.
ATL	OIG-13-104, July 2013	• Deficiencies, including "high" vulnerabilities, were identified; for example, a missing critical patch on 1 server and a guest account with excessive privileges on the other.
DFW	OIG-14-132, September 2014	• Deficiencies, including high vulnerabilities, were identified on 8 servers scanned.
JFK	OIG-15-18, January 2015	• Deficiencies, [redacted] "high" vulnerabilities, were identified on 2 servers scanned.
SFO	OIG-15-88, May 2015	• Deficiencies, [redacted] "high" vulnerabilities, were identified on 7 servers scanned. • Deficiencies, including hundreds of "high" vulnerabilities, were identified on 2 STIP servers scanned.
MCO	OIG-16-87, May 2016	• Deficiencies, including 12,282 "high" vulnerabilities, were identified on 71 of 74 (96%) servers scanned.

Source: OIG-compiled based on data from previous reports

As of February 2016, TSA had updated its ICS and FAMSNet servers to address technical security-related recommendations in response to our audit reports. For example, in response to our DFW report, TSA remediated high vulnerabilities we identified and provided vulnerability scans to document the scan results. As such, these recommendations on remediating high vulnerabilities on ICS and FAMSNet servers are resolved and closed. However, our report recommendations related to improving technical controls on TSA

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

STIP servers remain open and, except for recommendation 5 from our MCO report, resolved. Due to resource and funding constraints, TSA has not yet provided a schedule as to when all required software patches will be applied to STIP airport servers. We will continue to follow up on the status of TSA's corrective actions to address these recommendations until all planned actions are completed.

Out-of-Date Software

According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, maintaining software that is vendor-supported and routinely updated with patches to address new vulnerabilities as they emerge is critical to IT security. We reported out-of-date software related to TSA servers in 3 of our 10 airport security audit reports. Table 8 provides examples of out-of-date software deficiencies we identified across the various airports audited.

Table 8. Out-of-Date Software Deficiencies

Airport	OIG Report	Out-of-Date Software Deficiencies
IAD	OIG-07-25, January 2007	• Out-of-date operating systems were identified on both of the servers scanned.
DCA	OIG-07-44, May 2007	• No deficiencies were identified on the 3 routers scanned.
LAX	OIG-09-01, October 2008	• No deficiencies were identified on the 2 servers and 1 switch scanned.
IAD	OIG-09-66, May 2009	• No deficiencies were identified on the 3 servers scanned.
ORD	OIG-12-45, March 2012	• No servers or switches were scanned.
ATL	OIG-13-104, July 2013	• No deficiencies were identified on the 2 servers scanned.
DFW	OIG-14-132, September 2014	• No deficiencies were identified on [redacted] servers scanned.
JFK	OIG-15-18, January 2015	• No deficiencies were identified on the [redacted] servers scanned.
SFO	OIG-15-88, May 2015	• An operating system, unsupported by the vendor since December 2011, was identified on 1 of the 2 STIP servers scanned.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Airport	OIG Report	Out-of-Date Software Deficiencies
MCO	OIG-16-87, May 2016	• An operating system that the DHS Office of the Chief Information Security Officer recommended upgrading to ensure continued vendor support was identified on 47 of 74 (63%) servers scanned. • An operating system, unsupported by the vendor [redacted], was identified on 6 of 74 (8%) servers scanned. • An operating system, unsupported by the vendor [redacted], was identified on 2 of 74 (3%) servers scanned.

Source: OIG-compiled based on data from previous reports

All of the software deficiencies identified in this area related to out-of-date operating systems that no longer had vendor support. Without such support, no new security patches are provided by the vendors to update the operating systems and secure them from new vulnerabilities and threats that emerge. This is key to providing adequate security in the current age of global IT interconnectivity via the Internet.

In response to our report recommendations, TSA has taken actions to address the software deficiencies identified. Specifically, TSA updated servers with out-of-date operating systems at IAD, and our recommendation in this regard for IAD is resolved and closed. However, TSA has not yet provided a schedule for ensuring the use of vendor-supported operating systems on STIP servers at SFO and MCO. As such, these two recommendations are resolved but remain open pending completion of planned actions.

Servers Not Being Scanned

Vulnerability scanning is the process of identifying known vulnerabilities to information systems to determine whether the systems can be compromised. According to *DHS 4300A Sensitive Systems Handbook,* v12.0, Attachment O, *Vulnerability Management Program,* vulnerability assessment scans must be performed to inspect 95 percent of DHS and component systems at least monthly.

We disclosed that TSA was not scanning its servers in 6 of our 10 airport security audit reports. Table 9 shows the locations where we identified these server scanning deficiencies.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Table 9. Server Scanning Deficiencies

Airport	OIG Report	Server Scanning Deficiencies
IAD	OIG-07-25, January 2007	• No deficiencies were identified.
DCA	OIG-07-44, May 2007	• No deficiencies were identified.
LAX	OIG-09-01, October 2008	• No deficiencies were identified.
IAD	OIG-09-66, May 2009	• No deficiencies were identified.
ORD	OIG-12-45, March 2012	• TSA was not scanning STIP servers.
ATL	OIG-13-104, July 2013	• TSA was not scanning STIP servers.
DFW	OIG-14-132, September 2014	• TSA was not scanning STIP servers.
JFK	OIG-15-18, January 2015	[redacted]
SFO	OIG-15-88, May 2015	[redacted]
MCO	OIG-16-87, May 2016	[redacted]

Source: OIG-compiled based on data from previous reports

Without performing vulnerability scanning as required, TSA is unable to identify weaknesses in a system (or in system security procedures, hardware design, internal controls, etc.). Such weaknesses could be exploited to gain unauthorized access or to affect the systems' availability or data integrity.

TSA was not scanning STIP servers at airports because TSA did not designate STIP IT equipment at airports as IT assets. However, in TSA's management response to our MCO audit, TSA acknowledged that STIP servers at airports should be scanned. Due to resource and funding constraints, TSA has not yet provided a schedule as to when [redacted] will be scanned. We will continue to follow up until all planned corrective actions are completed.

TSA Is Not Providing Required Vulnerability Reports to the Department

Reporting system vulnerability scan results to authorities responsible for ensuring corrective action is essential. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, Attachment O, *Vulnerability Management Program*,

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

components must upload scan results into the DHS Enterprise Vulnerability Management System. Components must declare any inability to perform vulnerability assessments, analysis, and penetration testing or reporting to the DHS Vulnerability Management Branch and arrange for an alternate solution.

We disclosed vulnerability reporting issues related to TSA servers in 5 of our 10 airport security audit reports. Table 10 provides the locations and system we identified with vulnerability reporting deficiencies.

Table 10. Vulnerability Reporting Deficiencies

Airport	OIG Report	Vulnerability Reporting Deficiencies
IAD	OIG-07-25, January 2007	• No deficiencies were identified.
DCA	OIG-07-44, May 2007	• No deficiencies were identified.
LAX	OIG-09-01, October 2008	• No deficiencies were identified.
IAD	OIG-09-66, May 2009	• No deficiencies were identified.
ORD	OIG-12-45, March 2012	• TSA was not reporting vulnerabilities for STIP servers.
ATL	OIG-13-104, July 2013	• TSA was not reporting vulnerabilities for STIP servers. • TSA was not reporting vulnerabilities for a FAMSNet server.
DFW	OIG-14-132, September 2014	• TSA was not reporting vulnerabilities for STIP servers. • TSA was not reporting vulnerabilities for three ICS servers.
JFK	OIG-15-18, January 2015	• No deficiencies were identified.
SFO	OIG-15-88, May 2015	• TSA was not reporting vulnerabilities for STIP servers. • TSA was not reporting vulnerabilities for an ICS server.
MCO	OIG-16-87, May 2016	• TSA was not reporting vulnerabilities for STIP servers.

Source: OIG-compiled based on data from previous reports

Vulnerability reporting helps oversight entities identify and validate the number of systems that are noncompliant with DHS security guidance. To the extent that vulnerabilities are not timely or accurately reported, the Department will not have a correct understanding of deficiencies and problem areas that need to be addressed.

