OFFICE OF INSPECTOR GENERAL

Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport

Homeland Security

May 7, 2015

OIG-15-88

DHS OIG HIGHLIGHTS

Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport

May 7, 2015

Why We Did This

Our audits of information technology (IT) operational, management, and technical security controls at airports provide senior Department of Homeland Security (DHS) officials with an understanding of how components have implemented IT security policies at these critical sites.

What We Recommend

We recommended that DHS improve operational controls and implement information system security patches.

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

We audited security controls for Department of Homeland Security information technology systems at San Francisco International Airport. Five Department components—U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, Management Directorate, Transportation Security Administration, and U.S. Coast Guard—operate information technology systems that support homeland security operations at this airport.

Our audit focused on how these components have implemented computer security controls for their systems at the airport and nearby locations. We performed onsite inspections of the areas where information technology systems and equipment were located, interviewed departmental staff, and conducted technical tests of computer security controls.

The information technology security controls implemented at these sites had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' systems. For example, physical security and environmental controls for server rooms need improvement. Additionally, DHS components were not scanning some onsite servers for vulnerabilities.

Agency Response

The agency concurred with 21 of the 23 recommendations. The agency did not concur with recommendations 8 and 9. We consider these recommendations unresolved and open. Additionally, based on information provided, we consider recommendations 1, 2, 4, 11, and 16, resolved and closed.

Table of Contents

Appendixes

Abbreviations

CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CVE	common vulnerabilities and exposures
DHS	Department of Homeland Security
FAMSNet	Federal Air Marshal Service Network
ICE	U.S. Immigration and Customs Enforcement

ISSO	information system security officer
IT	information technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OneNet	DHS One Network
POA&M	plan of action and milestones
SFO	San Francisco International Airport
SOC	Security Operations Center
STIP	Security Technology Integrated Program
TSA	Transportation Security Administration
WFPS	Windows File and Print System
WRFL	West Region Field Local Area Network
USCG	U.S. Coast Guard

Results of Audit

We audited security controls for the Department of Homeland Security's information technology systems at San Francisco International Airport. Five Department components—U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, Management Directorate, Transportation Security Administration, and U.S. Coast Guard—operate information technology systems that support homeland security operations at this airport.

Our audit focused on how these components have implemented operational, technical, and management controls for ensuring security of their computer systems at the airport and nearby locations. We performed onsite inspections of the areas where information technology systems and equipment were located, interviewed departmental staff, and conducted technical tests of computer security controls. We also reviewed applicable policies, procedures, and other relevant documentation.

The information technology security controls implemented at these sites had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' information technology systems. For example, physical security and environmental controls for server rooms needed improvement. The components were not scanning all onsite servers regularly for vulnerabilities. Management Directorate's information technology security policies also need improvement.

We briefed the components, and the Department's Chief Information Systems Security Officer on the results of our audit. We also made 23 recommendations addressing the control deficiencies identified in this report.

Background

We designed our audits of information technology (IT) security controls at major Department of Homeland Security (DHS) locations to provide senior DHS officials with timely information on whether the components have properly implemented IT security policies at these critical sites. Our audit program is based on *DHS Sensitive Systems Policy Directive 4300A,* version 11.0, which provides direction to DHS component managers and senior executives regarding the management and protection of sensitive systems. This directive and an associated handbook outline policies on operational, technical, and management controls necessary to ensure confidentiality, integrity, and availability within the DHS IT infrastructure and operations. These controls are as follows:

- **Operational Controls** – Focus on 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** – Focus on security controls executed by information systems. These 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.

- **Management Controls** – Focus on managing system security controls and system risk. These controls include performing risk assessments, developing rules of behavior, and ensuring that security is an integral part of both system development and IT procurement processes.

We audited security controls for IT systems supporting homeland security operations of the following DHS components at San Francisco International Airport (SFO): U.S. Customs and Border Protection (CBP), Management Directorate, U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and U.S. Coast Guard (USCG). See appendix D for details on individual DHS component activities at SFO.

CBP Did Not Comply Fully with DHS Sensitive Systems Policies

CBP did not comply fully with DHS-recommended operational, technical, and management controls for its servers and switches operating at SFO. For example, although CBP had visitor logs in the server rooms, the visitor logs were not always being used. A CBP server room exceeded the temperature range recommended by DHS policies and CBP was not addressing known server software vulnerabilities. CBP also had not appointed an information system security officer (ISSO) for the Windows File and Print System (WFPS). Finally, CBP did not determine the reason a switch failed and caused a disruption in services at SFO. Collectively, these deficiencies placed at risk the confidentiality, integrity, and availability of data stored, transmitted, and processed by CBP at SFO.

Operational Controls

CBP maintained clean server rooms that were free of excessive storage and dust. However, CBP did not implement all physical and environmental controls according to DHS policies. These physical and environmental control deficiencies involved the use of visitor logs and temperature ranges in server rooms.

Physical Security Controls

CBP had placed visitor logs in each of its server rooms. Visitors entering any of DHS facilities containing information systems, equipment, and data are required according to DHS 4300A Policy to sign the log. This control tracked the flow of traffic in and out of the server rooms. Although we observed visitor logs in each of CBP's 20 server rooms and network closets during our site visit, only 10 logs were actually being used. According to CBP staff, visitor logs were only signed when non-CBP personnel entered the network closets. CBP personnel who did not have permanent physical access authorization to the server rooms were not required to sign the visitor logs.

According to *DHS Sensitive Systems Policy Directive 4300A*:

- Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

According to the National Institute of Standards and Technologies Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*:

- Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

Consistent use of visitor logs would help ensure physical security by assigning authorized CBP personnel the responsibility to escort and monitor activity by visitors, including CBP personnel who did not have physical access authorization, in areas that house information systems, equipment, and data.

Environmental Controls

CBP did not maintain the temperature in two of the three SFO server rooms within the DHS-recommended range. Specifically, at the time of our site visit, the CBP temperature reading in one server room was 72 degrees Fahrenheit—two degrees above the allowed range—although the average Office of Inspector General (OIG) temperature reading met the requirement. In contrast, the three server rooms were all within the DHS-recommended humidity range. Table 1 provides the temperature and humidity readings for each location.

Table 1. CBP Server Rooms Temperature and Humidity Averages

Location	Recommended Temperature: 60 – 70 Degrees Fahrenheit		Recommended Humidity: 35% – 65%	
	OIG Average	CBP Reading	OIG Average	CBP Reading
Room 1	65.4	68.1	56%	56.5%
Room 2	69.3	**72**	53%	51.6%
Room 3	65.3	**70.5**	56%	43.2%

Source: OIG-compiled data based on test results.

According to *DHS 4300A Sensitive Systems Handbook*:

- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.
- Humidity in computer storage areas should be at a level between 35 percent and 65 percent.

High temperatures can damage sensitive elements of computer systems. As such, maintaining proper room temperatures is important to preserve and ensure the availability of IT equipment.

Technical Controls

In August 2014, we observed CBP staff scanning servers at SFO for vulnerabilities. These technical scans detected critical and high vulnerabilities on CBP's three servers. CBP had also provided reports of vulnerabilities for the three servers at SFO to the DHS Vulnerability Management Branch, as required. These vulnerability reports include a description of the vulnerability, and whether there are associated common vulnerabilities and exposures (CVE). Table 2 provides the number of vulnerabilities identified for each server.

Table 2. Vulnerabilities and Common Vulnerabilities and Exposures (CVE)

CBP Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Critical or High CVEs	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
Server 1	0	1	2	Yes
Server 2	1	4	7	Yes
Server 3	1	4	4	Yes

Source: OIG-compiled data based on CBP test results.

According to *DHS 4300A Sensitive Systems Handbook*:

- Information security patches shall be installed in accordance with configuration management plans and in accordance with the timeframes or direction outlined in the Information Security Vulnerability Management (ISVM) message published by the DHS Security Operations Center (SOC).

The critical vulnerabilities identified on Servers 2 and 3 related to out-of-date antivirus software. According to CBP staff, the prior contract for the antivirus software was not renewed. CBP awarded a new antivirus software contract in April 2014. However, a change request to remove the old and install the new antivirus software was put on hold until further notice.

The unique high vulnerability on Server 1 was a "false-positive" related to system design requirements. A false-positive is a vulnerability that does not actually exist but is counted in a measurement.

Management Controls

One management control is the designation of an ISSO for each information system. However, the WFPS has been without an ISSO since January 2013. According to CBP staff, a management decision still needed to be made regarding designating the WFPS ISSO.

According to *DHS 4300A Sensitive Systems Handbook*:

- An ISSO shall be designated for every information system and server as the point of contact (POC) for all security matters related to that system.

ISSOs are the primary points of contact for the information systems assigned to them. They develop and maintain each system's information security plans and are responsible for overall information system security.

ISSOs also are part of the *DHS Sensitive Systems Security Policy Directive 4300A* waiver process. Specifically, components may request waivers to, or exceptions from, any portion of this Policy Directive for up to 6 months at any time they are unable to fully comply with a Policy Directive requirement. The component's waiver requests are routed through the component's ISSO for the system, to the Component's Chief Information Security Officer (CISO) or Information Systems Security Manager, and then to the DHS CISO. However, CBP had not requested waivers or exceptions for 17 of 21 WFPS plans of action and milestones (POA&Ms) that were originally scheduled for completion by October 9, 2012. According to CBP staff, CBP will remediate findings and/or seek waivers or exceptions, as necessary, once a WFPS ISSO is designated.

System Outage at SFO

On March 28, 2014, a 6-year-old data telecommunications switch in one of the CBP SFO server rooms failed. As CBP had not established redundant data telecommunications services for its local area network at SFO, this switch failure resulted in an information system outage for CBP at SFO.

According to CBP staff, the switch failure and the lack of redundancy adversely affected automated passenger processing. While CBP was able to process passengers using a backup system, this resulted in longer processing times for arriving international passengers. Local news reports described passengers waiting in lines for hours after they disembarked from their flights.

CBP received a replacement switch the next day and returned the failed switch to the vendor. However, CBP did not request that the vendor perform a root cause analysis to determine why the switch failed even though its contract with the vendor included this option.

According to *CBP HB1400-05D, Information Systems Security Policies and Procedures Handbook*:

- Determining root cause is important because correcting the underlying cause may eliminate more than one unrelated symptom or address a condition prevalent throughout an organization.

By not requesting a root cause analysis, CBP could not take steps to determine whether failure might be systemic with this switch model or with switches of a similar age.

We recommend that the CBP Chief Information Officer (CIO) improve operational, technical, and management controls for ensuring confidentiality, integrity, and availability of data stored, transmitted, and processed at SFO by:

Recommendation 1: Requiring that individuals (e.g., employees, contractors, and others) without permanent physical access authorization credentials sign visitor logs when accessing locations containing information systems, equipment, and data.

Recommendation 2: Maintaining the temperature and humidity of the identified server rooms within the temperature and humidity ranges established by the *DHS 4300A Sensitive Systems Handbook*.

Recommendation 3: Addressing and resolving identified vulnerabilities according to the timeframes or direction stated in the Information Security Vulnerability Management message published by DHS SOC.

Recommendation 4: Designating an ISSO for the WFPS.

Recommendation 5: Requesting the vendor perform a root cause analysis to determine and address whether a failure might be systemic with the device model or with devices of a similar age, when a telecommunications device failure adversely impacts passenger processing.

Agency Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director, Departmental Government Accountability Office-OIG Audit Liaison. We have included a copy of the comments in their entirety at appendix C.

Agency Comments to Recommendation 1:

CBP concurs and has instituted a new internal procedure to ensure that visitors sign the visitor log when accessing locations containing information systems, equipment, and data. At the beginning of each month a Field Support Technician will inspect the closets and if no one has entered during the last month, it will be noted "No outside visitors within the last month" on the sign-in log sheet.

OIG Analysis of Agency Comments to Recommendation 1:

CBP's new procedure satisfies the intent of this recommendation. This recommendation is considered resolved and closed.

Agency Comments to Recommendation 2:

CBP concurs that the temperature and humidity of the server rooms were not within the established ranges as outlined in *DHS 4300A Sensitive System Handbook*. CBP's Office of Information Technology (OIT) met with the SFO authority on January 2015 and the ambient air thermostats were lowered 2 degrees in those areas.

OIG Analysis of Agency Comments to Recommendation 2:

CBP's actions to lower the ambient air thermostats satisfy the intent of this recommendation. This recommendation is considered resolved and closed.

Agency Comments to Recommendation 3:

CBP concurs that identified vulnerabilities need to be addressed and resolved according to the timeframe or direction stated in the Information Security Vulnerability Management message published by DHS SOC.

OIG Analysis of Agency Comments to Recommendation 3:

CBP's actions satisfy the intent of this recommendation. CBP estimated that it will satisfy this recommendation on or by September 30, 2015. This recommendation is considered resolved but will remain open until CBP provides supporting documentation that the planned corrective actions are completed.

