OFFICE OF INSPECTOR GENERAL

Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised)

Homeland Security

January 16, 2015
OIG-15-18 (Revised)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

January 16, 2015

MEMORANDUM FOR: The Honorable Chip Fulghum
Acting Under Secretary for Management

FROM: John Roth
Inspector General

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport*

Attached for your information is our revised final report, *Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport.* This report contains findings and recommendations for improving security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS information technology infrastructure at this airport.

The procedural history of this report elicits an unfortunate commentary on the manner in which the Department handled this matter and bears review:

- We provided a draft of this report on July 22, 2014 to the Chief Information Officer for review. Pursuant to *Department of Homeland Security Directive 077-01, Follow-up, and Resolution for Office of Inspector General Report Recommendations,* we asked for agency comments, including a sensitivity review, within 30 days of receipt of the draft. This would have made the report due on or about August 22, 2014. Almost a week later, on August 27, 2014, the DHS Chief of Staff requested an extension to provide a response and technical comments. I granted the extension until September 17, 2014.

- On October 20, 2014, nearly 60 days after the original due date for agency comments, the Departmental GAO-OIG Liaison Office finally conveyed to us TSA's response to our request for a sensitivity review by marking several passages in the report as SSI. I disagree with this determination.

- On November 19, 2014, I sent a formal challenge memo to TSA Administrator John Pistole expressing my disagreement. Administrator Pistole had authority over all TSA programs and operations, including oversight of the SSI programs, and is my counterpart in DHS' leadership.

- Having received no reply, on December 16, 2014, I wrote to Administrator Pistole a second time, noting that this report had languished as a result of TSA's sensitivity review, and again requesting that he remove the SSI deletions from the report. As with the November 19, 2014 letter, I received no reply.

- Finally, on January 13, 2015, over five months after submitting the report for sensitivity review, and two months after writing to Administrator Pistole, I received a decision, not from the Acting TSA Administrator, but from the head of the SSI program office – the very same office that initially and improperly marked the information as SSI. Not surprisingly, the office affirmed its original redaction to the report.

I am disappointed in both the substance of the decision as well as its lack of timeliness. In 2006, Congress, concerned about delays in appeals of this nature, directed the Department to revise DHS Management Directive 11056.1 to require TSA to require timely SSI reviews. Given the clear requirement for timely SSI reviews in response to requests from the *public*, we hoped that TSA would approach an SSI appeal from the *Inspector General* with similar diligence, especially because TSA was aware of our deadlines.

Now, to meet our reporting requirement, we are compelled to publish a redacted report with SSI markings and will again ask the head of TSA to overrule the SSI program office's decision.

I believe that this report should be released in its entirety in the public domain. I challenged TSA's determination because this type of information has been disclosed in other reports without objection from TSA, and because the language marked SSI reveals generic, non-specific vulnerabilities that are common to virtually all systems and would not be detrimental to transportation security. My auditors, who are experts in computer security, have assured me that the redacted information would not compromise transportation security. Our ability to issue reports that are transparent, without unduly restricting information, is key to

accomplishing our mission. Congress, when it passed the *Reducing Over-Classification Act* in 2010, found that over-classification "interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information."

Consistent with our responsibilities under the *Inspector General Act*, and in compliance with 49 CFR 1520, we will provide appropriately marked and unredacted copies of our report to appropriate Congressional committees with oversight and appropriation responsibility for the Department of Homeland Security. We will post a redacted version of the report on our website pending a decision from the Acting TSA Administrator.

I appreciate your attention to this matter. Should you have any questions, please call me, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachments

cc: Melvin Carraway, Acting Administrator
Transportation Security Administration

The Honorable R. Gil Kerlikowske
Commissioner, U.S. Customs and Border Protection

The Honorable Sarah Saldaña
Assistant Secretary, U.S. Immigration and Customs Enforcement

Joseph Clancy, Acting Director
United States Secret Service

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

NOV 1 9 2014

MEMORANDUM FOR: The Honorable John Pistole
Administrator
Transportation Security Administration

FROM: John Roth
Inspector General

SUBJECT: Office of Inspector General's Challenge to Sensitive Security Information Office's Request to Mark OIG report: *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport* as SSI
OIG *Project No: 14-082-ITA-DHS*

The Inspector General Act requires the Office of Inspector General (OIG) to conduct audits and investigations that promote the economy, efficiency, and effectiveness of DHS programs and operations, and to inform the Secretary, Congress, and the public about any problems and deficiencies we identify. Our ability to issue reports to the public that are transparent, without unduly restricting information, is key to accomplishing our mission.