In response to our report recommendations, TSA was able to identify the cause and resolve vulnerability reporting deficiencies related to FAMSNet and ICS

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

servers at DFW and SFO.[7] We consider the associated recommendations resolved and closed. However, TSA has not developed a schedule to resolve this vulnerability reporting deficiency as it relates to STIP airport servers that are not connected to the network and cannot be remotely scanned. The associated recommendations for STIP are resolved, but they remain open pending completion of planned corrective actions.

TSA SOC Not Receiving STIP Computer Security Incident Reports

Timely computer security incident reporting is critical to ensuring effective, coordinated response and evaluation to safeguard DHS information systems from further occurrences. According to the *DHS 4300A Sensitive Systems Handbook*, Attachment F, *Incident Response*, all users of DHS information systems, including system and network administrators and security officers, are responsible for reporting incidents to their component Security Operations Centers (SOC) immediately upon suspicion or recognition.

As a result of our DFW fieldwork, we reported that TSA had not established procedures to report STIP-related computer security incidents to the TSA SOC. According to TSA staff, when STIP users identify a problem, they report it to a contractor-operated TSA Service Response Center. However, there were no procedures in place for this center to, in turn, refer computer security incidents to the TSA SOC.

STIP computer security incidents that are not reported to TSA SOC place at risk the confidentiality, integrity, and availability of TSA data. Specifically, without adequate reporting, TSA SOC may not be able to effectively coordinate incident response and initiate incident evaluation processes to a computer security incident.

We recommended in our DFW report, that TSA establish a process to report STIP computer security incidents to TSA SOC. Per its August 2014 management response to our DFW report, TSA planned to train staff on computer security incidence reporting. In September 2015, TSA provided additional documentation concerning their cybersecurity efforts. However, we noted in our response, that TSA had not provided documentation showing that the TSA Service Response Center is to contact the TSA SOC when there is a computer security incidence. This recommendation is resolved, but it will remain open until all implementing actions are completed.

[7] Our ATL report, OIG-13-104, did not have a recommendation regarding providing vulnerability scan reports to the Department.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

ISSOs Not Receiving/Reviewing Audit Logs

ISSOs develop and maintain Security Plans and are responsible for overall system security. One tool they use to monitor system security is a system's audit logs. For example, all failed logon attempts are to be recorded in an audit log and periodically reviewed. According to the *DHS 4300A Sensitive Systems Handbook*, v9.1, ISSOs should review audit records at least weekly, or in accordance with their component Security Plans.

As a result of our ATL audit, we reported that TSA ISSOs were not performing weekly monitoring of system audit logs. According to TSA officials, this was because the audit logs were sent to a platform to which the ISSO did not have remote access. Therefore, we recommended that the TSA Chief Information Officer (CIO) provide ISSOs with the capability to review audit logs.

In response to this report, TSA staff stated that the TSA SOC, rather than the ISSO, is responsible for monitoring the audit logs. Supporting this position, the Department updated the *DHS 4300A Sensitive Systems Handbook* in November 2015, adding the review of audit logs as a responsibility of component SOCs. Specifically, *DHS 4300A Sensitive Systems Handbook*, v12.0 now states:

> Component SOCs are responsible for incident response, handling and reporting those incidents that pertain to the Component's network and data. In addition, Component SOCs are responsible for all network and host-based monitoring activities within the Component's network. This includes the detection, investigation, and subsequent reporting to DHS Enterprise SOC upon confirmation.

Upon reviewing the updated DHS Handbook, we agreed with TSA's position and closed the recommendation from our ATL report.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

TSA's Management Controls for IT Systems

We previously reported on seven types of management control deficiencies from our airport security audits. These deficiencies include:

- system security documentation deficiencies,
- inadequate systems inventories,
- unauthorized or unsecure wireless devices,
- plans of actions and milestones not being reported,
- type accreditation issues,
- disaster recovery issues, and
- capital planning and investment control (CPIC) deficiencies.

Appendix G provides a matrix summarizing management control deficiencies identified across the airports reviewed.

In summary, TSA has taken several actions to address our management control deficiencies. For example, TSA—

- improved the system security in April 2009 by restructuring IT systems by type of IT equipment:
  1. ICS for servers, and
  2. EUC for desktops;
- placed STIP servers at its data centers within the boundaries of the ICS to better manage the IT security of the STIP servers at the data centers;
- included airport TSEs in the STIP system security plan to adequately provide an overview of the system's security requirements; and
- updated agreements between TSA and airports to clearly illustrate the security responsibilities related to in-line baggage systems.

In our view, these changes have resulted in better management of TSA's systems. However, there are still several areas where TSA could improve. For example, we determined that TSA business impact analyses (BIA) did not identify the impact of a potential system disruption on airport baggage and screening processes. The BIAs also did not document the airport's local area networks or the mission/business processes relying on those local area networks.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

The following subsections provide a recap of our findings in the seven management control areas for IT systems at the airports audited.

Inadequate System Security Documentation

System security documentation involves collection of detailed information in areas including functionality, system mission, types of data processed, system interfaces, system boundaries, hardware and software elements, system and network diagrams, cost of assets, system communications and facilities, and any additional system-specific information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls.

Our previous reports identified deficiencies in the following systems security documentation:

Business Impact Analysis (BIA) - According to the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, the purpose of the BIA is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption.

System Security Plans - According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, the system security plan provides an overview of the system's security requirements, describes the controls in place or planned, and delineates the responsibilities and expected behavior of all individuals who access the system.

Interconnection Security Agreements (ISA) - According to *DHS 4300A Sensitive Systems Handbook* v12.0, the ISA documents the security protections on the interconnected systems to ensure that only acceptable transactions are permitted.

We discussed system security documentation deficiencies in 3 of our 10 airport security reports. Table 11 provides examples of the system security documentation deficiencies at the airports audited.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Table 11. System Security Documentation Deficiencies

Airport	OIG Report	System Security Documentation Deficiencies
IAD	OIG-07-25, January 2007	• No deficiencies were identified.
DCA	OIG-07-44, May 2007	• No deficiencies were identified.
LAX	OIG-09-01, October 2008	• No deficiencies were identified.
IAD	OIG-09-66, May 2009	• No deficiencies were identified.
ORD	OIG-12-45, March 2012	• TSA had not prepared BIAs for TSA IT systems.
ATL	OIG-13-104, July 2013	• TSA had not prepared BIAs for TSA IT systems.
DFW	OIG-14-132, September 2014	• STIP systems security plan did not include all STIP assets. • TSA had no interconnection security agreements for managing relationships between STIP and the airport/airline baggage handling systems.
JFK	OIG-15-18, January 2015	• No deficiencies were identified.
SFO	OIG-15-88, May 2015	• No deficiencies were identified.
MCO	OIG-16-87, May 2016	• No deficiencies were identified.

Source: OIG-compiled based on data from previous reports

Inadequate or incomplete system security documentation prevents senior TSA management from fully understanding the risks associated with operating a system. Without a complete understanding of the risks, TSA management may not adequately balance the operational and economic costs of protecting the information systems and data that support their organization's missions.

As a result of our DFW audit, we reported deficiencies in the STIP system security plan and the lack of a STIP ISA. We considered the associated recommendations resolved and closed based on TSA's actions. Specifically, TSA updated the STIP system security plan to include TSE devices located at airports. TSA also now documents the roles and responsibilities for airport connections between STIP and the non-DHS baggage in-line baggage handling, including the specific roles and responsibilities for TSA and local airport authorities.

In response to our report recommendations to prepare BIAs, TSA provided BIAs for the TSANet, ICS, FAMSNet, and STIP in February 2014. We considered the associated recommendations resolved and closed.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

However, as part of this current effort to determine whether TSA should accept the increased risk of an outage due to a lack of telecommunications redundancy at airports, we re-reviewed the BIAs provided. We determined that these BIAs did not provide an adequate assessment of the impact to TSA's mission if airport networks suffer an outage. For example, the TSANet BIA does not document TSA's local area networks at airports. Additionally, the TSANet BIA does not include identification of TSA organizations at airports that provide data to or receive data from the TSANet or the points of contacts for any interconnected systems.