Agency Comments to Recommendation 4:

CBP concurs that an ISSO is needed for the WFPS. On December 3, 2014, CBP designated an ISSO for the WFPS.

OIG Analysis of Agency Comments to Recommendation 4:

CBP's designation of an ISSO for the WFPS satisfies the intent of this recommendation. This recommendation is considered resolved and closed.

Agency Comments to Recommendation 5:

CBP concurs that some situations may require that a root cause analysis be conducted by the vendor. However, CBP states that device failures as a result of mechanical parts are usually due to normal wear and tear and do not require further analysis. CBP OIT has monitoring in place today. When an outage cause is unknown, CBP OIT currently performs a root cause analysis and brings in relevant government and contractor resources to research and identify the cause.

OIG Analysis of Agency Comments to Recommendation 5:

We agree that CBP has procedures in place to request a root cause analysis on failed data telecommunications devices. However, it is our opinion that these procedures should be expanded to request a root cause analysis whenever a data telecommunications device failure adversely impacts passenger processing. This recommendation is considered resolved but will remain open until CBP provides supporting documentation that all corrective actions are completed.

ICE Did Not Comply Fully with DHS Sensitive Systems Policies

ICE complied fully with DHS-recommended technical and management controls for its IT equipment operating at SFO. However, ICE did not comply fully with DHS-recommended operational controls for its servers and switches located at the airport. For example, an ICE server room exceeded the temperature range as required by DHS policies. Table 3 provides both the temperature and humidity readings for this location.

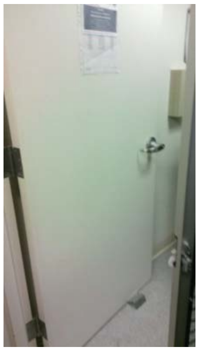
Table 3. ICE Server Room Temperature and Humidity Averages

Location	Recommended Temperature: 60 – 70 Degrees Fahrenheit		Recommended Humidity: 35% – 65%	
	OIG Average	ICE Reading	OIG Average	ICE Reading
Room 1	**72.4**	**74.3**	53.1%	49%

Source: OIG-compiled data based on test results.

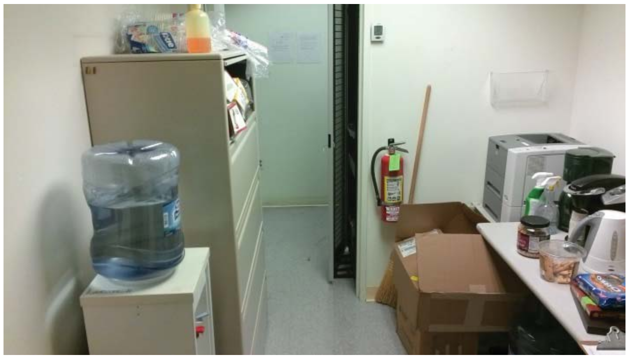
Unapproved methods to control the room temperature exacerbated the situation. Specifically, this server was located in a closet within an ICE break room in an ICE-controlled area. Both the outer door and the door to the server rack were permanently propped open due to the inability to keep the server cool. However, leaving the door open inappropriately provided all ICE staff and visitors with access to the IT equipment in this area. (See figures 1 and 2.)

Figure 1. Outer Door



Source: OIG.

Figure 2. Rack Door



Source: OIG.

Because the data telecommunications switch located in this closet was the sole telecommunications link for two other ICE switches at SFO, it constituted a single point of failure for information processing at SFO.

There was another ICE switch located in a CBP-operated server room with adequate environmental and physical security controls. According to staff we interviewed, ICE had not considered moving the server from its current location to the CBP server room as ICE did not have unrestricted access to that CBP space.

According to *DHS 4300A Sensitive Systems Handbook*:

- Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit.

- Humidity should be at a level between 35 percent and 65 percent.

- 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.

- Risk and Infrastructure – A risk-based management decision is made on the requirements for telecommunication services. The availability requirements for the system will determine the time period within which the system connections must be available. If continuous availability is required, redundant telecommunications services may be an option.

Physical security vulnerabilities such as high temperatures can damage sensitive elements of computer systems. Therefore, the maintenance of proper temperatures is important to ensure the availability and preservation of IT equipment. Further, uncontrolled access and single points of failure that are not mitigated place at risk the confidentiality, integrity, and availability of ICE data processing.

Recommendation 6. We recommend that the ICE CIO determine the cost effectiveness of relocating the ICE SFO server to an existing CBP server room at SFO that ensures adequate physical and environmental controls, and take appropriate action.

Agency Comments and OIG Analysis

Agency Comments to Recommendation 6:

ICE concurs and will determine if it is cost effective to relocate the ICE SFO server to an existing CBP server room or alternate solutions at SFO. ICE estimated that it will satisfy this recommendation on or by September 30, 2015.

OIG Analysis of Agency Comments to Recommendation 6:

ICE's actions to determine if it is cost effective to relocate the ICE SFO server to an existing CBP server room satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until ICE provides supporting documentation that the planned corrective actions are completed.

Management Directorate Needs to Improve DHS Sensitive Systems Policies

We did not identify operational, technical, or managerial control deficiencies related to Management Directorate's IT resources onsite at SFO. However, we identified areas in DHS system security policies that could be improved. The DHS CISO within the Management Directorate is the authority for interpretation, clarification, and modification of the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook*, including all appendices and attachments.

Physical Security Controls

The Management Directorate could improve its policy regarding use of visitor logs. This policy, as outlined in the *DHS 4300A Sensitive Systems Handbook*, is as follows:

- Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

However, the *DHS 4300A Sensitive Systems Handbook* did not define who is a visitor. This lack of definition has created concerns with adhering to the visitor log requirement. The Management Directorate would benefit from using a definition of a visitor found in government-wide criteria. For example, according to National Institute of Standards and Technologies Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*:

- Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

Environmental Controls

DHS policy did not equally specify recommended temperature ranges for both unclassified and classified systems. The *DHS 4300A Sensitive Systems Handbook* distinguished between guidance for DHS Sensitive Systems and DHS National Security Systems. The *DHS 4300A Sensitive Systems Handbook* recommended temperature and humidity ranges for sensitive systems. However, all DHS National Security Systems were to use guidance provided in the *DHS National Security Systems Policy Directive 4300B* series, dated April 19, 2013, which was available on the DHS CISO website. According to DHS National Security Systems Policy Instruction Number 4300B.102 Version 9.0, “National Security System Security Control Guidance”:

- The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at acceptable levels, as defined by the organization; [DHS] and b. Monitors temperature and humidity levels periodically.

However, *Policy Directive 4300B* did not specify recommended temperature or humidity ranges for server rooms containing classified systems. The directive was silent in this regard.

Technical Controls

DHS could improve its guidance regarding domain controllers. The *DHS Windows Server 2008 Configuration Guidance* Version 2012.6, June 2012, provided guidance on the configuration of servers using the Windows 2008 Server software. However, this guidance did not apply to Windows 2008 Servers being used as domain controllers.

According to *DHS Windows Server 2008 Configuration Guidance:*

- This document is not for domain controllers, general use servers, or other specialized servers. The common baseline configuration for these systems will be addressed in future baseline configuration guidance and future updates to this document.

As of November 2014, a Windows 2008 server configuration guidance document for domain controllers had not been issued by the Office of the Chief Information Security Officer.

We recommend the DHS CISO improve DHS system security policies by:

Recommendation 7. Including the government-wide definition of "visitor" in the *DHS 4300A Sensitive Systems Handbook*.

Recommendation 8. Authorizing use of the *DHS 4300A Sensitive Systems Handbook* for classified systems until the *DHS National Security Systems Policy Directive 4300B* is updated to provide guidance in the area of environmental controls.

Recommendation 9. Authorizing use of the *DHS Windows Server 2008 Configuration Guidance 4300A Sensitive Systems Handbook* for configuration of servers used as domain controllers until specific domain controller guidance is issued.

Agency Comments and OIG Analysis

Agency Comments to Recommendation 7:

The DHS CISO concurs and will include the government-wide definition of "visitor" in the next version of the *DHS 4300A Sensitive Systems Handbook*. This is expected to be completed on or by June 30, 2015.

OIG Analysis of Agency Comments to Recommendation 7:

The DHS CISO actions to include the government-wide definition of "visitor" in the next version of the *DHS 4300A Sensitive Systems Handbook* satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until the DHS CISO provides documentation that the planned corrective actions are completed.

Agency Comments to Recommendation 8:

The DHS CISO does not concur with this recommendation. According to the

DHS CISO, the *DHS National Security Systems Policy Directive 4300B* Version 9.0, dated April 19, 2013, addresses environmental controls. Specifically, the policy is not detailed as to the exact temperature or humidity range, as it is left up to the organization to provide "acceptable levels" at those facilities. The DHS CISO requests that OIG consider this recommendation resolved and closed.

OIG Analysis of Agency Comments to Recommendation 8:

We do not agree that this recommendation should be resolved and closed. We agree that the current Departmental guidance on environmental controls in the *DHS National Security Systems Policy Directive 4300B* is not detailed. However, this lack of detail places an undue burden on the components to determine the operating temperatures of all critical assets in server rooms housing National Security Systems. This recommendation is considered unresolved and will remain open until the DHS CISO provides documentation that corrective actions are completed.

Agency Comments to Recommendation 9:

The DHS CISO does not concur with this recommendation. According to the DHS CISO, Windows Server 2008 has reached the end of its mainstream support lifecycle. Instead of using the Windows Server 2008 guidance for the domain controllers, the components will be directed to use Server 2012 Active Directory guidance, for which there is existing configuration guidance. The DHS CISO requests that OIG consider this recommendation resolved and closed.

OIG Analysis of Agency Comments to Recommendation 9:

We agree that Windows Server 2008 has reached the end of its mainstream support lifecycle. However, the DHS CISO has not provided the documentation informing components that alternate guidance should be used for domain controllers with this operating system. This recommendation is considered unresolved and will remain open until the DHS CISO provides documentation that corrective actions are completed.

TSA Did Not Comply Fully with DHS Sensitive Systems Policies

TSA did not comply fully with DHS-recommended operational, technical, and management controls for its servers and switches operating at SFO. For example, not all TSA IT equipment was physically secured from access by unauthorized staff and contractors. One switch at SFO was a single point of failure for 23 other TSA switches. Further, technical scans identified several vulnerabilities on TSA servers operating at SFO. Collectively, these deficiencies placed at risk the confidentiality, integrity, and availability of data stored, transmitted, and processed by TSA at SFO.

Operational Controls

Operational controls implemented for TSA server rooms and communications closets containing IT equipment at SFO and at the nearby TSA and Federal Air Marshal Service facilities did not conform fully to DHS policies. Deficiencies existed in both physical security and environmental controls. TSA's IT equipment at SFO also did not provide redundant data telecommunications to ensure system connectivity in the event of a hardware failure.

Physical Security Controls

Not all TSA IT equipment at SFO was physically secured from unauthorized staff/contractors. According to *DHS 4300A Sensitive Systems Handbook*:

- 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.

However, some TSA telecommunications racks were not completely enclosed. This made it possible for non-authorized individuals to gain access and potentially damage or compromise TSA IT equipment. Further, non-TSA equipment was located in some TSA racks. This equipment included closed-circuit television equipment owned by the airport but purchased with TSA funds. As a result, non-authorized personnel needed access to racks containing TSA equipment. This placed TSA IT equipment at risk of unauthorized access and potential damage or modification.

Environmental Controls

The temperatures for seven TSA server rooms at SFO did not meet the DHS requirement. However, the TSA server rooms were within the recommended DHS humidity range. Table 4 provides the temperature and humidity readings for each location.

Table 4. TSA Server Rooms Temperature and Humidity Averages

Location	Recommended Temperature: 60 – 70 Degrees Fahrenheit		Recommended Humidity: 35% – 65%	
	OIG Average	TSA Reading	OIG Average	TSA Reading
Room 1[1]	**77.3**	**70.4**	42.1%	50.4%
Room 2	**73.8**	**73.2**	44.6%	47%
Room 3	**71.1**	66	44.1%	No sensor.
Room 4	**75.2**	**71.6**	39.5%	46%
Room 5	**70.5**	**72**	55.9%	50%
Room 6	68.6	68	53.6%	55%
Room 7	**70.9**	66	54.4%	No sensor.
Room 8	69.2	**71**	52.8%	No sensor.
Room 9	No OIG reading.[2]	No sensor.	No OIG reading.	No sensor.

Source: OIG-compiled data based on test results.

According to *DHS 4300A Sensitive Systems Handbook*:

- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.
- Humidity should be at a level between 35 percent and 65 percent.

High temperatures can damage sensitive elements of computer systems. Therefore, maintaining proper storage room temperature is important to ensure the availability and preservation of IT equipment.