I am concerned that the Department's review and response to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport*, indicated that several statements within the report were determined to be Sensitive Security Information (SSI). I disagree with this determination and I am submitting this formal challenge according to procedures outlined in DHS Management Directive MD 11056.1, Sensitive Security Information. Under DHS MD 11056.1.F.2, a formal challenge may be submitted, in writing, to the person who made the SSI markings or to the SSI Office.

We issued the draft report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* to the Department on July 22, 2014. On August 6, 2014, a SSI Senior Program Analyst, provided a response and marked as SSI several passages in this report. See Attachment A for a copy of this draft report with the suggested SSI content highlighted. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe the information in our draft report was

improperly marked as SSI and I am challenging this determination based on the following:

First, the same or similar information as that marked SSI in the current draft report was disclosed to the public in previously released DHS OIG and GAO reports. The Department reviewed and approved the content of these previously released reports and did not determine at that time that the information was SSI. For example:

- On page 5 of our draft report, we discuss physical security issues in TSA's space at JFK airport. The SSI Office marked this information as SSI based on 49 C.F.R. § 1520.5(b) (5). I challenge this request. In GAO audit report *General Aviation: Security Assessments at Selected Airports*, GAO-11-298 dated May 2011, GAO published similar information. Specifically, the GAO report discusses and reports the security measures and potential vulnerabilities at selected airports. (page 7, Attachment B)
- Also, on page 5 of our draft report, we display a picture of TSA equipment in a corridor accessible by unsecured double doors to public area prior to TSA terminal security checkpoint. The SSI Office marked this picture SSI. I challenge this request. This is a picture of IT equipment similar to the IT equipment pictured in figures 4, 5, and 6 of our draft report, yet the SSI Office did not mark those figures SSI. This item shows an example of a TSA equipment cabinet that is in an area accessible to non TSA staff and the public. This risk can be controlled and eliminated by TSA simply securing the terminal corridor from unauthorized access. In addition, our report did not provide the specific location of this cabinet.
- On pages 14 and 21 of our draft report, the SSI office marked one sentence on each page as SSI information. These sentences are located in the TSA (page 14) and CBP (page 21) Patch Management Sections of our report. I challenge this request. Similar or the same wording was used in our last two publically released technical security airport reviews at Dallas Ft. Worth (*Audit of Security Controls for DHS Information Technology Systems at Dallas/Ft. Worth International Airport*, OIG-14-132) and Atlanta's Hartsfield (*Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport*, OIG-13-104) airports. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

- Also on pages 14 and 21 of our draft report, the SSI office marked information in the tables in the TSA and CBP Patch Management sections of the report as SSI information. I challenge this request. Similar content in the same table format was reported in our last two publically released DHS OIG audit reports on Dallas/Ft. Worth, OIG-14-132, and Atlanta Hartsfield airports OIG-13-104. (pages 10, 18, and 25 in Attachment C and pages 10, 20, and 31 in Attachment D)

Second, although the SSI Office marked information in the TSA and CBP Patch Management sections of the draft report as SSI, the SSI Office did not mark the same information in the ICE section of the same report as SSI. Specifically, the ICE section of the draft report includes the same table and wording regarding scanning vulnerabilities that is in the TSA and CBP sections. However, the SSI office did not mark the ICE information as SSI. The SSI determination appears to be inconsistently applied.

Further, even if past reports had not released similar information, I still do not believe its release in this report would be detrimental to transportation security. For example, the language marked SSI reveals generic vulnerabilities that are common to virtually all systems. In addition, the descriptions of the vulnerabilities are not specific enough to be detrimental.