Senior TSA management is accepting the risk of a communications outage on a local area network at an airport without a complete understanding of the impact on its business processes. Therefore, for the TSA IT systems used at airports, we are making one new recommendation that TSA prepare business impact analyses that comply with best practices.

Inadequate System Inventory

The increasing costs required to adequately protect agency information systems necessitates an agency-wide view of security to make the costs more manageable. An agency must consider its entire inventory of information systems when developing appropriate strategies and programs for protecting those systems and managing agency-level risks. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, a DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local government agency on behalf of DHS. DHS systems include general support systems and major applications. Within DHS, component CIOs are responsible for ensuring that accurate information systems inventories are established and maintained.

As a result of our LAX audit, we reported that not all TSA IT resources at LAX were accounted for in TSA's system inventory. For example, a logistics server and database were not included in the TSA system inventory or the TSA security authorization process.[8] TSA management cannot be assured that IT systems and data are adequately secured unless the various required activities

[8] Security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

in the security authorization are performed, and the risks associated with operating the systems are accepted in writing. In response to our report recommendation to address this issue, TSA provided documentation that the LAX server and database were included in a larger system. As such, the associated recommendation is resolved and closed.

In another instance, we reported that TSA did not designate an information system for inclusion in the TSA system inventory. Specifically, as a result of our JFK audit, we reported that the closed-circuit television (CCTV) security system at the airport was not recognized as an IT system. In response to our JFK audit, TSA indicated it does not have a relationship at the JFK Airport that meets the definition of *DHS 4300A Sensitive Systems Handbook* for DHS IT systems. TSA stated that, because the intrusion detection and surveillance security systems are owned and operated by the Airport Authority, it had no responsibility to ensure that IT security and privacy controls were met. As such, DHS did not concur with our recommendation to designate detection and surveillance systems as DHS IT systems and to initiate appropriate IT security and privacy controls for the CCTV system. We do not agree with DHS' response to this recommendation. The response did not provide for corrective actions to address the security and privacy concerns identified.

As of April 2016, TSA had not developed a plan to resolve these recommendations. In April 2016, the DHS Inspector General sent a memo to the DHS Under Secretary for Management.[9] The Inspector General pointed out that JFK is operating the CCTV system at the TSA checkpoints for the benefit of TSA. TSA paid for it, requires its maintenance, has unlimited access to and control over its recordings, and uses it on a daily basis to ensure efficient checkpoint operations. As such, TSA needs to ensure that it implements for the CCTV the same management, technical, operational, and privacy controls and reviews applicable to all other DHS information systems. We are continuing to coordinate with DHS to resolve this issue.

[9] Inspector General John Roth, *Unresolved Recommendation: Audit of Security Controls for DHS Information Technology Systems and JFK International Airport, Dated January 16, 2015*, April 15, 2016.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Unauthorized or Unsecure Wireless Devices

Wireless devices pose a range of security issues well beyond the vulnerabilities of hardwired technology. For example, eavesdropping on wireless communications with commercially available equipment is common; it is relatively easy to detect and exploit wireless access points. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, Authorizing Officials, the senior management officials with responsibility for operating an information system at an acceptable level of risk, are to specifically approve or prohibit the use of wireless communications technologies within the Department.

In 2 of our 10 reports, we disclosed concerns about TSA's use of unauthorized or unsecure wireless devices at airports. Table 12 aligns the wireless deficiencies we identified with the various airport locations.

Table 12. Wireless Device Deficiencies

Airport	OIG Report	Wireless Device Deficiencies
IAD	OIG-07-25, January 2007	• An unauthorized wireless router was in use.
DCA	OIG-07-44, May 2007	• TSA was using an unapproved version of a wireless security protocol.
LAX	OIG-09-01, October 2008	• No deficiencies were identified.
IAD	OIG-09-66, May 2009	• No deficiencies were identified.
ORD	OIG-12-45, March 2012	• No deficiencies were identified.
ATL	OIG-13-104, July 2013	• No deficiencies were identified.
DFW	OIG-14-132, September 2014	• No deficiencies were identified.
JFK	OIG-15-18, January 2015	• No deficiencies were identified.
SFO	OIG-15-88, May 2015	• No deficiencies were identified.
MCO	OIG-16-87, May 2016	• No deficiencies were identified.

Source: OIG-compiled based on data from previous reports

In response to our IAD report recommendation, TSA agreed to require approval for wireless devices. TSA also reconfigured the wireless devices at DCA to the correct wireless security protocol. We consider both of the associated recommendations resolved and closed.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Plan of Action and Milestones

POA&Ms are a management tool to help identify and track remediation of identified weakness. According to the *DHS 4300A Sensitive Systems Handbook*, v12.0, a POA&M is required as part of the system authorization package, which is submitted to the official responsible for authorizing operation of the information system. The POA&M documents any system weaknesses that management will mitigate and the corrective actions that must be taken. The POA&M also details required resources, milestones, and scheduled completion dates, and assigns action items to individuals.

Two of our 10 airport security audit reports discussed POA&M deficiencies. Table 13 ascribes the POA&M deficiencies found to the various airport locations.

Table 13. POA&M Deficiencies

Airport	OIG Report	POA&M Deficiencies
IAD	OIG-07-25, January 2007	• Deficiencies were identified; specifically, there were no POA&Ms for 84 of 85 (99%) of the vulnerabilities identified during the TSANet risk assessment.
DCA	OIG-07-44, May 2007	• No deficiencies were identified.
LAX	OIG-09-01, October 2008	• No deficiencies were identified.
IAD	OIG-09-66, May 2009	• No deficiencies were identified.
ORD	OIG-12-45, March 2012	• No deficiencies were identified.
ATL	OIG-13-104, July 2013	• No deficiencies were identified.
DFW	OIG-14-132, September 2014	• No deficiencies were identified.
JFK	OIG-15-18, January 2015	• No deficiencies were identified.
SFO	OIG-15-88, May 2015	• Deficiencies were identified; no disaster recovery related POA&M, for FAMSNet and ICS.
MCO	OIG-16-87, May 2016	• No deficiencies were identified.

Source: OIG-compiled based on data from previous reports

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

We verified that, as we recommended, TSA created the necessary POA&Ms to resolve known and reported deficiencies identified in our IAD report. In response to our SFO report, TSA concurred and documented all vulnerabilities discovered during its security assessment of FAMSNet. Accordingly, the associated recommendations are resolved and closed.

Type Accreditation

Type accreditation allows for consolidating common security controls across the sites and for conducting a single master security authorization. *DHS 4300A Sensitive Systems Handbook*, v12.0, recommends that components pursue Type Accreditation for information resources that—

- are under the same direct management control;
- have the same function or mission objective, operating characteristics, security needs;
- reside in the same general operating environment; or
- in the case of a distributed system, reside in various locations with similar operating environments.

We reported in our DFW report that not all STIP assets were documented in the STIP information security plan. For example, we disclosed that the STIP system security plan, which is a security authorization process document, did not describe the servers, switches, and workstations associated with the system. In December 2014, in response to our report recommendation, TSA reported that STIP transportation security equipment was included in the STIP system security plan.

However, as stated in our SFO report, TSA also needed to document the security controls for those new IT assets as part of the authorization process. Additionally, we stated that the STIP system was now too large for one authorization package to adequately document the risks inherent in operating the STIP. Therefore, in our SFO report, we recommended that TSA determine whether it was necessary and cost effective to use 'type' authorization for STIP servers.

Subsequently, TSA re-authorized the STIP to operate and provided documentation that demonstrated that a type accreditation methodology was used. This recommendation is resolved and closed.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Inadequate Disaster Recovery Capability

Without an established STIP disaster recovery capability, TSA's managers may not be able to adequately track TSE baggage and passenger screening performance if the DHS data center becomes inaccessible due to a natural or manmade disaster such as a telecommunications or power outage. According to *DHS 4300A Sensitive Systems Handbook,* v12.0, systems with an impact level of high for availability require an established alternate site as part of their continuity plans, and resources for establishing an alternate site must be identified and made available.