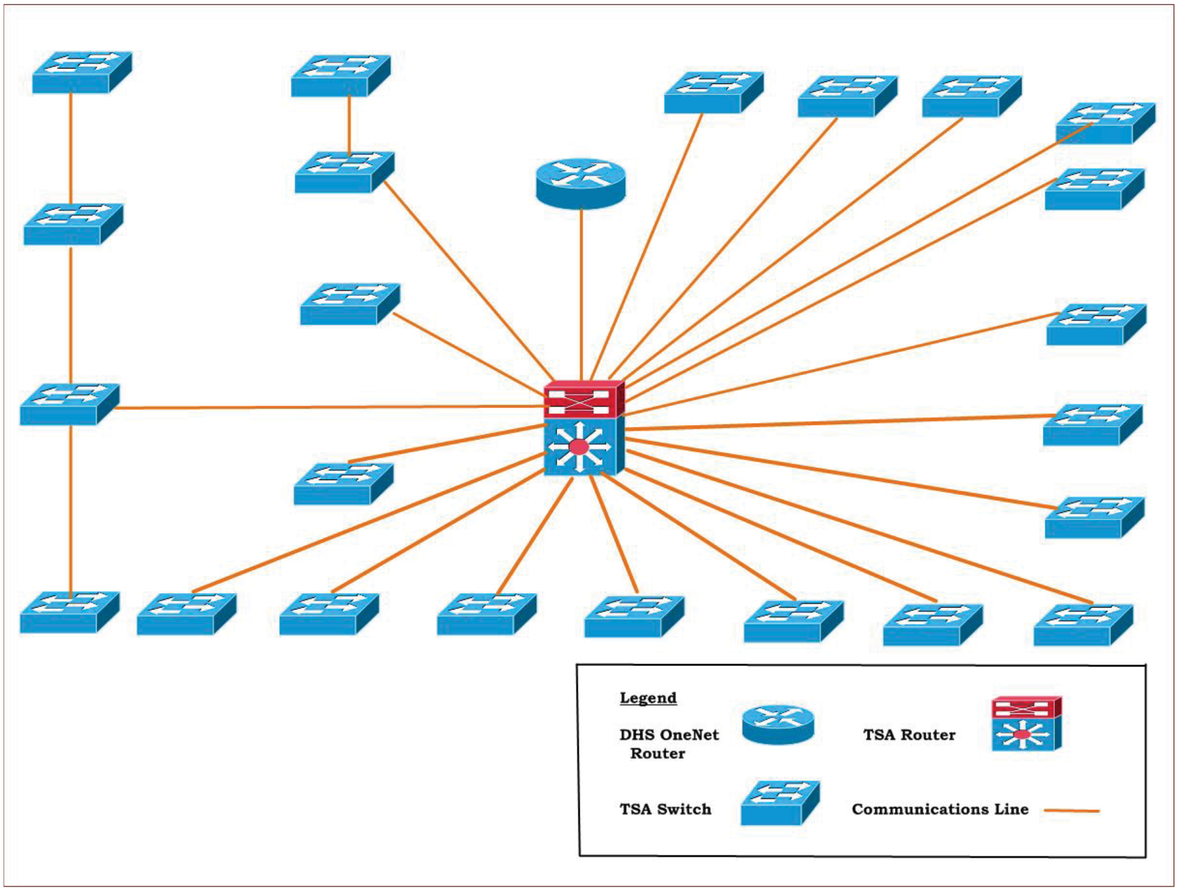
Redundant Data Telecommunications Services

Based on our analysis of data provided by TSA, one telecommunication device represented a single point of failure for 23 other switches at SFO. This means that if this one switch experiences a hardware failure, TSA staff at SFO would not have remote access to other TSA IT resources. See figure 3 for details.

[1] According to TSA staff, they have corrected the temperature deficiency in this room since the time of our site visit.

[2] OIG auditors did not record temperature and humidity in the TSA room with classified IT equipment.

Figure 3. TSA Data Telecommunications Network at SFO



Source: OIG-compiled based on data obtained from TSA.

During our onsite visit, we observed that the switch representing a single point

of failure 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 staff, they have since corrected the temperature deficiency in this room.

According to *DHS 4300A Sensitive Systems Handbook*:

- Risk and Infrastructure – A risk-based management decision is made on the requirements for telecommunication services. The availability requirements for the system will determine the time period within which the system connections must be available. If continuous availability is required, redundant telecommunications services may be an option.

Technical Controls

According to *DHS 4300A Sensitive Systems Handbook*:

- Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management (ISVM) message published by the DHS SOC.

Further, detailed vulnerability assessment scan schedules and results are to be provided to the DHS Vulnerability Management Branch in order to satisfy requirements for enterprise-wide security awareness of assets and risks. However, TSA had not provided vulnerability assessment reports to the DHS Vulnerability Management Branch for one of these SFO servers.

In October 2014, we observed while TSA staff scanned the remotely accessible TSA servers located at SFO. These technical scans detected critical and high vulnerabilities on all seven servers, including vulnerabilities that could be exploited for denial of service or code execution attacks. A software update, e.g., a "patch," for one of the vulnerabilities was first released in 2007, but the vulnerability still had not been addressed. According to TSA, one of the high vulnerabilities was a false-positive as the associated account had been disabled. Table 5 provides the number of vulnerabilities for each server.

Table 5. Vulnerabilities and CVEs

TSA Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Critical or High CVEs	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
Server 1	0	3	1	Yes
Server 2	1	6	6	Yes
Server 3	1	16	12	Yes
Server 4	0	4	4	Yes
Server 5	0	3	1	No
Server 6	0	4	3	Yes
Server 7	0	3	1	Yes
Total:	2	39	28	

Source: OIG-compiled data based on TSA test results.

Additionally, the Security Technology Integrated Program (STIP) servers that TSA operated at SFO also had potential vulnerabilities. According to TSA, these STIP servers were not connected to the Transportation Security Administration Network and therefore could not be scanned remotely either by us or TSA officials. As such, TSA did not provide vulnerability assessments of these servers to DHS as required.

Nonetheless, in coordination with TSA staff, we identified two STIP servers with the same operating systems as the STIP servers at SFO. In November 2014, we observed while TSA staff scanned these similar servers. These technical scans detected critical and high vulnerabilities on both servers. Additionally, the software vendor has not been supporting the operating system on Server 2 since December 2011. Lack of support implied that no new security patches for the product would be released by the vendor and the software was likely to contain security vulnerabilities. Table 6 provides the number of vulnerabilities for each STIP server that was scanned.

Table 6. STIP Vulnerabilities and CVEs

STIP Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Critical or High CVEs	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
Server 1	11	155	848	Not Reported
Server 2	4	2	4	Not Reported
Total:	15	157	852	

Source: OIG-compiled data based on test results.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data. For example, one of the vulnerabilities could allow attackers to carry out denial of service attacks on TSA's information systems. A denial of service attack could result in the IT resources not being able to perform their required functions.

Management Controls

Management controls, including the POA&M process for TSA systems operating at SFO, did not conform fully to DHS policies. Information system owners use the POA&M process to manage vulnerabilities and correct deficiencies in security controls. However, POA&Ms for the Federal Air Marshal's Network and the Infrastructure Core System did not address TSA's lack of an effective recovery site. According to TSA staff, there was an enterprise-level POA&M that documented this recovery deficiency.

According to *DHS 4300A Sensitive Systems Handbook*, the component CISO is to:

- Implement and manage a Plan of Action and Milestones (POA&M) process for remediation by creating a POA&M for each known vulnerability.

Management controls also include documenting in the system's information security plan all the system's assets. While we reported in September 2014 that not all STIP assets were documented in the information security plan, TSA is taking steps to address this deficiency.[3] However, as TSA included new STIP transportation security equipment within the STIP boundary, TSA also needed to document the security controls for these new IT assets and also re-authorize the STIP to operate. TSA had created a high-level milestone plan for completing this re-authorization by May 31, 2015.

The goal of the authorization process is to allow a component's authorizing official to accept the residual risk to the Department's operations or assets. It is our opinion, however, that the STIP system may now be too large for one authorization package to adequately document the risks inherent in operating the STIP. TSA could place STIP servers in one system and STIP transportation security equipment in another system, just as it does for other systems. For example, TSA has placed file and print servers in its Infrastructure Core Services system while placing desktops in its Enterprise User Computing system. However, TSA has not decided to break the STIP into two or more systems based on similar operating characteristics.

According to *DHS 4300A Sensitive Systems Handbook*:

- It is recommended that components pursue *Type Security Authorization Process* for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, and security needs; and reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments.

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

We recommend that the TSA CIO improve operational, technical, and management controls for ensuring confidentiality, integrity, and availability of data stored, transmitted, and processed at SFO by:

Recommendation 10. Complying with DHS policy concerning physical security and temperature at SFO locations housing TSA servers.

Recommendation 11. Determining whether it is necessary and cost effective to establish redundant data telecommunications services at SFO and taking appropriate action.

Recommendation 12. Scanning TSA servers routinely to resolve identified vulnerabilities in accordance with the timeframe or direction stated in the DHS SOC's Information Security Vulnerability Management message.

Recommendation 13. Providing required vulnerability assessment reports to the DHS Vulnerability Management Branch for servers operating at SFO.

Recommendation 14. Providing required vulnerability assessment reports to the DHS Vulnerability Management Branch for STIP servers tested, similar to those operating at SFO.

Recommendation 15. Updating the operating systems on STIP servers to a vendor-supported version that can be patched to address emerging vulnerabilities.

Recommendation 16. Documenting in the Infrastructure Core System and Federal Air Marshal Service Network (FAMSNet) POA&Ms, the lack of an effective recovery site.

Recommendation 17. Determining whether it is necessary and cost effective to use 'type' authorization for STIP servers.

Agency Comments and OIG Analysis

Agency Comments to Recommendation 10:

TSA concurs and will ensure that temperature and humidity sensors are installed and functional at SFO locations housing TSA servers. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

OIG Analysis of Agency Comments to Recommendation 10:

TSA's actions to implement temperature and humidity sensors partially implement this recommendation. TSA has not provided documentation that all SFO server rooms are within the required temperature range. Additionally, TSA has not provided documentation supporting actions to resolve identified physical security issues. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 11:

TSA concurs and has conducted a review to determine whether it is necessary and cost effective to establish redundant data telecommunications services at SFO. According to the review performed by TSA, it would not be cost effective to install redundant data circuits for each of the individual circuits 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 given the multiple communications and connectivity capabilities already available. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

OIG Analysis of Agency Comments to Recommendation 11:

TSA's determination that it is not necessary or cost effective to establish redundant data telecommunications services at SFO satisfies the intent of this recommendation. This recommendation is considered resolved and closed.

Agency Comments to Recommendation 12:

TSA concurs and has provided a copy of the Information Assurance and Cyber Security Division Standard Operating Procedure 1401: *Plan of Action and Milestones (POA&M) Process,* which outlines TSA's POA&M process. Additionally, TSA servers are scanned on a monthly basis to identify and resolve vulnerabilities. The results or data feeds containing the results are submitted to the DHS Vulnerability Management Branch on the 21st of every month via the Continuous Monitoring Working Group SharePoint site. Data feeds support Information Security Scorecard reporting, Office of Management and Budget CyberScope monthly reporting, and the Federal Information Security Management Act Inventory. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

OIG Analysis of Agency Comments to Recommendation 12:

TSA has provided procedures for resolving technical vulnerabilities on its servers. However, TSA has not provided documentation supporting the resolution of all critical and high vulnerabilities identified on FAMSNet and Infrastructure Core Services servers at SFO. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 13:

TSA concurs and says that the Infrastructure Core Services and FAMSNet systems are scanned on a monthly basis and the results or data feeds are submitted to the DHS Vulnerability Management Branch on the 21st of every month via the Continuous Monitoring Working Group SharePoint site. Also, screen captures showing that the .NET service packs have been updated on the associated target servers have been provided to OIG under separate cover. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

OIG Analysis of Agency Comments to Recommendation 13:

TSA's procedures to scan servers on a monthly basis satisfy the intent of this recommendation. However, TSA has not provided documentation that all identified servers are now included in monthly reports to the Department. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 14:

TSA concurs and is planning for the development of a detailed project plan by August 31, 2015. This plan will identify the following five key areas:

1. IT Security Scanning
2. Physical Security
3. Access Control
4. External Interfaces
5. IT Security Requirements for Vendors

OIG Analysis of Agency Comments to Recommendation 14:

TSA's project 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 15:

TSA concurs and is currently working toward development of a detailed project plan to ensure sustainable IT security. TSA's Office of Security Capability will leverage approved IT Security clauses from the CIO to insert into current and future contracts. The project plan will be completed by August 31, 2015.