For these reasons, I am requesting that you reconsider and remove your SSI markings from our draft report. These markings impede the effectiveness and transparency of our office. I feel that based on the reasons I have outlined above, our OIG report, *Technical Security Evaluation of DHS Activities at JFK International Airport,* should be released in its entirety in the public Domain.

I appreciate your attention to this matter. Please feel free to contact me with any questions.

cc: Jim Crumpacker, Director, DHS GAO/OIG Liaison Office
Shelly Peterson, Audit Liaison for the Chief Information Officer
Susan Perkins, TSA, Audit Liaison
Tamara Lilly, DHS CISO, Audit Liaison
John Buckley, CBP, CISO
Judy Wright, CBP, Audit Liaison
Tom DeBiase, ICE, Acting CISO

Joanna Perkins, ICE, Audit Liaison
Jill Vaughan, TSA, CISO
Thomas Feltrin, TSA, Audit Liaison
Doug Blair, SSI Program Chief
Rob Metzler, Senior Analyst

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

DEC 1 6 2014

MEMORANDUM FOR: The Honorable John Pistole
Administrator
Transportation Security Administration

FROM: John Roth
Inspector General

SUBJECT: Follow up to my Challenge Memo to the SSI Markings to draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport-Sensitive Security Information*

I am writing to follow up on the memo I sent you on November 19, 2014, regarding my challenge to Sensitive Security Information (SSI) markings to our draft report, *Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport.* We are preparing to issue this report as final. However, I am concerned that I have not heard back from you regarding my request to remove the SSI markings from our report so that we may issue it in its entirety in the public domain.

In response to a law passed by the Congress in 2006, the Department revised DHS Management Directive (MD) 11056.1, to require TSA to ensure a timely SSI review of public requests for release of information. Given MD 11056.1, section V.B.7's requirement for timely SSI reviews in response to requests from the public, we hoped that TSA would approach our SSI appeal from a fellow component with similar diligence, especially since TSA is aware of our deadlines. We are disappointed.

In its October 20, 2014, response to our draft report, the Department indicated that several statements within the report were determined to be SSI. I disagree with the markings and submitted my challenge to you in accordance with guidance provided under MD 11056.1.

I again request that you reconsider and remove the SSI markings from our draft report. I recognize the SSI Office's process to identify and safeguard SSI information. However, I believe that improperly marking information in our draft report as SSI impedes our ability to issue reports to the public that are transparent, without unduly restricting information, which is key to accomplishing our mission. Per DHS MD

11056.1, VI.A.3, SSI markings should not be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency.

This report has languished for months because of TSA's sensitivity review. Absent a decision from you, we will be forced to publish a redacted report to meet our timeliness requirements. The report will contain our objections to the redactions. Consistent with our responsibilities under the *Inspector General Act*, we will provide unredacted copies of our report to Congressional Committees with oversight and appropriations responsibility for the Department of Homeland Security.

I appreciate your personal attention to this matter and I await your response. Should you have any questions, please call me.

Attachment

Errata page for OIG-15-18

Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport (Redacted)

Changes made for Redactions page 5, 1st paragraph and figure 2 (see below):

Revised SSI marking redactions applied.

Change made to the Management Comments and OIG Analysis section, page 31, 1st paragraph (see below):

The following statement has been removed from our report for clarity:

We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

Change made to the Management Comments and OIG Analysis section, page 39, 1st paragraph (see below):

The following statement has been removed from our report for clarity:

We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

The revisions did not change the findings or recommendations made in this report.

Table of Contents

Appendixes

Abbreviations

Airport Authority	Port Authority of New York and New Jersey
CBP	U.S. Customs and Border Protection
CCTV	closed-circuit television
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security

FAMS	Federal Air Marshall Service
FAMSNet	Federal Air Marshall Service Network
GAO	Government Accountablity Office
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
JFK	John F. Kennedy International Airport
OIG	Office of Inspector General
OMB	Office of Management and Budget
OneNet	DHS One Network
PIA	privacy impact assessment
PII	personally identifiable information
PTA	privacy threshold assessment
Security System	Airport Authority Selected Surveillance Systems
TECS	Treasury Enforcement Communication System
TSA	Transportation Security Administration
TSANet	Transportation Security Administration Network
UPS	uninterruptible power supply
USSS	United States Secret Service

Executive Summary

As part of our Technical Security Evaluation Program, we evaluated technical and information security policies and procedures of Department of Homeland Security components at the John F. Kennedy International Airport. Four Department components – the Transportation Security Administration, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Secret Service – operate information technology systems that support homeland security operations at this major airport.