As a result of our MCO audit, we reported that TSA had not established an effective disaster recovery capability for STIP servers residing at the DHS data center. Specifically, at the time of our audit, there was insufficient STIP server processing capacity at the designated backup site to provide full operational capability.

In response to our report, TSA plans to conduct an analysis to determine the level of effort necessary to create full operational recovery capabilities in an alternate location for the STIP servers. However, the implementation of the solution will be dependent on the availability of funds and acquisition of the engineering services required. The associated recommendation is resolved, but it remains open pending completion of planned corrective actions.

Capital Planning and Investment Controls

Visibility over IT investments in the CPIC process is essential to ensure each investment is well managed, cost effective, and supports the mission and strategic goals of the Department. Various criteria help define what constitutes IT and the oversight that is required to manage it. Specifically:

- *DHS 4300A Sensitive Systems Handbook*, v12.0, cites Division E of the *Information Technology Management Reform Act of 1996*, Public Law 104-106, commonly referred to as the *Clinger-Cohen Act of 1996*, and defines IT as "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency." The "equipment" referred to that which may be used by any DHS component or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

product in support of DHS. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

- *DHS 4300A Sensitive Systems Handbook*, v12.0, further states information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved to the maximum extent possible in all aspects of the acquisition process, including drafting contracts, and procurement documents.

- OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, July 2014 – Revised November 2014, Section 55.6, states agency reporting of its IT portfolio should include all of an agency's annual IT costs. The agency's complete IT portfolio must be reported, including all major, non-major, migration related, and funding contributions IT investments.

- OMB's *FY 2017 IT Budget – Capital Planning Guidance*, Revised June 2015, says if OMB or the agency Chief Information Officer determines data reported to the IT Dashboard is not timely and reliable, the CIO (in consultation with the agency head) must notify OMB through the Integrated Data Collection process and establish within 30 days of this determination an improvement program to address the deficiencies. The CIO will collaborate with OMB to develop a plan that includes root cause analysis, timeline to resolve, and lessons learned. In addition, the CIO will communicate steps being taken to execute the data improvement program and progress to OMB and notify the agency head. Agencies will provide updates on the status of this program on a quarterly basis as a part of their Integrated Data Collection submission until the identified deficiency is resolved.

As a result of our MCO audit, we reported that TSA was not effectively managing all IT Components of STIP as IT investments. Based on guidance from the TSA Associate Administrator, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts, which promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP TSEs from the network. TSA also did not identify all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

We made two recommendations to TSA to improve the STIP-related CPIC process. TSA concurred with both recommendations. However, according to TSA's response to our report, full implementation of these recommendations will be dependent on funding and resources. Additionally, TSA has not provided a schedule for when these recommendations will be fully implemented. We will continue to follow up to ensure TSA actions address these recommendations.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Summary and Status of Prior OIG Recommendations to TSA

We made a total of 56 recommendations to the TSA Administrator to address the operational, technical, and management control deficiencies we identified as a result of our previous audits of the security of TSA IT systems at selected airports. Table 14 provides a tally of all recommendations by airport report and security control area.

Table 14. Tally of Recommendations by Airport

		Recommendations			
Airport	OIG Report	TSA Total	Operational Control	Technical Control	Management Control
IAD	OIG-07-25, January 2007 and OIG-09-66, May 2009	7	2	3	2
DCA	OIG-07-44, May 2007	3	2	1	0
LAX	OIG-09-01, October 2008	4	1	2	1
ORD	OIG-12-45, March 2012	4	2	1	1
ATL	OIG-13-104, July 2013	6	2	1	3
DFW	OIG-14-132, September 2014	7	2	2	3
JFK	OIG-15-18, January 2015	6	4	1	1
SFO	OIG-15-88, May 2015	8	2	4	2
MCO	OIG-16-87, May 2016	11	1	3	7
	TOTALS:	56	18	18	20

Source: OIG-compiled based on data from previous reports

A senior TSA official has acknowledged the value of our individual audits of security controls at the airports and has made significant corrective actions in response to our recommendations to address the issues we identified. As such, 40 of the 56 (71 percent) recommendations from our prior airport IT security audit reports have been resolved and closed.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Other recommendations are resolved and open based on TSA's POA&Ms for addressing them. Specifically, 14 recommendations related to the STIP are resolved but open. TSA concurred with all of our recommendations to address STIP-related deficiencies included in our DFW, SFO, and MCO airport security reports. However, according to TSA, the implementation of solutions will depend on the availability of funds and the acquisition of required engineering services.

Additionally, while TSA concurred with recommendation 5 in our MCO airport security report regarding changing the passwords on vendor-managed servers, TSA's action plan, and 90-day update of July 2016, did not specifically address when TSA would change the passwords. As such, recommendation 5 remains open and unresolved. We continue to work with TSA staff and Departmental officials to address this issue.

In one instance, TSA disagreed with our recommendation, which remains open and unresolved. This recommendation related to the CCTVs, including cameras, placed in the screening area at JFK airport remains unresolved and open. The systems are designed to view and record TSA checkpoint operations. TSA disagreed with our recommendation to designate these devices as DHS IT systems that require TSA management, technical, operational, and privacy control reviews. Appendix H contains a copy of our Inspector General's memo elevating this issue to the DHS Under Secretary for Management for resolution, which details our position.

See appendix I for a detailed list of the recommendations on the security of TSA's airport systems that remain open and the status of TSA efforts to address them.

As a result of our analysis to compile this summary report, we are making two new recommendations to improve security controls for TSA's IT systems at airports. Specifically, TSA needs to fully assess the risk of not having redundant data communications capability to sustain operations at airports in case of circuit outages. TSA must ensure that BIAs of its IT systems at airports identify the mission/business processes supported by the system and the impact of a system disruption on those processes.

Additionally, while TSA has scheduled reviews of security controls for its IT systems at 17 of 440 airports in the United States, it would benefit from establishing a plan to conduct the reviews on a recurring basis nationwide. This would provide TSA the opportunity to assess the FAMSNet, ICS, STIP, and TSANet assets that we examined as part of our airport security control audits.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

We conclude that addressing these outstanding issues will better position TSA to effectively accomplish its mission of ensuring the security of the Nation's transportation systems and supporting the freedom of movement of people and commerce.

Recommendations

We recommend that the TSA CIO:

Recommendation 1: Update TSA's Business Impact Analyses for TSANet and STIP to include the TSA LANs, points of contact, and business processes that would be adversely affected by a potential communications outage at airports.

Recommendation 2: Establish a plan to conduct recurring reviews of the operational, technical, and management security controls for TSA IT systems at U.S. airports nationwide.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the TSA Deputy Administrator. We have included a copy of the comments in their entirety in appendix B. TSA concurred with both of the recommendations. We reviewed the Deputy Administrator's comments, as well as the technical comments previously submitted under separate cover, and made changes to the report as appropriate. Following is our evaluation of the Administrator's comments, as well as his response to each recommendation in the draft report provided for agency review and comment.

Agency Comments to Recommendation 1:

TSA concurs with this recommendation. TSA will create a template and train the TSANet and STIP System Owners and Information System Security Officers on completing a BIA in fiscal year 2017. The scheduled completion date for the BIA is September 30, 2017. In addition, TSA will suggest to DHS to incorporate BIAs of Mission Essential Systems as required artifacts in the DHS Information Assurance Compliance System and the risk management framework. This will bridge the policy gap with the DHS 4300A Handbook Section 3.5. The estimated closure date for these actions is September 30, 2017.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

OIG Analysis of Agency Comments to Recommendation 1:

TSA's plans satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 2:

TSA concurs with this recommendation. Currently, TSA reviews operational, technical, and management security controls for U.S. airports nationwide through multiple methods. The security controls of IT systems at the airports are given oversight by the Office of Information Technology in cooperation with IT system owners. There are plans to visit airports throughout the year to address the physical and environmental controls of the TSA Information System Restricted Access areas. TSA will conduct reviews on a recurring basis nationwide. During site visits, TSA will inspect IT cabinets, network infrastructure, servers, and environmental and physical security controls.