OIG Analysis of Agency Comments to Recommendation 15:

TSA's development of project plans satisfies 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 16:

TSA concurs and has documented in the Infrastructure Core Services and FAMSNet POA&Ms the need for an effective recovery site. The FAMSNet Authority to Operate package includes the Security Assessment Report that lists all vulnerabilities discovered during the assessment. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

OIG Analysis of Agency Comments to Recommendation 16:

TSA's inclusion of the recovery site vulnerability in the Infrastructure Core Services and FAMSNet POA&Ms satisfies the intent of this recommendation. This recommendation is considered resolved and closed.

Agency Comments to Recommendation 17:

TSA concurs and agrees that an assessment needs to be conducted to determine the necessity and cost-effectiveness of conducting a type authorization of STIP servers. The research on a 'type' authorization (as defined by NIST SP 800-37 Revision 1) will be accomplished by the end of calendar year 2015.

OIG Analysis of Agency Comments to Recommendation 17:

TSA plans to research 'type' authorization for the STIP satisfythe intent of this recommendation. This recommendation is considered resolved, but will remain open until TSA provides documentation to support that the planned corrective actions have been completed.

USCG Did Not Comply Fully with DHS Sensitive Systems Policies

USCG did not comply fully with DHS-recommended operational and technical controls for its servers and switches operating at SFO. Specifically, the two USCG server rooms we reviewed had excessive storage and exceeded temperature ranges established by DHS policies. USCG had not established redundant telecommunications capability at SFO. The USCG also had not patched a software program to address known vulnerabilities.[4] Collectively, these deficiencies placed at risk the confidentiality, integrity, and availability of data stored, transmitted, and processed by USCG at SFO.

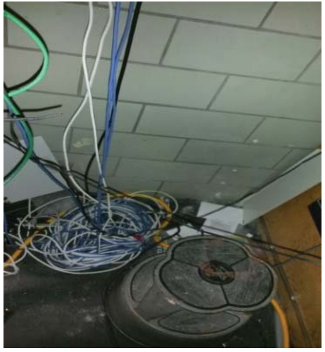
Operational Controls

USCG did not maintain uncluttered, clean server rooms as required. In addition, the temperatures in two USCG server rooms did not comply with DHS policies.

Excess Storage and Housekeeping

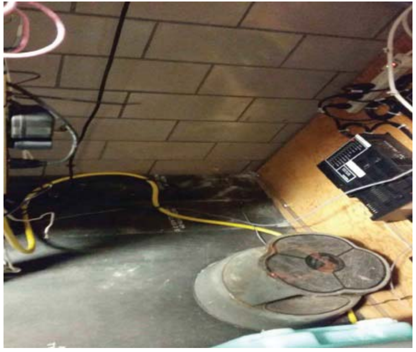
USCG server rooms and telecommunications closets onsite at SFO were used for surplus storage. Specifically, we observed a server room storing excess wire and a telecommunications closet filled with boxes, chairs, and wire. Following our June 2014 site visit, USCG began addressing the issue by removing items that should not be stored in rooms containing IT resources. (See figures 4a and 4b, and 5a and 5b.)

Figure 4a. Before



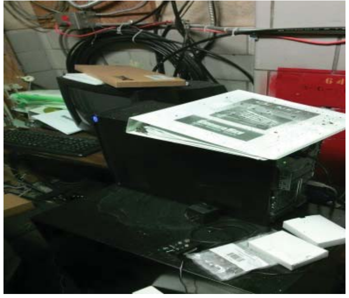
Source: OIG.

Figure 4b. After



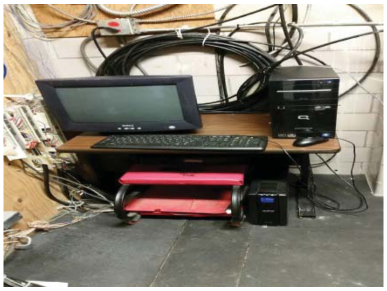
Source: USCG.

Figure 5a. Before



Source: OIG.

Figure 5b. After

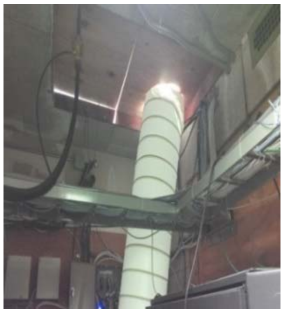


Source: USCG.

[4] USCG complied fully with DHS recommended management controls for its IT equipment operating at SFO.

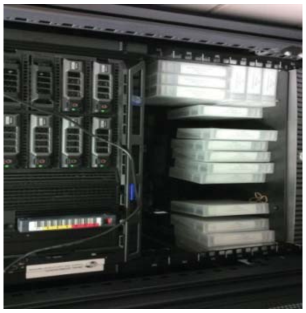
Further, there was excessive dust in one server room. The accumulated dust was due to a room above that was being refurbished and an air conditioner duct that was not completely sealed at the roof area. (See figure 6.) Backup tapes, exposed to contamination and the elements due to storage in the same room placed USCG's data recovery capability at risk. (See figure 7.)

Figure 6. Ventilation Tube



Source: OIG.

Figure 7. Backup Tapes



Source: OIG.

According to *DHS 4300A Sensitive Systems Handbook*:

- Dusting of hardware and vacuuming of work areas should be performed weekly with trash removal performed daily.
- Backup copies of data should be stored at secure offsite locations.

Dust accumulation inside of computer monitors and hard drives is a hazard that can damage data processing equipment. Dust buildup also can cause IT equipment to perform slowly, adversely affecting the USCG's ability to record daily flight information to support its search and rescue mission.

Environmental Controls

USCG's two server rooms at SFO exceeded the temperature range allowed by DHS policies for unclassified systems.[5] However, both server rooms were within the established humidity range. Table 7 provides the temperature and humidity readings for each location.

[5] Temperature and humidity requirements were not included in the *DHS 4300B National Security System Policy*.

Table 7. USCG Server Rooms Temperature and Humidity Averages

Location	Recommended Temperature: 60 – 70 Degrees Fahrenheit		Recommended Humidity: 35% – 65%	
	OIG Average	USCG Reading	OIG Average	USCG Reading
Room 1	**73.8**	70	39.1%	65%
Room 2	No OIG reading.[6]	**80**	No OIG reading.	41%

Source: OIG-compiled based on data from testing results.

The high temperature in Room 1 was related to the area above being refurbished and the ceiling not being completely enclosed. The air conditioning was not working in the classified server room, causing it to overheat. Since our June 2014 site visit, the air conditioning equipment has been replaced.

According to *DHS 4300A Sensitive Systems Handbook*:

- Temperatures in computer storage areas should be between 60 and 70 degrees Fahrenheit.
- Humidity should be at a level between 35 percent and 65 percent.

High temperatures can damage sensitive elements of computer systems. Therefore, maintaining proper server room temperature is important to ensure the availability and preservation of IT equipment.

Redundant Data Telecommunications Services

USCG had one telecommunications provider and had not arranged for redundant telecommunications capability at SFO. Although USCG had two telecommunications circuits, both were provided by the same vendor. As a result, mission performance at SFO was vulnerable to disruption in the event that the one telecommunications service provider experienced operational problems. According to USCG staff, USCG is currently installing another telecommunications line with a different telecommunications service provider. Once installed, the USCG would have built-in redundancy. Therefore, if one telecommunications service provider experiences disruption, USCG will be able to switch to the second telecommunications service provider.

According to *DHS 4300A Sensitive Systems Handbook*:

- Risk and Infrastructure – A risk-based management decision is made on the requirements for telecommunications services. The availability requirements for the system will determine the time period within which the system connections must be available. If continuous availability is

[6] OIG Auditors did not record temperature and humidity in the USCG room with classified IT equipment.

required, redundant telecommunications services may be an option.

Technical Controls

In July 2014, we observed USCG staff performing technical scans of the one USCG server located at SFO. The technical scans detected a critical vulnerability on the server. Table 8 provides the total number of vulnerabilities on this server.

Table 8. Vulnerabilities and CVEs

USCG Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Critical or High CVEs	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
Server 1	1	1	20	Yes

Source: OIG-compiled based on data from testing results.

The vulnerabilities on this server were related to an out-of-date version of a software package and missing information security patches. USCG had not reported these vulnerabilities in its POA&M. However, during our field work, USCG tested and installed an updated version of the software to provide the missing information security patches.

According to *DHS 4300A Sensitive Systems Handbook*:

- Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management (ISVM) message published by the DHS SOC.

Missing information security patches place USCG systems at risk. Addressing vulnerabilities and implementing information security patches on a consistent basis can mitigate the risks to USCG IT systems integrity and availability.

We recommend the USCG CIO improve operational, technical, and management controls for ensuring confidentiality, integrity, and availability of data stored, transmitted, and processed at SFO by:

Recommendation 18. Ensuring compliance with DHS policy concerning housekeeping at SFO locations housing USCG IT equipment.

Recommendation 19. Storing backup tapes in a secure location as required.

Recommendation 20. Maintaining server room temperatures within DHS-recommended ranges.

Recommendation 21. Providing for redundancy in telecommunications services.

Recommendation 22. Addressing known vulnerabilities by applying the necessary information security patches.

Recommendation 23. Documenting known vulnerabilities in a POA&M.

Agency Comments and OIG Analysis

Agency Comments to Recommendation 18:

USCG concurs and will comply with DHS policy concerning housekeeping at SFO locations housing USCG IT equipment by May 31, 2015. USCG has begun addressing the housekeeping issue by removing items that should not be stored in rooms containing IT resources.

OIG Analysis of Agency Comments to Recommendation 18:

USCG actions to address housekeeping issues at SFO locations housing IT equipment satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until USCG provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 19:

USCG concurs and will store backup tapes in a secure location as required by May 31, 2015.

OIG Analysis of Agency Comments to Recommendation 19:

USCG plans to store backup tapes in a secure location satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCG provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 20:

USCG concurs and will maintain server room temperatures within DHS-recommended ranges. This is estimated to be completed by May 31, 2015.

OIG Analysis of Agency Comments to Recommendation 20:

USCG plans to maintain server room temperatures within DHS-recommended ranges satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until USCG provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 21:

USCG concurs and will provide for redundancy in telecommunications services. This is estimated to be completed by May 31, 2015.

OIG Analysis of Agency Comments to Recommendation 21:

USCG plans to provide for telecommunications redundancy satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until USCG provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 22:

USCG concurs and will address known vulnerabilities by applying the necessary information security patches. This is estimated to be completed by May 31, 2015.

OIG Analysis of Agency Comments to Recommendation 22:

USCG plans to apply the necessary information security patches satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until USCG provides supporting documentation that all corrective actions are completed.

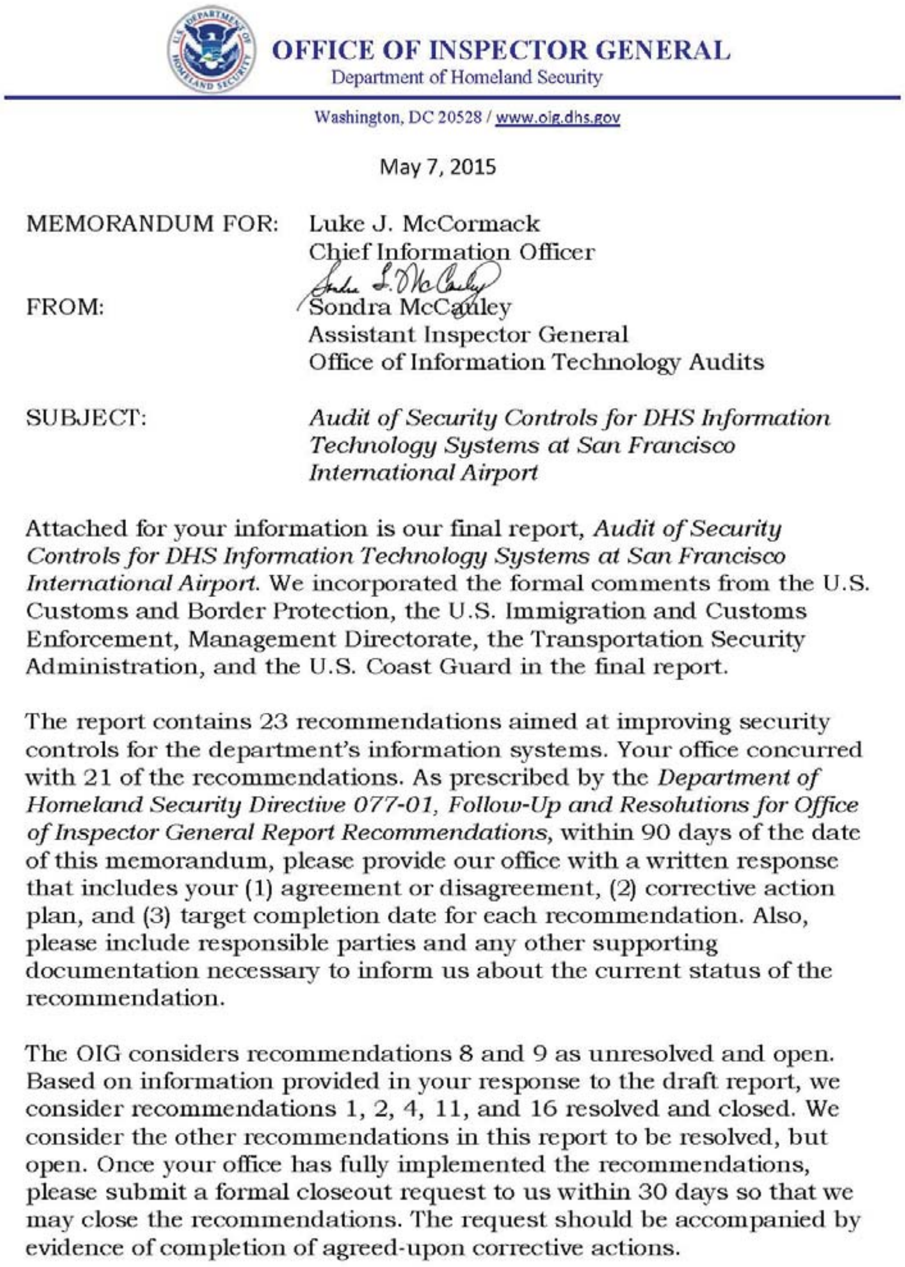
Agency Comments to Recommendation 23:

USCG concurs and will document known vulnerabilities in a POA&M. This is estimated to be completed by May 31, 2015.