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

The Department's sensitive system security policies, the information technology security controls implemented at several sites had deficiencies that, if exploited, could have resulted in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration. Additionally, operational environmental controls and security documentation needed improvement. Further, information security vulnerabilities were not resolved timely. Technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also needed improvement. The Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement did not perform required security authorization or privacy reviews on closed–circuit television and surveillance monitoring room technology. The U.S. Secret Service fully complied with DHS sensitive security policies at the airport.

The draft report included 14 recommendations and DHS concurred with 13 of the 14 recommendations. DHS did not concur with recommendation number six. We do not agree with DHS's response to this recommendation, as it does not provide for corrective actions to address the security and privacy concerns identified in our report. To help ensure that these security and privacy concerns get addressed properly, we issued two additional recommendations for the DHS Chief Information Officer and DHS Chief Privacy Officer. We have included a copy of the Department's comments to the draft report in their entirety in appendix B.

Background

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security officials with timely information on whether they had properly implemented DHS information technology (IT) security policies at critical sites. Our program audit was based on the requirements identified within *DHS Sensitive Systems Policy Directive 4300A,* version 10.0, 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 the 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 to improve system security. For example, operational control mechanisms 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 applications and data security requirements. For example, technical controls include passwords for systems.

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

We evaluated security controls for IT systems that support homeland security operations of the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (USSS) at John F. Kennedy International Airport (JFK). Figure 1 shows Terminal Four at JFK.

Figure 1-JFK Terminal Four

JFK is the sixth busiest airport in the United States. With arrivals and departures from almost every international airline in the world, JFK is an international gateway for passengers and heavy freight. Below are some facts about JFK.

- JFK, on the Jamaica Bay in New York City, is a designated port of entry.[1] The airport covers over 4,930 acres, including 30 miles of roadway. JFK has 6 operating airline terminals and more than 125 airline gates.

- Port Authority of New York and New Jersey (Airport Authority) operates JFK under a lease with the City of New York since 1947, with the current lease continuing until 2050. The Airport Authority has invested over $10 billion in the airport.

- JFK contributes about $30.6 billion in economic activity annually to the New York/New Jersey region, generating approximately $4.2 billion in direct wages; 71,000 jobs and indirect wages of $30.5 billion for 213,400 jobs.

- JFK is a leading international air cargo center. This facility has more than four million square feet of office and warehouse space dedicated to cargo operations serving the New York and New Jersey region. The entire air cargo area has automated and computer-controlled terminals containing one or more restricted access sites.

[1] Port of entry is defined as a designated controlled entry points into the United States from foreign countries.

See appendix C for specific details of DHS component activities at the JFK airport.

Results of Audit

TSA Did Not Comply Fully with DHS Sensitive Systems Policies

TSA did not comply fully with DHS operational, technical, and management policies for its servers and switches operating at JFK. Specifically, physical security and access controls for numerous TSA server rooms and communication closets were deficient. Additionally, TSA had not implemented known software patches to its servers at JFK. Finally, TSA did not designate the closed-circuit television (CCTV) cameras as a DHS IT system nor did it implement the applicable, operational, technical, and managerial controls for the cameras. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability, of the data stored, transmitted, and processed by TSA at JFK.

Operational Controls

We evaluated TSA server rooms and communication closets containing IT assets at JFK. We identified operational controls that did not conform fully to DHS policies. Specifically, we identified deficiencies in physical security, visitor logs, the fire protection system, storage and housekeeping, electronic power supply protection, and humidity and temperature controls.