TSA will perform 10 site visits within FY 2017. Scheduled plans are as follows:

- Phoenix, PHX- October 18 through November 1, 2016
- Miami, MIA- October 31 through November 17, 2016
- Seattle, SEA - December 5 through December 16, 2016
- Indianapolis, IND - January 6 through January 13, 2017
- Denver, DEN -January 27 through February 8, 2017

TSA is currently procuring vendor support so that it can implement a plan of recurring reviews. The estimated closure date for these actions is September 30, 2017.

OIG Analysis of Agency Comments to Recommendation 2:

TSA's plans satisfy the intent of this recommendation. Although TSA has published plans for a partial schedule, full implementation is dependent on procuring vendor support. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix A
Objective, Scope, and Methodology

The DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

We previously reported on deficiencies in IT security controls of TSA IT systems at selected airports. Our audits entailed interviewing key officials, reviewing security authorization documentation, conducting vulnerability assessment scans, and evaluating the physical and environmental conditions of server rooms and network closets at airports. We examined IT security documentation, such as business impact analyses and IT system security plans. We reviewed guidance DHS provided to its Components in the areas of system documentation, information security patch management, and wireless security. We evaluated applicable DHS and Component policies and procedures, as well as government-wide guidance. We subsequently provided briefings and presentations to TSA staff on the results of our fieldwork and the information we planned to report.

This summary of our 10 prior reports is focused on TSA, not the other DHS components. This audit was undertaken to determine whether reported IT operational, management, and technical security control vulnerabilities for TSA's onsite IT systems increased or decreased over time. An additional objective was to determine whether TSA's actions to address reported IT security control deficiencies have been adequate, effective, and have addressed underlying causes. We reviewed previous audit reports, interviewed TSA staff, and reviewed recommendation status information.

We conducted this performance audit between January 2016 and July 2016 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

We appreciate the efforts of DHS management and staff to provide the information and access necessary to accomplish this review. Major OIG contributors to the audit are identified in appendix J.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix B
Agency Comments to the Draft Report

OCT 2 4 2016

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

Transportation
Security
Administration

MEMORANDUM FOR: John Roth
Inspector General
U.S. Department of Homeland Security

FROM: Huban A. Gowadia, Ph.D. 24 Oct 16
Deputy Administrator
Transportation Security Administration

SUBJECT: Management's Response to OIG Draft Report: *Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports*, Project No. 16-005-ITA-TSA

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

The Department is pleased to note the OIG's positive recognition of the various actions the Transportation Security Administration (TSA) has taken to implement previous recommendations and improved information technology (IT) security policies and procedures at TSA airport security operations. DHS appreciates the OIG's acknowledgement that most of these recommendations are resolved and closed. TSA remains committed to enabling global transportation security by providing world-class information technologies and services.

Specifically, OIG acknowledges TSA has actively taken steps to resolve all deficiencies identified in these recommendations. In the area of operational controls, all recommendations are resolved and closed. Most of the recommendations involving technical vulnerabilities and management controls have also been resolved and closed. However, TSA continues to address recommendations involving the Security Technology Integrated Program (STIP) and Closed Circuit Television (CCTV). The TSA Cybersecurity plan has been created to address the STIP issues and is being implemented to remediate all identified deficiencies. The Undersecretary for Management (USM) is addressing the matter of designating the CCTV systems as a DHS IT system.

As a result of the analysis, OIG has made two new recommendations to improve security controls for TSA's IT systems at airports. Please see the attached for our detailed response to each recommendation.

Attachment

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Responses to Recommendations

Recommendation 1: Update TSA's Business Impact Analyses for TSANet and STIP, and to include the TSA local area networks (LANs), points of contact, and business processes that would be adversely affected by a potential communications outage at airports.

Response: Concur. TSA will create a template and train the TSANet and STIP System Owners and Information System Security Officers (ISSOs) on completing a Business Impact Analyses (BIA) in fiscal year (FY) 2017. The scheduled completion date for the BIAs is September 30, 2017. In addition, TSA will suggest to DHS to incorporate BIAs of Mission Essential Systems as a required artifact in the DHS Information Assurance Compliance System (IACS) and within the risk management framework. This will bridge the policy gap with the DHS 4300A Handbook Section 3.5. The estimated closure date is September 30, 2017.

Recommendation 2: Establish a plan to conduct recurring reviews of the operational, technical, and management security controls for TSA IT systems at U.S. airports nationwide.

Response: Concur. Currently, TSA reviews operational, technical, and management security controls for U.S. airports nationwide through multiple methods. The security controls assessed of IT systems that reach the airports are given oversight by the Office of Information Technology (OIT) in cooperation with IT System Owners. There are plans to visit airports throughout the year to address the Physical and Environmental (PE) controls of the TSA Information System Restricted Access areas. TSA will conduct reviews on a recurring basis nationwide. During site visits, TSA will inspect IT cabinets, network infrastructure, servers, and environmental and physical security controls.

TSA will perform 10 site visits within FY 2017. Current scheduled plans are as follows:

- Phoenix, PHX – October 18 through November 1, 2016
- Miami, MIA – October 31 through November 17, 2016
- Seattle, SEA – December 5 through December 16, 2016
- Indianapolis, IND – January 6 through January 13, 2017
- Denver, DEN – January 27 through February 8, 2017

TSA is currently procuring vendor support so that it can implement a plan of recurring reviews. The estimated closure date is September 30, 2017.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix C
Previous Audit Reports on Security Controls of TSA's IT Systems at Airports

Technical Security Evaluation of DHS Activities at Dulles International Airport, OIG-07-25, January 2007 (Unclassified Summary)

https://www.oig.dhs.gov/assets/Mgmt/OIG_07-25_Jan07.pdf

Technical Security Evaluation of DHS Activities at Ronald Reagan Washington National Airport, OIG-07-44, May 2007 (Unclassified Summary)

https://www.oig.dhs.gov/assets/Mgmt/OIG_07-44_May07.pdf

Technical Security Evaluation of DHS Activities at Los Angeles International Airport, OIG-09-01, October 2008 (Redacted)

https://www.oig.dhs.gov/assets/Mgmt/OIGr_09-01_Oct08.pdf

DHS Progress in Addressing Technical Security Challenges at Washington Dulles International Airport, OIG-09-66, May 2009 (Redacted)

https://www.oig.dhs.gov/assets/Mgmt/OIG_09-66_May09.pdf

Technical Security Evaluation of DHS Components at O'Hare Airport, OIG-12-45, March 2012 (Redacted)

https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-45_Mar12.pdf

Technical Security Evaluation of DHS Activities at Hartsfield-Jackson Atlanta International Airport, OIG-13-104, July 2013

https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-104_Jul13.pdf

Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport, OIG-14-132, September 2014

https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-132_Sep14.pdf

Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport, OIG-15-18, January 2015 (Redacted)

https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-88_May15.pdf

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport, OIG-15-88, May 2015

https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-88_May15.pdf

IT Management Challenges Continue in TSA's Security Technology Integrated Program (Redacted), OIG-16-87, May 2016

https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-87-May16.pdf

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix D
TSA IT Systems at Selected U.S. Airports

TSA's activities at the selected airports we audited included screening passengers and baggage on departing flights. See appendix C for selected list of the airports audited. TSA staff at these locations used the following systems:

- EUC - provides TSA employees and contractors with desktops, laptops, local printers, and other end-user computing applications at the various DHS/TSA locations and sponsored sites.

- FAMSNet – provides the IT infrastructure to support the FAMS mission. FAMS staff includes law enforcement officers that help to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. FAMSNet supports FAMS' overall critical mission by providing Internet access, as well as internal access, to FAMS information systems including, but not limited to, email, database(s), file sharing, printing, and a number of critical administrative and enforcement related programs. FAMSNet also provides a communication pathway to third-party and government networks, such as those used by DHS, TSA, the Federal Aviation Administration, and other State and local law enforcement entities. FAMSNet has been designated a mission-essential system.

- ICS – provides core services, including file and print services, to the entire TSA user community. ICS has been designated a mission-essential system.