OIG Analysis of Agency Comments to Recommendation 23:

USCG plans to document known vulnerabilities in a POA&M satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until USCG provides supporting documentation that all corrective actions are completed.

Appendix A
Transmittal to Action Official



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 7, 2015

MEMORANDUM FOR: Luke J. McCormack
Chief Information Officer

Sondra L. McCauley

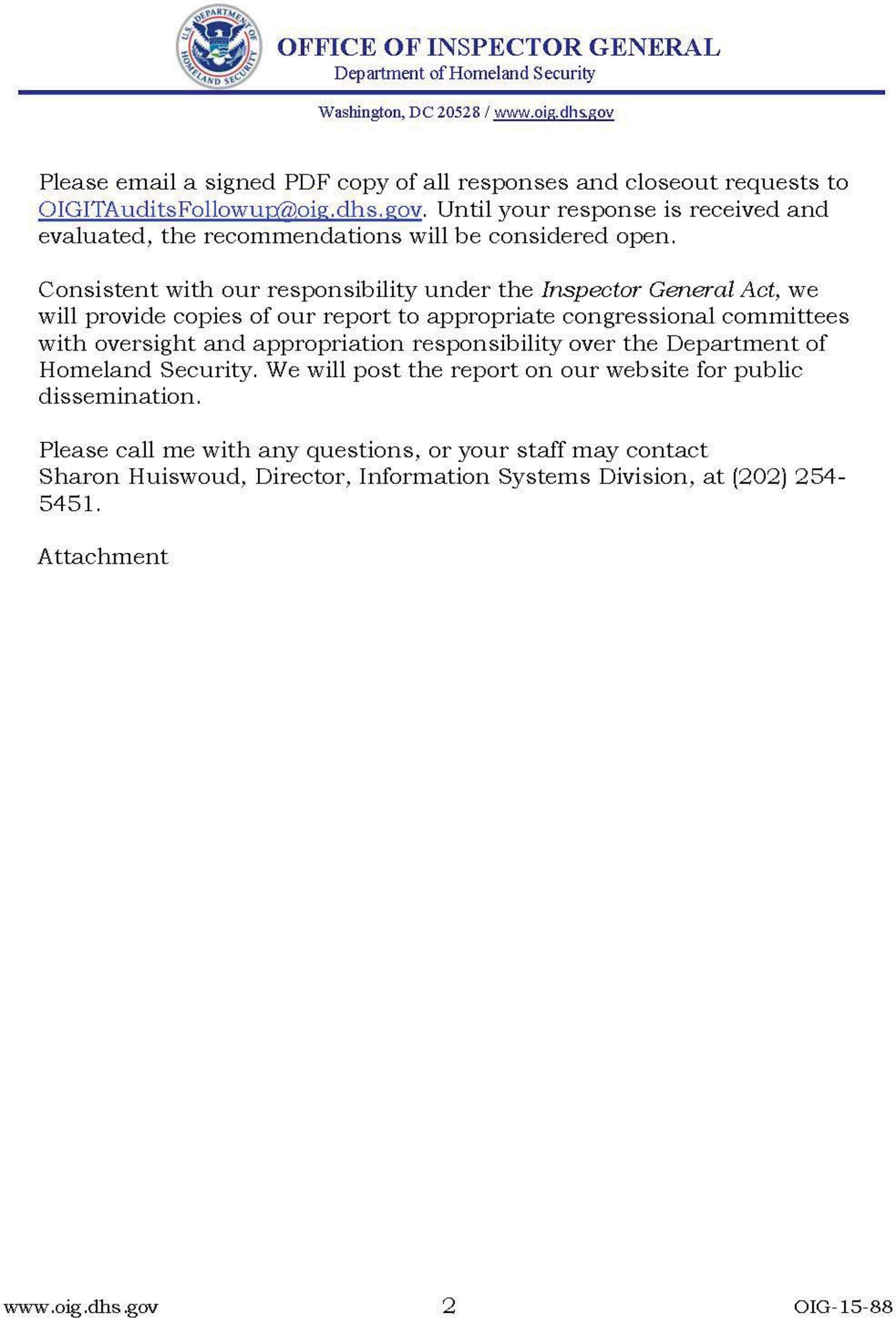
FROM: Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport*

Attached for your information is our final report, *Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport*. We incorporated the formal comments from the U.S. Customs and Border Protection, the U.S. Immigration and Customs Enforcement, Management Directorate, the Transportation Security Administration, and the U.S. Coast Guard in the final report.

The report contains 23 recommendations aimed at improving security controls for the department's information systems. Your office concurred with 21 of the recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions 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.

The OIG considers recommendations 8 and 9 as unresolved and open. Based on information provided in your response to the draft report, we consider recommendations 1, 2, 4, 11, and 16 resolved and closed. We consider the other recommendations in this report to be resolved, but 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 the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sharon Huiswood, Director, Information Systems Division, at (202) 254-5451.

Attachment

Appendix B
Scope and Methodology

The Department of Homeland Security Office of Inspector General 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.

This audit is part of a program to examine, on an ongoing basis, the implementation of DHS technical and information security policies and procedures at DHS sites. The objective of this program is to determine the extent to which critical DHS sites comply with the Department's technical and information security policies and procedures, according to *DHS Sensitive Systems Policy Directive 4300A* and its companion document, the *DHS 4300A Sensitive Systems Handbook.* Our primary focus was on auditing the security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS IT infrastructure at this site. For example, we recorded temperature and humidity at different locations in the server rooms, and averaged these readings. We also recorded component humidity and temperature readings obtained from component sensors that existed in the rooms during field work. We then compared these readings with DHS guidance.

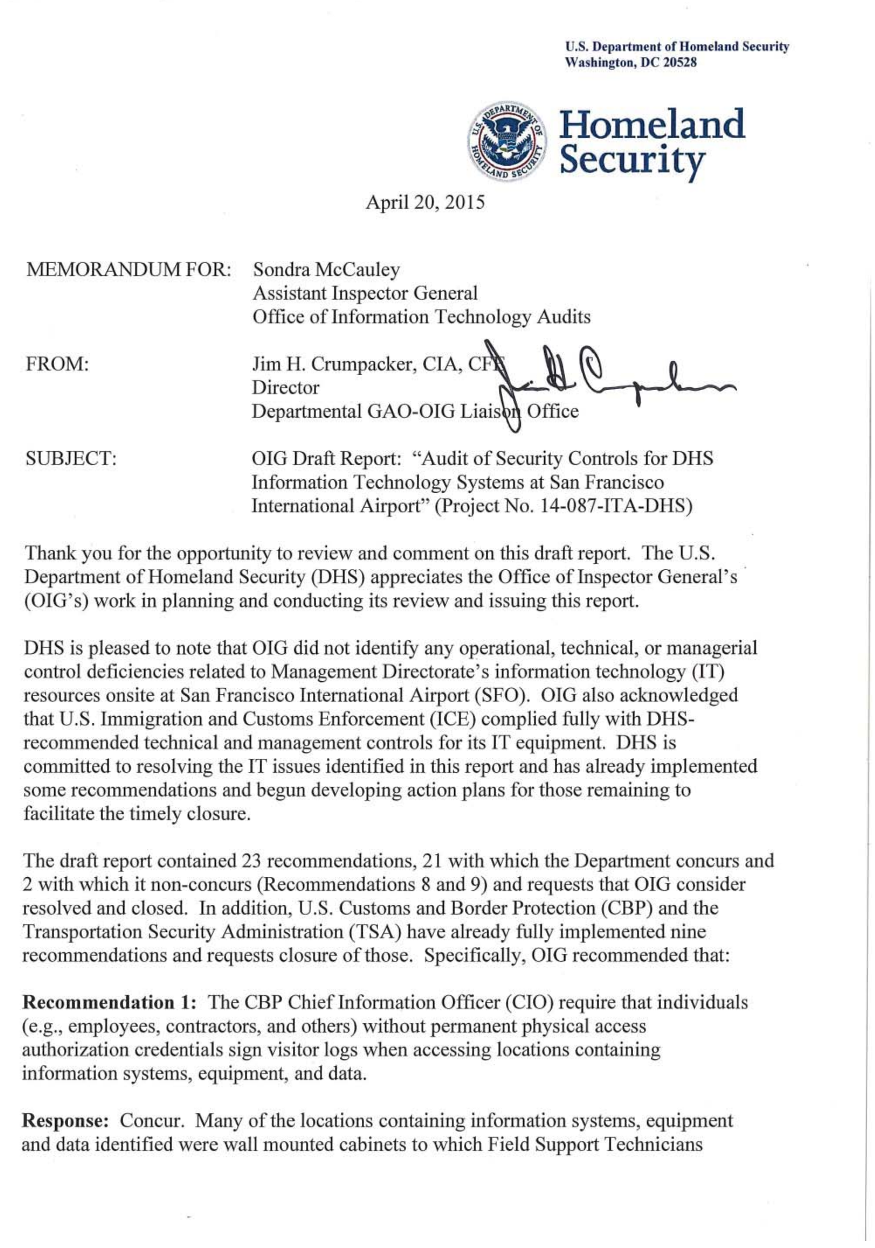
We coordinated the implementation of this audit of IT security controls with the DHS CISO. We interviewed CBP, ICE, Management Directorate, TSA, and USCG staff. We conducted visits to CBP, ICE, TSA, and USCG facilities at and near SFO. We compared the DHS IT infrastructure that we observed on site with the documentation provided by the auditees. We observed DHS staff performing vulnerability scans on servers that could be accessed remotely. We also watched TSA staff perform vulnerability scans on servers similar to servers operating at SFO that could not be accessed remotely.

We reviewed Information Assurance Compliance System documentation, such as the authority-to-operate letter, contingency plans, and system security plans. We reviewed guidance provided by DHS to its components in the areas of system documentation, information security patch management, and wireless security. We reviewed applicable DHS and component policies and procedures, as well as government-wide guidance. We provided briefings and presentations to DHS staff on the results of our field work and the information summarized in this report.

We conducted this performance audit between May 2014 and November 2014 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.

We appreciate the efforts of DHS management and staff to provide the information and access necessary to accomplish this review. The principal OIG points of contact for the audit are Sondra McCauley, Assistant Inspector General for Information Technology Audits, (202) 254-4100, and Sharon Huiswoud, Director of the Information Systems Division, (202) 254-5451. Major OIG contributors to the audit are identified in appendix E.