Physical Security

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

[redacted]

The door to the secure Explosive Detection Systems room, where TSA reviews x-ray images of luggage to determine if suspicious checked luggage requires additional inspection, was propped open to vent a portable air conditioning unit, violating physical security controls. Figures 3a, 3b, and 3c show the required access control into the room, a secondary door to the room left open, and an air conditioning unit venting hot air out through the open door.

Figure 3a-Access Control

Figure 3b-Unsecured Door

Figure 3c-Climate Control

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Physical security vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data. Unauthorized access to TSA server rooms may result in the loss of IT processing capability used for passenger and baggage screening.

Visitor Logs

At JFK, TSA did not have visitor logs in any of its communication rooms to document the entry and exit of visitors to these rooms that contain sensitive IT equipment.

According to DHS Sensitive System 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.

When unauthorized individuals gain access to locations where sensitive computing resources reside, there is an increased risk of system compromise and data confidentiality, integrity, and availability concerns.

Fire Protection System

Fire protection, detection, and suppression controls were not present in many TSA communication rooms. Specifically, 14 of the 21 rooms inspected that contained sensitive equipment did not have fire extinguishers. Additionally, 8 of the 21 rooms did not have a fire suppression system installed. As a result, 5 rooms were in violation of fire protection policy. Table 1 shows the existence or lack of fire protection equipment at the locations inspected.

Table 1-TSA Fire Protection

TSA Fire Protection			
Identification of the room	**Smoke Detector**	**Fire Extinguisher**	**Fire Suppression**
TSA Location 1	Yes	No	Yes
TSA Location 2	Yes	No	Yes
TSA Location 3, TSA/FAMS	No	No	Yes
TSA Location 4, Terminal 1	No	No	No
TSA Location 5, Terminal 1	No	No	Yes
TSA Location 6 Terminal 1	Yes	No	Yes
TSA Location 7, Terminal 2	No	No	Yes
TSA Location 8, Terminal 4	No	No	Yes
TSA Location 9, Terminal 4	Yes	Yes	No
TSA Location 10, Terminal 4	No	No	No
TSA Location 11, Terminal 4	Yes	Yes	No
TSA Location 12, Terminal 5	No	No	Yes
TSA Location 13, Terminal 5	Yes	No	Yes
TSA Location 14, Terminal 5	No	Yes	Yes
TSA Location 15, Terminal 7	No	No	No
TSA Location 16, Terminal 7	No	Yes	No
TSA Location 17, Terminal 7	No	No	No
TSA Location 18, Terminal 7	No	No	No
TSA Location 19, Terminal 8	Yes	Yes	Yes
TSA Location 20, Terminal 8	No	Yes	Yes
TSA Location 21, Terminal 8	No	Yes	Yes

According to DHS 4300A Sensitive Systems Handbook:

> Fire protection systems should be serviced by professionals on a recurring basis to ensure that the systems stay in proper working order. The following should be considered when developing a fire protection strategy:
>
> - When a centralized fire suppression system is not available, fire extinguishers should be readily available.
> - Facilities should make available/provide Class C fire extinguishers, designed for use with electrical fire and other types of fire.
> - Fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve one.

Compounding the issue of fire detection and mitigation, only 7 of 21 the rooms inspected contained smoke detectors. Smoke detectors alert the appropriate personnel of a potential fire and possible hazard.

The DHS 4300A Sensitive Systems Handbook also states:

> In addition to the physical security controls discussed above, facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:
>
> - Fire protection, detection, and suppression

In addition to DHS 4300A Sensitive Systems Handbook, TSA's Information Assurance Handbook states:

> The Facility Security manager shall employ and maintain fire suppression and detection devices/systems (to include sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) for the TSA facility information systems that are supported by an independent energy source. When centralized fire suppression is not available, Class C fire extinguishers should be readily available. Each class C fire extinguisher

should be located in such a way that the user would not need to travel more than 50 feet to retrieve it.

The lack of fire notification capabilities and unmitigated suppression system vulnerabilities place at risk the availability of TSA data. For example, sensitive equipment damaged by fire may not be available for TSA's passenger and baggage screening processes.