- STIP – combines many different types of components, including TSE, servers and storage, software/application products, and databases. A user physically accesses the transportation security equipment to perform screening or other administrative functions. TSA's STIP enables the remote management of TSE by connecting it to a centralized server that supports data management, aids threat response, and facilitates equipment maintenance, including automated deployment of software and configuration changes. STIP-enablement of TSE encompasses explosive trace detectors, explosive detection systems, advanced technology X-ray, advanced imaging technology, and credential authentication technology. STIP has been designated a mission-essential system.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

TSA's Office of Security Capabilities (OSC) is responsible for the Passenger Screening Program, the Electronic Baggage Screening Program, and STIP. OSC's mission is to safeguard our nation's transportation systems through the qualification and delivery of innovative security capabilities and solutions. STIP stakeholders include TSA Headquarters, OSC, Office of Information Technology, Office of Intelligence and Analysis, airport leadership/management, original equipment manufacturers, and maintenance service providers.

- TSANet – provides connectivity for airports and their users. TSANet consists of a geographically dispersed wide-area network and each site's LAN. The network is connected to the DHS OneNet and has been designated a mission-essential system.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix E
TSA Operational Controls Issues

Report	Redundant Data Circuits	Physical Security	Environmental Controls	House-keeping	Fire Protection	Uninterruptible Power Supply
IAD, OIG-07-25, January 2007	No	Yes	No	No	No	Yes
DCA, OIG-07-44, May 2007	No	Yes	No	Yes	Yes	Yes
LAX, OIG-09-01, October 2008	No	Yes	Yes	Yes	Yes	No
IAD, OIG-09-66, May 2009	No	Yes	No	Yes	No	No
ORD, OIG-12-45, March 2012	Yes	No	Yes	No	No	No
ATL, OIG-13-104, July 2013	Yes	No	No	Yes	Yes	No
DFW, OIG-14-132, September 2014	Yes	Yes	Yes	Yes	No	Yes
JFK, OIG-15-18, January 2015	No	Yes	Yes	Yes	Yes	Yes
SFO, OIG-15-88, May 2015	Yes	Yes	Yes	No	No	No
MCO, OIG-16-87, May 2016	No	Yes	No	No	No	No

Source: OIG-compiled based on data from previous reports

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix F
TSA Technical Controls Issues

Report	Technical Vulnerabilities	Out-of Date Software	Not Scanning Servers	Not Reporting Server Scans	ISSOs Not Receiving/ Reviewing Audit Logs	STIP/ TSA SOC Issues
IAD, OIG-07-25, January 2007	Yes	Yes	No	No	No	No
DCA, OIG-07-44, May 2007	Yes	No	No	No	No	No
LAX, OIG-09-01, October 2008	Yes	No	No	No	No	No
IAD, OIG-09-66, May 2009	Yes	No	No	No	No	No
ORD, OIG-12-45, March 2012	No	No	Yes	No	No	No
ATL, OIG-13-104, July 2013	Yes	No	Yes	Yes	Yes	No
DFW, OIG-14-132, September 2014	Yes	No	Yes	Yes	No	Yes
JFK, OIG-15-18, January 2015	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
SFO, OIG-15-88, May 2015	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
MCO, OIG-16-87, May 2016	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Source: OIG-compiled based on data from previous reports

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix G
TSA Management Controls Issues

Report	System Security Documentation (SP, BIA, ISA) Deficiencies	Inadequate Systems Inventory	POA&Ms Were Not Being Reported	Type Accreditation	Unsecure Wireless Devices	Disaster Recovery	CPIC
IAD, OIG-07-25, January 2007	No	No	Yes	No	Yes	No	No
DCA, OIG-07-44, May 2007	No	No	No	No	Yes	No	No
LAX, OIG-09-01, October 2008	No	Yes	No	No	No	No	No
IAD, OIG-09-66, May 2009	No	No	No	No	No	No	No
ORD, OIG-12-45, March 2012	Yes	No	No	No	No	No	No
ATL, OIG-13-104, July 2013	Yes	No	No	No	No	No	No
DFW, OIG-14-132, September 2014	Yes	No	No	No	No	No	No
JFK, OIG-15-18, January 2015	No	Yes	No	No	No	No	No
SFO, OIG-15-88, May 2015	No	No	Yes	Yes	No	No	No
MCO, OIG-16-87, May 2016	No	No	No	No	No	Yes	Yes

Source: OIG-compiled based on data from previous reports

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix H
April 15, 2016 Memo to TSA Administrator

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

April 15, 2016

MEMORANDUM FOR: The Honorable Russell C. Deyo
Under Secretary for Management

FROM: John Roth
Inspector General

SUBJECT: *Unresolved Recommendation: Audit of Security Controls for DHS Information Technology Systems and JFK International Airport, Dated January 16, 2015*

Pursuant to Office of Management and Budget Circular A-50 (Revised), DHS Management Directive 077-01, and DHS Delegation Number 00109, we are elevating TSA's non-concurrence with Recommendation 6 of OIG-15-18, *Audit of Security Controls for DHS Information Technology Systems and JFK International Airport*, dated January 16, 2015.[1] Specifically, our audit recommended that TSA "Designate the intrusion detection and surveillance Security Systems [at JFK International Airport] as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews." The Systems at issue are a number of Closed Circuit Television (CCTV) cameras and recording equipment that have been placed in the screening area at JFK International Airport (JFK) and are designed to view and record TSA checkpoint operations. The audit report is included with this memorandum as Attachment A, and a full discussion of the issue is on pages 16-23 of the audit report.

TSA believes that it is not required to designate the CCTV systems in use at JFK as a DHS IT system, and thus is not required to conduct a privacy threshold analysis or privacy impact assessment, nor is it required to fulfill security authorizations for the system. TSA's full statement of objection is

[1] DHS Delegation Number 00109 purports to delegate the Secretary's oversight of follow-up to audit recommendations made by the Office of Inspector General to the Under Secretary for Management. This delegation violates *The Inspector General Act*, section 3, which provides that the Inspector General is under the "general" supervision of the Secretary, which may be delegated only to the Deputy Secretary, and no lower. Courts have interpreted this to mean "apart from the limited supervision of the top two agency heads, no one else in the agency may provide any supervision to Inspectors General." *NRC v. FLRA*, 25 F.3d 229, 234 (4th Cir. 1994). Nevertheless, in this situation, we ask you to resolve this impasse regarding one of our recommendations.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

included in discussion at pages 22 and 23 of the audit report, as well as reprinted in full at pages 45-49 of the report. Additionally, subsequent to the audit report, TSA and DHS prepared two memoranda: one dated September 3, 2015 from Stephen Rice, TSA's Chief Information Officer, to Luke McCormack, the DHS Chief Information Officer (hereinafter the Rice Memorandum at Attachment B), and a second memorandum dated June 24, 2015, from Randi Kieffer, TSA's Chief Information Security Officer (Acting), to CIO Rice (hereinafter the Kieffer Memorandum at Attachment C).

The JFK CCTV System is a DHS IT System

Whether a system must be designated as a "DHS IT system," and thus be required to have certain management, security, and privacy controls, is governed by DHS Sensitive Systems Handbook, section 1.4.7. That section reads:

> A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) *operated by another Federal, state, or local Government agency on behalf of DHS.*

The agreement between TSA and JFK, signed by the parties in May 2012 makes clear that the CCTV system is being operated on behalf of TSA.[2]

- TSA provided over $7.2 million – 100% of the anticipated cost – for the CCTV system in question. As part of the contract signed between JFK and TSA (a contract that by its terms is judicially enforceable), JFK was to procure the system, but was to do so according to Federal contracting procedures, and to report to TSA on milestones for the project's completion.

- JFK is required to maintain and repair the system throughout its useful life. JFK is bound by the contract to make repairs in a reasonable fashion and with the same level of effort as other airport systems (owned by JFK).

- TSA and JFK's stated purpose of the system, according to the contract, was to "provide *greater surveillance of TSA areas* to enhance security at JFK, aid in the speedy resolution of claims, and assist in the resolution

[2] Other Transaction Agreement between Department of Homeland Security and The Port Authority of New York and New Jersey Regarding the John F. Kennedy International Airport (JFK) Selected Surveillance Systems, HSTS04-12-H-CT4006, included as Attachment D.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

of law enforcement issues." The contract also noted that the system was to be for the "shared use" of the parties.