Appendix C
Agency Comments to the Draft Report



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

April 20, 2015

MEMORANDUM FOR: Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: OIG Draft Report: "Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport" (Project No. 14-087-ITA-DHS)

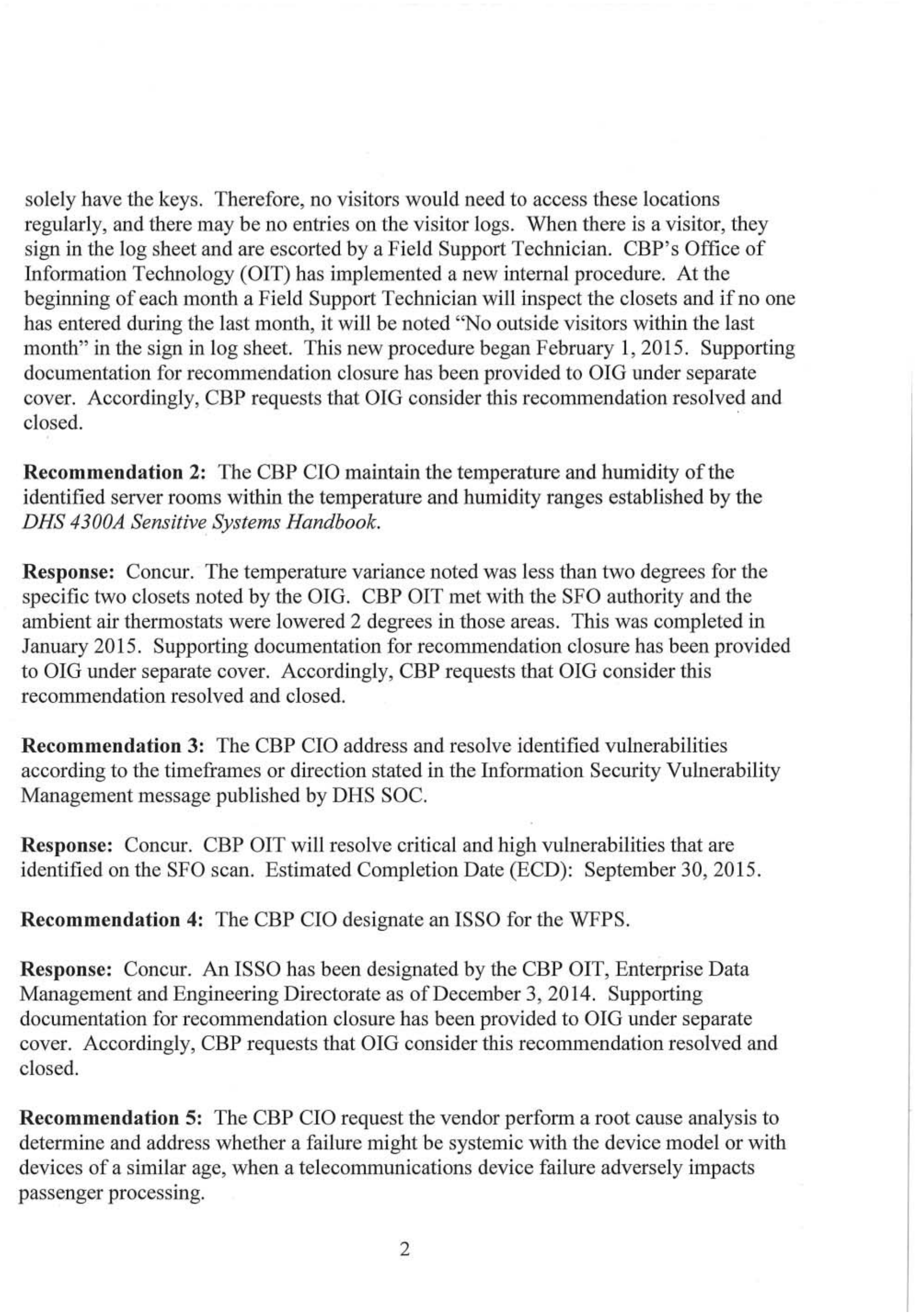
Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

DHS is pleased to note that OIG did not identify any operational, technical, or managerial control deficiencies related to Management Directorate's information technology (IT) resources onsite at San Francisco International Airport (SFO). OIG also acknowledged that U.S. Immigration and Customs Enforcement (ICE) complied fully with DHS-recommended technical and management controls for its IT equipment. DHS is committed to resolving the IT issues identified in this report and has already implemented some recommendations and begun developing action plans for those remaining to facilitate the timely closure.

The draft report contained 23 recommendations, 21 with which the Department concurs and 2 with which it non-concurs (Recommendations 8 and 9) and requests that OIG consider resolved and closed. In addition, U.S. Customs and Border Protection (CBP) and the Transportation Security Administration (TSA) have already fully implemented nine recommendations and requests closure of those. Specifically, OIG recommended that:

Recommendation 1: The CBP Chief Information Officer (CIO) require that individuals (e.g., employees, contractors, and others) without permanent physical access authorization credentials sign visitor logs when accessing locations containing information systems, equipment, and data.

Response: Concur. Many of the locations containing information systems, equipment and data identified were wall mounted cabinets to which Field Support Technicians



solely have the keys. Therefore, no visitors would need to access these locations regularly, and there may be no entries on the visitor logs. When there is a visitor, they sign in the log sheet and are escorted by a Field Support Technician. CBP's Office of Information Technology (OIT) has implemented a new internal procedure. At the beginning of each month a Field Support Technician will inspect the closets and if no one has entered during the last month, it will be noted "No outside visitors within the last month" in the sign in log sheet. This new procedure began February 1, 2015. Supporting documentation for recommendation closure has been provided to OIG under separate cover. Accordingly, CBP requests that OIG consider this recommendation resolved and closed.

Recommendation 2: The CBP CIO maintain the temperature and humidity of the identified server rooms within the temperature and humidity ranges established by the *DHS 4300A Sensitive Systems Handbook*.

Response: Concur. The temperature variance noted was less than two degrees for the specific two closets noted by the OIG. CBP OIT met with the SFO authority and the ambient air thermostats were lowered 2 degrees in those areas. This was completed in January 2015. Supporting documentation for recommendation closure has been provided to OIG under separate cover. Accordingly, CBP requests that OIG consider this recommendation resolved and closed.

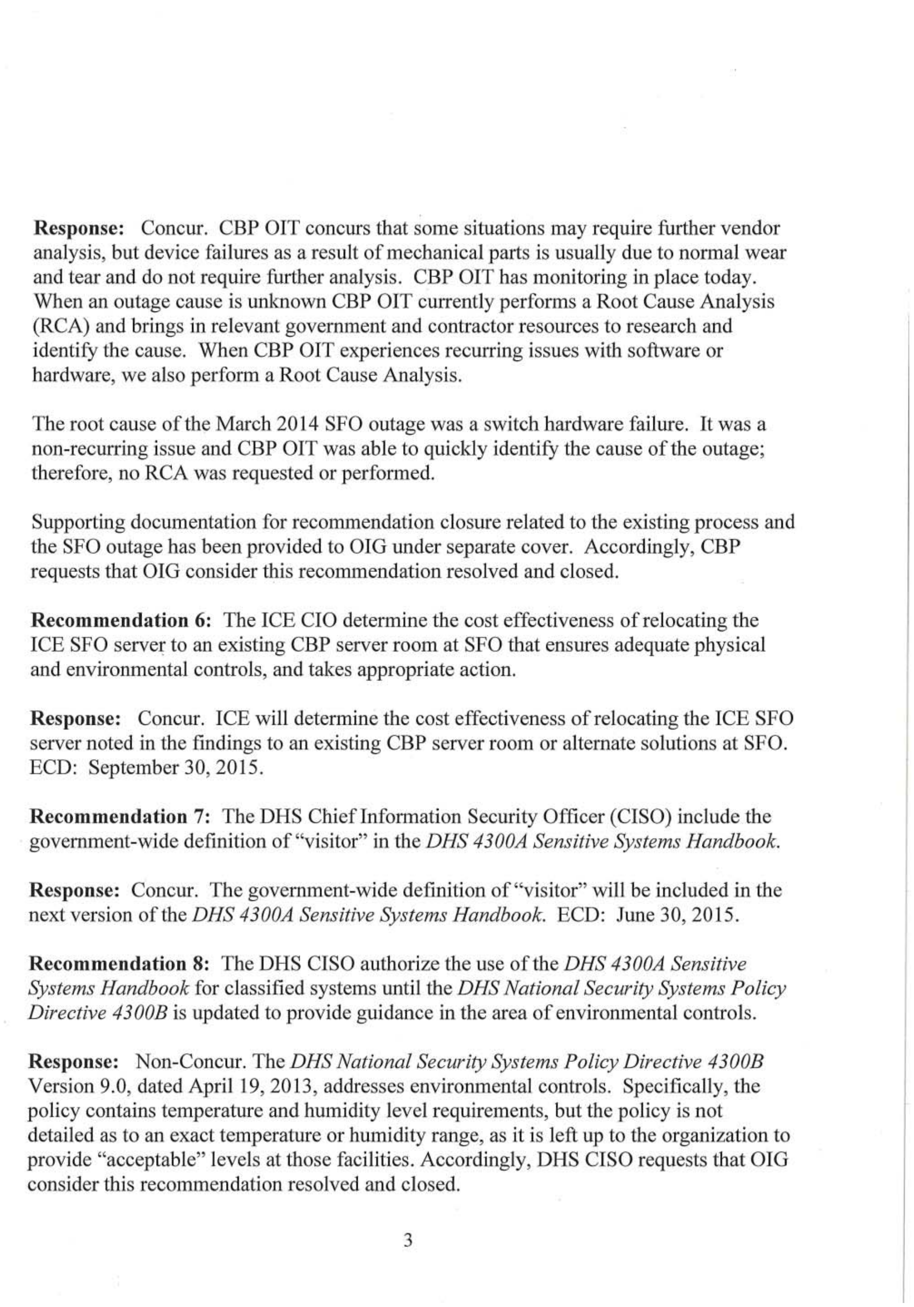
Recommendation 3: The CBP CIO address and resolve identified vulnerabilities according to the timeframes or direction stated in the Information Security Vulnerability Management message published by DHS SOC.

Response: Concur. CBP OIT will resolve critical and high vulnerabilities that are identified on the SFO scan. Estimated Completion Date (ECD): September 30, 2015.

Recommendation 4: The CBP CIO designate an ISSO for the WFPS.

Response: Concur. An ISSO has been designated by the CBP OIT, Enterprise Data Management and Engineering Directorate as of December 3, 2014. Supporting documentation for recommendation closure has been provided to OIG under separate cover. Accordingly, CBP requests that OIG consider this recommendation resolved and closed.

Recommendation 5: The CBP CIO request the vendor perform a root cause analysis to determine and address whether a failure might be systemic with the device model or with devices of a similar age, when a telecommunications device failure adversely impacts passenger processing.



Response: Concur. CBP OIT concurs that some situations may require further vendor analysis, but device failures as a result of mechanical parts is usually due to normal wear and tear and do not require further analysis. CBP OIT has monitoring in place today. When an outage cause is unknown CBP OIT currently performs a Root Cause Analysis (RCA) and brings in relevant government and contractor resources to research and identify the cause. When CBP OIT experiences recurring issues with software or hardware, we also perform a Root Cause Analysis.

The root cause of the March 2014 SFO outage was a switch hardware failure. It was a non-recurring issue and CBP OIT was able to quickly identify the cause of the outage; therefore, no RCA was requested or performed.

Supporting documentation for recommendation closure related to the existing process and the SFO outage has been provided to OIG under separate cover. Accordingly, CBP requests that OIG consider this recommendation resolved and closed.

Recommendation 6: The ICE CIO determine the cost effectiveness of relocating the ICE SFO server to an existing CBP server room at SFO that ensures adequate physical and environmental controls, and takes appropriate action.

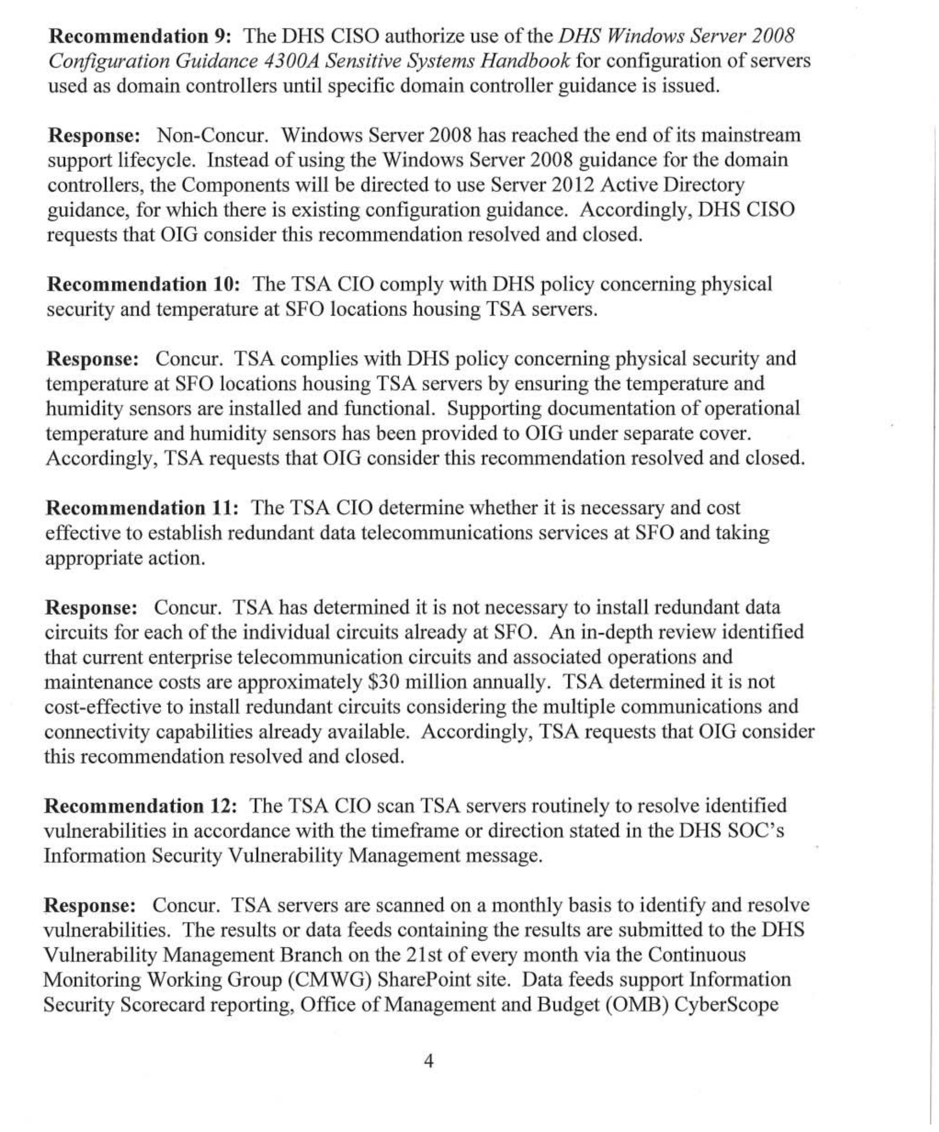
Response: Concur. ICE will determine the cost effectiveness of relocating the ICE SFO server noted in the findings to an existing CBP server room or alternate solutions at SFO. ECD: September 30, 2015.

Recommendation 7: The DHS Chief Information Security Officer (CISO) include the government-wide definition of "visitor" in the *DHS 4300A Sensitive Systems Handbook*.

Response: Concur. The government-wide definition of "visitor" will be included in the next version of the *DHS 4300A Sensitive Systems Handbook*. ECD: June 30, 2015.

Recommendation 8: The DHS CISO authorize the use of the *DHS 4300A Sensitive Systems Handbook* for classified systems until the *DHS National Security Systems Policy Directive 4300B* is updated to provide guidance in the area of environmental controls.

Response: Non-Concur. The *DHS National Security Systems Policy Directive 4300B* Version 9.0, dated April 19, 2013, addresses environmental controls. Specifically, the policy contains temperature and humidity level requirements, but the policy is not detailed as to an exact temperature or humidity range, as it is left up to the organization to provide "acceptable" levels at those facilities. Accordingly, DHS CISO requests that OIG consider this recommendation resolved and closed.



Recommendation 9: The DHS CISO authorize use of the *DHS Windows Server 2008 Configuration Guidance 4300A Sensitive Systems Handbook* for configuration of servers used as domain controllers until specific domain controller guidance is issued.

Response: Non-Concur. Windows Server 2008 has reached the end of its mainstream support lifecycle. Instead of using the Windows Server 2008 guidance for the domain controllers, the Components will be directed to use Server 2012 Active Directory guidance, for which there is existing configuration guidance. Accordingly, DHS CISO requests that OIG consider this recommendation resolved and closed.

Recommendation 10: The TSA CIO comply with DHS policy concerning physical security and temperature at SFO locations housing TSA servers.

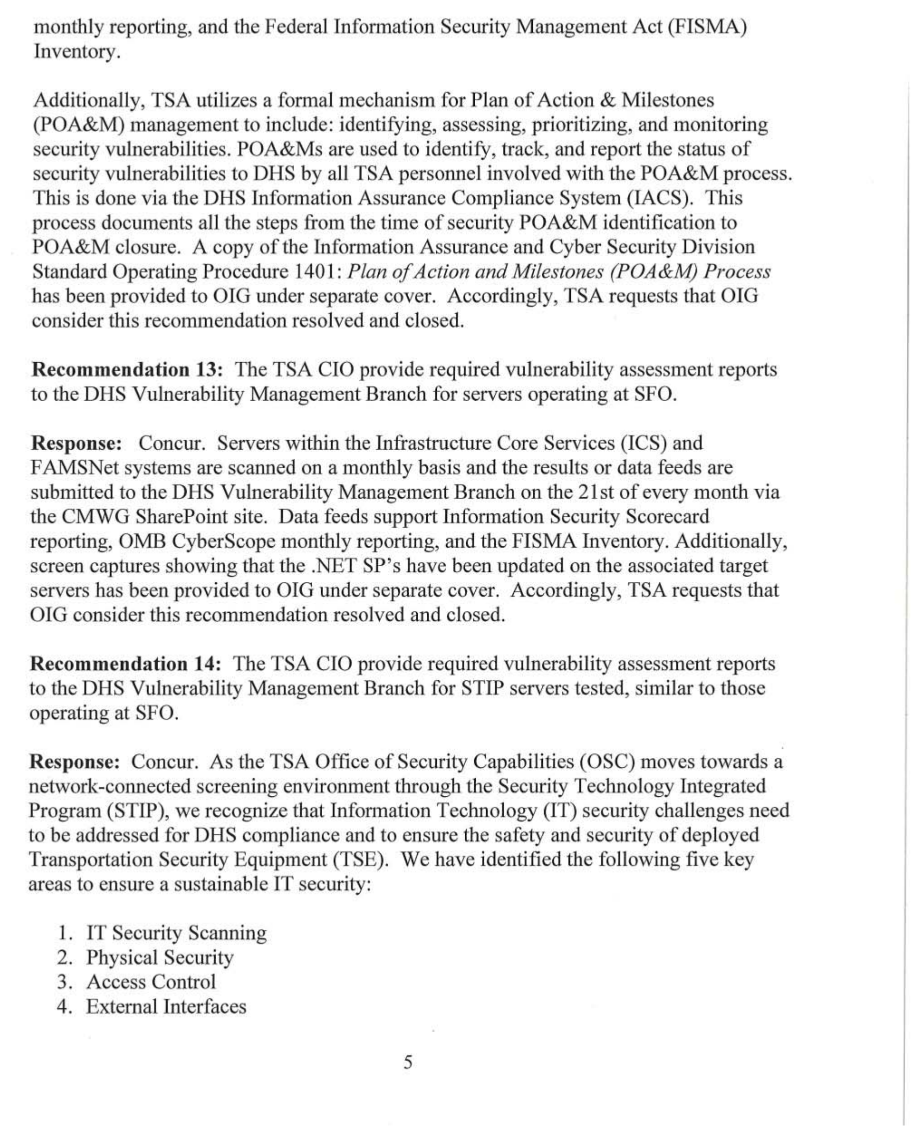
Response: Concur. TSA complies with DHS policy concerning physical security and temperature at SFO locations housing TSA servers by ensuring the temperature and humidity sensors are installed and functional. Supporting documentation of operational temperature and humidity sensors has been provided to OIG under separate cover. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 11: The TSA CIO determine whether it is necessary and cost effective to establish redundant data telecommunications services at SFO and taking appropriate action.

Response: Concur. 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. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 12: The TSA CIO scan TSA servers routinely to resolve identified vulnerabilities in accordance with the timeframe or direction stated in the DHS SOC's Information Security Vulnerability Management message.

Response: Concur. TSA servers are scanned on a monthly basis to identify and resolve vulnerabilities. The results or data feeds containing the results are submitted to the DHS Vulnerability Management Branch on the 21st of every month via the Continuous Monitoring Working Group (CMWG) SharePoint site. Data feeds support Information Security Scorecard reporting, Office of Management and Budget (OMB) CyberScope



monthly reporting, and the Federal Information Security Management Act (FISMA) Inventory.

Additionally, TSA utilizes a formal mechanism for Plan of Action & Milestones (POA&M) management to include: identifying, assessing, prioritizing, and monitoring security vulnerabilities. POA&Ms are used to identify, track, and report the status of security vulnerabilities to DHS by all TSA personnel involved with the POA&M process. This is done via the DHS Information Assurance Compliance System (IACS). This process documents all the steps from the time of security POA&M identification to POA&M closure. A copy of the Information Assurance and Cyber Security Division Standard Operating Procedure 1401: *Plan of Action and Milestones (POA&M) Process* has been provided to OIG under separate cover. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

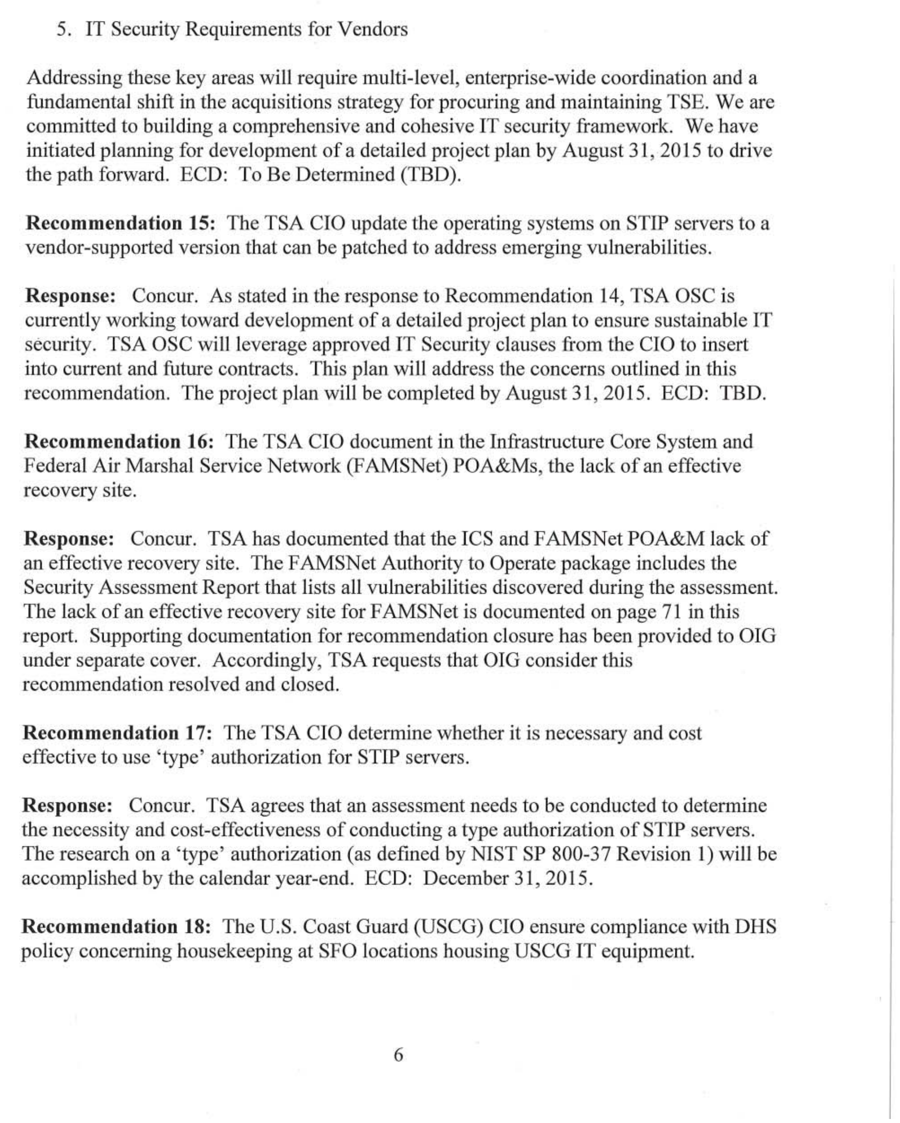
Recommendation 13: The TSA CIO provide required vulnerability assessment reports to the DHS Vulnerability Management Branch for servers operating at SFO.

Response: Concur. Servers within the Infrastructure Core Services (ICS) and FAMSNet systems are scanned on a monthly basis and the results or data feeds are submitted to the DHS Vulnerability Management Branch on the 21st of every month via the CMWG SharePoint site. Data feeds support Information Security Scorecard reporting, OMB CyberScope monthly reporting, and the FISMA Inventory. Additionally, screen captures showing that the .NET SP's have been updated on the associated target servers has been provided to OIG under separate cover. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 14: The TSA CIO provide required vulnerability assessment reports to the DHS Vulnerability Management Branch for STIP servers tested, similar to those operating at SFO.

Response: Concur. As the TSA Office of Security Capabilities (OSC) moves towards a network-connected screening environment through the Security Technology Integrated Program (STIP), we recognize that Information Technology (IT) security challenges need to be addressed for DHS compliance and to ensure the safety and security of deployed Transportation Security Equipment (TSE). We have identified the following five key areas to ensure a sustainable IT security:

1. IT Security Scanning
2. Physical Security
3. Access Control
4. External Interfaces



5. IT Security Requirements for Vendors

Addressing these key areas will require multi-level, enterprise-wide coordination and a fundamental shift in the acquisitions strategy for procuring and maintaining TSE. We are committed to building a comprehensive and cohesive IT security framework. We have initiated planning for development of a detailed project plan by August 31, 2015 to drive the path forward. ECD: To Be Determined (TBD).