- The agreement requires that JFK's video system use policy is consistent with TSA's Surveillance System Usage Policy Guidance.
- JFK is required by TSA to provide for 30 days' storage of video.
- The video time and date stamps must be synchronized appropriately, and to the satisfaction of TSA.
- TSA has the right to unlimited access to the video from the system for a variety of purposes, including TSA administrative investigations, training, or quality control. JFK conversely has no right to refuse to turn over video to TSA on request, nor does JFK have any ability to control what TSA does with the video.

The terms of the contract show TSA desired to have greater surveillance of its own areas. The award was not a grant; the money was awarded to JFK not for JFK's benefit, but for the only permissible purpose under TSA's contract authority: "to carry out the functions of the Administrator and the Administration." 49 U.S.C. §§ 106(l)(6), 114(m)(1).

TSA routinely uses the system to review Transportation Security Officer (TSO) and passenger conduct. We are aware of a number of administrative investigations conducted by TSA that use video. Video is also used in training. TSA uses the video for public relations purposes, including publishing certain TSO-passenger interactions on their public blog and on YouTube.com, where they can be viewed by millions of individuals worldwide.[3]

TSA's interests in the existence of the CCTV system vastly outweigh JFK's interests. It is in TSA's interest to ensure that the cameras are operating and maintained, that the video is preserved, and that TSA is able to make use of the video for its own purposes. Conversely, JFK has a minimal interest in checkpoint operations, since the authority and responsibility for passenger and luggage screening is TSA's alone.

[3] See e.g., https://www.youtube.com/watch?v=BkPevfpWDso; http://blog.tsa.gov/2010_11_11_archive.html; http://blog.tsa.gov/2013/04/thank-you-corporal-justin-rogers.html; https://www.youtube.com/watch?v=-Jzyp-1fhzE; http://blog.tsa.gov/2009/10/response-to-tsa-agents-took-my-son.html; A determination of whether publishing for public relations purposes videos of TSO-passenger interactions – often during times of extreme personal stress – is wise policy, or even a lawful use of personally identifiable information, is beyond the scope of this memorandum.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Other indicia that the systems are operated for the benefit of TSA include the fact that TSA takes the position in its memorandum that the video is subject to disclosure under the Freedom of Information Act (FOIA) (Kieffer Memorandum, p. 5). If TSA did not believe it owned the video in question (or at least had unlimited access to it and the right to do with it what it wished), it would not consider such videos subject to its disclosure obligations under the FOIA. TSA also filed with the National Archives and Records Administration a records destruction schedule for checkpoint video (Attachment E, items 6, 7, and 8). Finally, TSA's System of Records Notification for its Transportation Security Enforcement Record System includes videos taken in relation to the passenger screening function. 78 Federal Register 73868.

Because TSA believes its analysis on the CCTV systems extends to all airports across the county (Kieffer Memorandum, fn.3), we looked at agreements between TSA and other airports. Boston, for example, has a similar arrangement to the one at JFK, which allows TSA to have both historical and real-time access to checkpoint videos; requires the same 30 days' storage, imposes the same duty on the airport to maintain the equipment, and even has the right to dictate the camera viewing angle and pan, tilt and zoom functions. In order to accomplish this, the agreement requires Boston to provide passwords to its system for TSA's use (Attachment F). Miami-Dade Airport has a contract similar to JFK's. We believe that similar arrangements are in place across the country (Attachment G).

TSA's position

TSA's post-hoc legal analysis[4] relies on the fact that the CCTV systems in question are "owned and operated by Airport Authorities," and that the cameras themselves are on property not owned and controlled by TSA. (Kieffer memorandum p. 3, 4) There is little dispute that this is factually accurate; it is also irrelevant. The OIG's findings are based squarely on the third prong of section 1.4.7 – that these CCTV systems are operated on behalf of TSA – not that they are owned or controlled by TSA.

TSA's statement that "TSA has neither a landlord/tenant nor other contractual relationship within the meaning of Directive 4300A IT systems" (Kieffer Memorandum, p. 2) is simply inaccurate. As we noted earlier, the operation of the system is governed by contract, which by its own terms is judicially enforceable. The contract states that the purpose of the installation of the

[4] TSA produced legal justification in a memorandum signed on June 24, 2015, almost two years after the contract between JFK and TSA was signed. OIG-15-18 was delivered in final on January 16, 2015, some six months before TSA's analysis of the issue.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

CCTV system is for the shared use between JFK and TSA and is to provide greater surveillance of TSA areas. The contract gives TSA enforceable rights to access the video and requires JFK to perform specific actions to the satisfaction of TSA.

The JFK CCTV System Requires a Privacy Analysis

TSA also takes the position that the video does not implicate privacy interests under Section 222 of the Homeland Security Act or Section 208 of the E-Government Act of 2002. This is not true.

First, the argument is irrelevant under DHS policy. If the system is a "DHS system," then the component Chief Information Security Officer must ensure that it is formally assessed through a comprehensive evaluation of DHS' management, operational, and technical security controls.

Second, TSA misapprehends the nature of the privacy analysis. There should be no question that video images captured at checkpoint operations are Personally Identifiable Information (PII). DHS policy defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual." *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* (March 2012), p. 4. Images, of course, can be used to identify individuals. Depending on the circumstances, video images could even be sensitive PII, requiring special handling. DHS defines sensitive PII to include PII that "could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual." *Id.*, p.6. Certain images, if identified as part of a law enforcement or other investigation, for example, could be considered sensitive PII. In any event, any system that contains PII, as the JFK CCTV system surely does, must be considered under 4300A to be a Privacy Sensitive System.

TSA has the apparent ability to, and in fact does, broadcast interactions between TSOs and passengers, oftentimes depicting regrettable conduct, to millions worldwide. There are apparently no controls on how, when, to whom, and why these videos are distributed. To say that this implicates *no* privacy interests defies common sense.

TSA's assertion that the system does not require a privacy assessment under the E-Government Act of 2002 is also incorrect. A privacy assessment is triggered under the Act for "information technology that collects, maintains, or disseminates information that is in an identifiable form." Section 208(b)(1)(A)(i). "Identifiable form," in turn, means "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Section 208(d). Images

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

and videos, of course, permit the identity of an individual, and would thus trigger the privacy impact requirements of section 208. These should have been done prior to the system going on line.[5]

Conclusion

The facts show that JFK is operating the CCTV system at the TSA checkpoints for the benefit of TSA. TSA paid for it, requires its maintenance, has unlimited access to and control over the recordings, and uses it on a daily basis to ensure efficient checkpoint operations. As such, TSA needs to ensure that it implements the management, technical, operational, and privacy controls and reviews applicable to all other DHS information systems.

Attachments

[5] TSA notes that the system is not searchable by any personal identifiers and there is no reasonable expectation of privacy in the images. (Kieffer Memorandum, p. 5). None of those factors, even if true, bear on whether this is an information system for which a privacy analysis must be conducted, nor on whether there must be a comprehensive evaluation of its management, operational, and technical security controls. Nor does the fact that TSA could carry on operations without the system add to the analysis. Such factors are present in a number of DHS information systems.

That CCTV must undergo a privacy analysis, regardless of these factors, is confirmed by the fact that the DHS Privacy Office has routinely conducted a Privacy Impact Assessment on a number of CCTV systems throughout the Department, including on the exterior of government buildings and other publicly accessible spaces. See, *Privacy Impact Assessment for the DHS CCTV Systems*, DHS/ALL/PIA-042, (July 18, 2012) (retrieved from https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-cctv-may2013.pdf.)