Recommendation 15: The TSA CIO update the operating systems on STIP servers to a vendor-supported version that can be patched to address emerging vulnerabilities.

Response: Concur. As stated in the response to Recommendation 14, TSA OSC is currently working toward development of a detailed project plan to ensure sustainable IT security. TSA OSC will leverage approved IT Security clauses from the CIO to insert into current and future contracts. This plan will address the concerns outlined in this recommendation. The project plan will be completed by August 31, 2015. ECD: TBD.

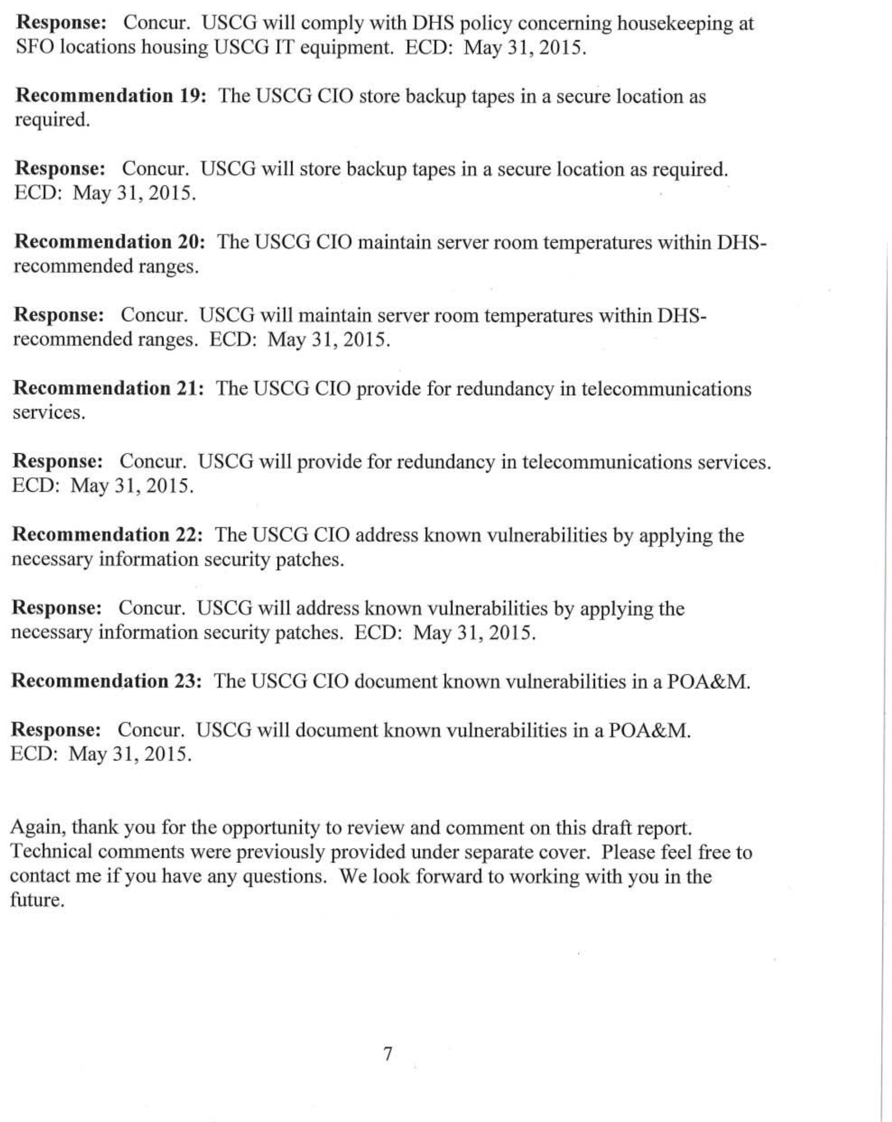
Recommendation 16: The TSA CIO document in the Infrastructure Core System and Federal Air Marshal Service Network (FAMSNet) POA&Ms, the lack of an effective recovery site.

Response: Concur. TSA has documented that the ICS and FAMSNet POA&M lack of an effective recovery site. The FAMSNet Authority to Operate package includes the Security Assessment Report that lists all vulnerabilities discovered during the assessment. The lack of an effective recovery site for FAMSNet is documented on page 71 in this report. Supporting documentation for recommendation closure has been provided to OIG under separate cover. Accordingly, TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 17: The TSA CIO determine whether it is necessary and cost effective to use 'type' authorization for STIP servers.

Response: Concur. TSA agrees that an assessment needs to be conducted to determine the necessity and cost-effectiveness of conducting a type authorization of STIP servers. The research on a 'type' authorization (as defined by NIST SP 800-37 Revision 1) will be accomplished by the calendar year-end. ECD: December 31, 2015.

Recommendation 18: The U.S. Coast Guard (USCG) CIO ensure compliance with DHS policy concerning housekeeping at SFO locations housing USCG IT equipment.



Response: Concur. USCG will comply with DHS policy concerning housekeeping at SFO locations housing USCG IT equipment. ECD: May 31, 2015.

Recommendation 19: The USCG CIO store backup tapes in a secure location as required.

Response: Concur. USCG will store backup tapes in a secure location as required. ECD: May 31, 2015.

Recommendation 20: The USCG CIO maintain server room temperatures within DHS-recommended ranges.

Response: Concur. USCG will maintain server room temperatures within DHS-recommended ranges. ECD: May 31, 2015.

Recommendation 21: The USCG CIO provide for redundancy in telecommunications services.

Response: Concur. USCG will provide for redundancy in telecommunications services. ECD: May 31, 2015.

Recommendation 22: The USCG CIO address known vulnerabilities by applying the necessary information security patches.

Response: Concur. USCG will address known vulnerabilities by applying the necessary information security patches. ECD: May 31, 2015.

Recommendation 23: The USCG CIO document known vulnerabilities in a POA&M.

Response: Concur. USCG will document known vulnerabilities in a POA&M. ECD: May 31, 2015.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Appendix D
DHS Activities at San Francisco International Airport

U.S. Customs and Border Protection

At SFO, CBP personnel staff up to 80 primary passenger lanes.[7] These personnel review flight data for terrorist-related activities, collect duties and, when CBP discovers a violation of law, assess fines and civil penalties. CBP staff at nearby locations use IT equipment to perform cargo manifest and outbound passenger review and targeting.

We audited IT security controls at the following CBP locations:

- Central Block,
- SFO Terminals 1, A and G, and
- SFO International Terminal.

CBP staff at these locations use the following systems:

- West Region Field Local Area Network (WRFL) –The WRFL provides the General Support Network Infrastructure and end points for DHS/CBP users. The WRFL consists of 158 geographically dispersed sites utilizing over 3,000 devices connected to the DHS One Network (OneNet) for providing application services to CBP field offices. The WRFL incorporates desktop computers, laptops, printers, interconnected wiring, and associated network management software.

- CBP Network Operations Center – Maintains the performance, management, and administration capabilities of the CBP core network. The CBP Network Operations Center deploys and maintains a network management system and a suite of network devices that collect and report real-time information. The CBP Network Operations Center system enforces authorizations within the system and between interconnected systems (DHS OneNet and CBP Field Sites) in accordance with CBP/DHS Sensitive Security Policy. The CBP Network Operations Center has been designated a mission-essential system.

- Authorized Desktop Build – The CBP Authorization Desktop Build is a set of configuration standards for building a Desktop/Laptop/Tablet operating system environment. The “DHS Windows 7/Internet Explorer 8 Configuration Guidance version 1010.7 Interim” is being followed in the CBP Authorization Desktop Build configuration.

[7] As a Category X airport, SFO had a total of 44.7 million passengers from July 2012 to June 2013. SFO was ranked 7th in North America and was ranked 22nd in the world in 2012.

- WFPS – Provides CBP with file and printing services using the Microsoft Windows Server 2008 x64 platform. WFPS has not been designated a mission-essential system.

- TECS – Supports enforcement and inspection operations for several components of DHS and is a vital tool for law enforcement and intelligence communities at the local, State, tribal, and Federal Government levels.[8] TECS comprises several subsystems that include enforcement, inspection, and intelligence records relevant to the antiterrorism and law enforcement mission of CBP and the other Federal agencies it supports. TECS has been designated a mission-essential system.

U.S. Immigration and Customs Enforcement

ICE staff at SFO conduct criminal investigations related to violations of Customs and Immigration laws. They are the primary investigative component for DHS at SFO.

We audited IT security controls at the following ICE locations:

- SFO Central Block, and
- SFO Terminal G.

ICE staff at these locations use the following systems:

- Office of the Chief Information Officer Workstations with File and Print Servers – Provides workstation, laptop, print services, and file services to ICE program areas nationwide. Print servers allow ICE users to conduct networked printing. The file servers provide a networked file repository for groups and users. This system includes workstations, laptops, file servers, printers, and print servers at each field site. This system has not been designated a mission-essential system.

- ICE Communication over Networks – This general support system provides support for network devices and data communications throughout ICE and 287(g) sites in the Continental United States.[9] The authorization boundary for ICE Communication over Networks includes ICE Operations-managed switches, firewalls, and intrusion detection sensors. ICE Communication over Networks has not been designated a mission-essential system.

[8] Formerly known as the Treasury Enforcement Communications System, TECS is no longer an acronym (effective December 19, 2008) and is principally owned and managed by CBP.
[9] The 287(g) program, under the *Immigration and Nationality Act*, allows a state and local law enforcement entity to enter into a partnership with ICE, under a joint Memorandum of Agreement, in order to receive delegated authority for immigration enforcement within their jurisdiction.

Management Directorate

The Management Directorate's Office of the Chief Information Officer provides connectivity for DHS components at SFO through:

- DHS OneNet – Provides network communications for the DHS sensitive but unclassified environment. DHS OneNet supports communication and interaction among many organizational entities within and outside of DHS and has been designated as a DHS mission-essential system.

DHS OneNet equipment is located within TSA, CBP, ICE, and USCG facilities at SFO locations. We did not identify operational, technical, or management control deficiencies related to DHS OneNet equipment.

Transportation Security Administration

The Office of Security Operations deters, detects, and prevents hostile acts against all modes of transportation in the United States to ensure freedom of movement for people and commerce. We audited IT security controls at the following TSA locations:

- Office of the Federal Security Director, San Francisco, CA,
- Office of Federal Air Marshal Service, San Francisco, CA,
- SFO Terminals 1, 2, and 3, and
- SFO International terminal.

TSA staff at these locations use the following systems:

- FAMSNet – Provides the IT infrastructure to support the Federal Air Marshal program, such as internet access and internal access to 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.

- Infrastructure Core System – Provides core services, including file and print services, to the entire TSA user community. The Infrastructure Core System has been designated a mission-essential system.

- STIP – Combines many different types of components, including transportation security equipment, servers and storage, and databases. A user physically accesses STIP transportation security equipment to perform screening or other administrative functions. Transportation security equipment includes Explosive Trace Detectors, Explosive Detection Systems, Advanced Technology X-ray, Advanced Imaging Technology, and Credential Authentication Technology. STIP has not been designated a mission-essential system.

- Transportation Security Administration Network – Provides connectivity for airports and their users. The Transportation Security Administration Network consists of a geographically dispersed wide-area network and each site's local area network. The network is connected to the DHS OneNet and has been designated a mission-essential system.

U.S. Coast Guard

The USCG operates four MH-65D helicopters at Air Station San Francisco. The USCG also provides Search and Rescue coverage along 300 miles of California coastline, from Point Conception to Fort Bragg. Other USCG missions include:

- patrolling ports and waterways, and providing coastal security,
- protecting living marine resources and supporting environmental response operations,
- enforcing Federal and international laws and regulations, and
- providing logistics support to USCG and partner agencies.

We audited IT security controls at the following USCG locations:

- Hangar Telecommunication Room,
- Port Security Room,
- Telecommunication Administration Room, and
- Classified Room.

The USCG staff at these locations use the Sensitive But Unclassified Local Area Network Maintenance Logistics Command Pacific Area. This is a General Support System supporting the USCG mission by providing users with office automation support, access to files, application services, connectivity to the USCG intranet, and the Internet via Coast Guard One.

Appendix E
Major Contributors to This Report

Sharon Huiswoud, IT Audit Director
Kevin Burke, IT Audit Manager
Charles Twitty, Senior IT Auditor
Craig Adelman, Referencer

Appendix F
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
Commissioner, CBP
CBP CIO
CBP Audit Liaison
Director, ICE
ICE CIO
ICE Audit Liaison
Administrator, TSA
TSA CIO
TSA Audit Liaison
Commandant, USCG
USCG Assistant Commandant of Resource
USCG Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

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