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix I
Open TSA Airport IT Security Recommendations

Status	Recommendation	TSA Corrective Actions	OIG Analysis
DFW OIG-14-132, September 2014			
Resolved/ Open	3. Establish a process to report STIP computer security incidents to TSA Security Operations Center.	TSA provided documentation of its Office of Security Capabilities (OSC) Cybersecurity Management Framework and TSA OSC Cybersecurity Plan.	TSA did not provide the procedures for the TSA Service Response Center to contact the TSA SOC when there is a computer security incident.
Resolved/ Open	5. Provide required vulnerability assessment reports to the DHS Vulnerability Management Branch.	During the timeframe of the OIT fieldwork, technical problems were experienced with the scanning tool resulting in inconsistent and incomplete results.	TSA has not provided documentation that a waiver has been requested or that scan information for STIP servers at DFW are provided to the DHS Vulnerability Management Branch.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Status	Recommendation	TSA Corrective Actions	OIG Analysis
JFK OIG-15-18, January 2015			
Unresolved/ Open	6. Designate the intrusion detection and surveillance security systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.	DHS did not concur with recommendation 6. According to TSA, because the intrusion detection and surveillance security systems are owned and operated by the Airport Authority, it had no responsibility to ensure that IT security and privacy controls were met.	TSA's response does not provide for corrective actions to address the security and privacy concerns identified. DHS needs to perform security and privacy reviews of the surveillance systems at JFK airport.
SFO OIG-15-88, May 2015			
Resolved/ Open	14. Provide required vulnerability assessment reports to the DHS Vulnerability Management Branch for STIP servers tested, similar to those operating at SFO.	TSA provided documentation of its OSC Cybersecurity Management Framework and TSA OSC Cybersecurity Plan.	TSA has not provided documentation that actions have been taken.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Status	Recommendation	TSA Corrective Actions	OIG Analysis
SFO OIG-15-88, May 2015			
Resolved/ Open	15. Update the operating systems on STIP servers to a vendor-supported version that can be patched to address emerging vulnerabilities.	[redacted]	[redacted]
MCO OIG-16-87, May 2016			
Resolved/ Open	1. Ensure that IT security controls are included in STIP system design and implementation so that STIP servers are not deployed with known technical vulnerabilities.	TSA has developed a Cybersecurity Statement of Objective (SOO) to bring legacy transportation security equipment (TSE) into compliance. TSA has initially estimated that $4.66 million in future year funding.	TSA's plans satisfy the intent of this recommendation. However, implementation of this recommendation requires the issuance of the SOO, new procurements, and new support staff.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Status	Recommendation	TSA Corrective Actions	OIG Analysis
MCO OIG-16-87, May 2016			
Resolved/ Open	2. Ensure that STIP servers use approved operating systems for which the Department has established minimum security baseline configuration guidance.	TSA is working with vendors to remediate TSEs with outdated operating systems that cannot be entirely removed from the screening process due to their criticality to mission effectiveness.	Complete implementation of this recommendation includes using only approved operating systems on STIP servers.
Resolved/ Open	3. Ensure that STIP servers have the latest software patches installed so that identified vulnerabilities will not be exploited.	The Cybersecurity SOO contains necessary requirements around Operating System Currency/Security Patching. Implementation will vary and is dependent on each vendor and TSA's ability to fund those efforts.	Complete implementation of this recommendation includes using only approved operating systems, with the latest required software patches, on STIP servers.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Status	Recommendation	TSA Corrective Actions	OIG Analysis
MCO OIG-16-87, May 2016			
Resolved/ Open	4. Ensure that IT security testing is performed so that STIP servers are not deployed with known technical vulnerabilities.	Timely remediation of server vulnerabilities is one of the key requirements embedded in the TSA Cybersecurity SOO. TSA estimates that the governance document mandating scanning of STIP servers will be changed by June 30, 2016.	Complete implementation of this recommendation includes using only approved operating systems, with the latest required software patches on STIP servers, in addition to scanning these servers.
Unresolved/ Open	5. Ensure that authorized TSA staff obtain and change administrator passwords for all STIP servers at airports so that contractors no longer have full control over this equipment at airports.	TSA concurs with this recommendation. The Cybersecurity SOO includes requiring vendors with access to the TSEs to be adjudicated and controlled by TSA through the STIP. The Cybersecurity SOO mandates that TSA obtain administrative access to conduct remote security scanning of TSEs.	TSA has not provided the steps to obtain and change administrator passwords for STIP servers at airports. This recommendation is considered unresolved and will remain open until TSA provides supporting documentation that all corrective actions are completed.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

MCO OIG-16-87, May 2016			
Resolved/ Open	6. Implement a contractor oversight process so that only authorized and approved software, along with timely updates, is installed on STIP airport servers.	TSA will review logical and physical access controls as they apply to TSEs. Once TSA Cybersecurity SOO requirements are implemented, automated configuration audits will be possible to identify any unauthorized deviation from approved configuration baselines for TSEs.	Complete implementation of this recommendation includes the implementation of an oversight process, such as the identified automated configuration process.
Resolved/ Open	7. Inventory all locations at Orlando International Airport housing STIP servers and switches and ensure that these locations comply with DHS policy concerning physical security controls.	TSA is currently planning an asset inventory effort to identify and validate the locations of TSA-owned IT equipment attached to TSEs, including STIP EDS servers and associated peripherals.	While TSA is currently planning to conduct an inventory to identify the airport locations containing STIP assets, TSA has not provided the schedule for inventorying STIP locations at Orlando International Airport.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Status	Recommendation	TSA Corrective Actions	OIG Analysis
MCO OIG-16-87, May 2016			
Resolved/ Open	8. Ensure an adequate operational recovery capability for STIP servers at DC1 in case DC2 becomes inaccessible.	TSA will conduct an analysis to determine the level of effort necessary to create full operational recovery capabilities in an alternate location for the STIP servers presently operating in DC2. The implementation of the solution will depend on the availability of funds and acquisition of the engineering services required.	TSA plans to analyze the feasibility of creating a full operational recovery capability at an alternative location. However, TSA has not provided the schedule for implanting the selected capability.
Resolved/ Open	9. Establish a process for providing STIP server vulnerability assessment reports to the Department so that DHS leadership may adequately monitor system compliance capability.	TSA will review any gaps in this reporting and ensure that the reports are provided for all applicable STIP servers in the data center. The Cybersecurity SOO mandates that TSA obtain administration access to conduct remote security scanning of TSEs.	Complete implementation of this recommendation includes scanning these servers and providing the scanning results to the Department.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

MCO OIG-16-87, May 2016			
Resolved/ Open	10. Ensure that IT security requirements are included in equipment procurement contracts for IT components of STIP and passenger and checked baggage screening equipment systems as required.	TSA will specify the nine cybersecurity requirements that must be met by various vendors' TSEs prior to connection to TSANet. TSA will investigate and put into place compensating security controls as an interim risk mitigation measure as noncompliant TSEs are phased out of the enterprise. TSA will also actively investigate and put into place compensating security controls as an interim risk mitigation measure as noncompliant TSEs are phased out of the enterprise.	Complete implementation of this recommendation requires the issuance of the SOO as well as new or updated procurements.

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Status	Recommendation	TSA Corrective Actions	OIG Analysis
MCO OIG-16-87, May 2016			
Resolved/ Open	11. Institute controls so that all IT costs associated with STIP are accurately captured and reported in annual budget submissions as required.	TSA would have to redesignate the Passenger Screening Program and Electronic Baggage Screening Programs (both Non-IT DHS Level I Acquisition Programs) as IT programs in order to meet the recommendation. This redesignation would impose substantial burdens on these programs, as well as constraints on current and future TSE procurement and maintenance contracts. This would be disruptive to current security operations and impact TSA's mission readiness.	Complete implementation of this recommendation requires the capture and reporting of all IT costs associated with STIP.

Source: OIG-compiled based on data from previous reports

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix J
Office of IT Audits Contributors to This Report

Sharon Huiswoud, IT Audit Director
Kevin Burke, Supervisory IT Auditor
Charles Twitty, Senior IT Auditor
Robert Durst, Senior Program Analyst
Christopher Browning, Referencer

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Appendix K
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Director, Government Accountability Office/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
DHS CISO
DHS CISO Audit Liaison
Administrator, TSA
TSA CIO
TSA Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

~~SENSITIVE SECURITY INFORMATION~~
~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: 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 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