Storage and Housekeeping

Several TSA communication closets located in the JFK terminals contained storage items and cleaning supplies. For example, we found TSA equipment on top of an unlocked TSA telecommunication cabinet surrounded by a ladder, boxes, trash, and cleaning supplies. The ladder, boxes, and cleaning supplies are all harmful to IT equipment. Additionally, there was no sign in sheet, and non-TSA personnel used the room for equipment storage. Figures 4 and 5, show cleaning supplies and maintenance equipment stored with TSA IT hardware in a communication room and communication closet.

Figure 4 -
Unlocked Communication Cabinet with Unsecured TSA Equipment

Figure 5 -
Communication Room used as Storage

Items being stored in the room were an obstruction and preventing access to the TSA IT equipment cabinets. A lack of housekeeping and maintenance caused a buildup of dust on TSA IT hardware stored within cabinets as shown in figure 6.

Figure 6- Dust covered Sensitive Equipment

According to DHS 4300A Sensitive Systems Handbook:

- Dusting of hardware and vacuuming of work area should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware.
- Cleaning supplies should not be stored inside the computer room.

Storage and housekeeping issues place the availability of TSA data at risk. Computer hardware damaged by dust and debris has the potential to cause delays for TSA's passenger and baggage screening processes.

Electronic Power Supply Protection

TSA did not have an operable uninterruptible power supply (UPS) in three communication cabinets. Figure 7 shows an unlocked cabinet and figure 8 shows inoperable UPS equipment.

Figure 7-
Accessible Equipment

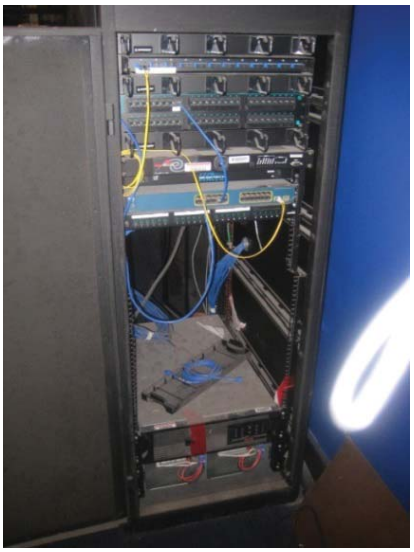

Figure 8-
Inoperable UPS

A sensitive equipment cabinet located in a public area was unlocked and left open to run an extension cord to a nearby electrical outlet for power. Upon closer inspection, we determined that the UPS was inoperable and not being used to provide backup power to IT equipment. Additionally, the attached extension cord prohibited the cabinet from closing and locking.

According to the *DHS 4300A Sensitive Systems Handbook*:

> Electrical power must be filtered through an UPS system for all servers and critical workstations and surge suppressing power strips used to protect all other computer equipment from power surges.

Electrical power supply vulnerabilities place TSA data availability at risk. For example, TSA servers that are not connected to a working UPS may not operate following a power outage.

Humidity and Temperature Controls

TSA did not have any device to measure humidity in the 21 server/switch rooms that we visited at JFK. Additionally, 13 out of the 21 server/switch rooms did not contain temperature sensors. Of the eight rooms that had temperature sensors, only two had temperature readings within the acceptable range established by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

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

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

TSA's implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, identified vulnerabilities on TSA servers at JFK had not been resolved or patched in a timely fashion.

Patch Management

In February 2014, we observed TSA staff scan two servers located at JFK for vulnerabilities. [redacted] [2] Table 2 provides the number of vulnerabilities by server.

[2] Critical vulnerabilities should be addressed immediately due to the imminent threat to a network.

Table 2- Critical, High, and Medium Vulnerabilities

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

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

> Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of TSA data.

Management Controls

TSA's implementation of management controls for the Airport Authority's Security Systems operating at JFK did not conform fully to DHS policies. Specifically, TSA had not designated the Security System as a DHS IT system. As a result, TSA had not performed the applicable security authorization processes and privacy requirements over the surveillance system at JFK terminals.

CCTVs and Surveillance Systems

TSA did not designate the JFK CCTV cameras and surveillance system as DHS IT systems. As a result, the component did not implement the applicable, operational, technical, and managerial controls for the cameras and the systems. TSA officials stated that it was not responsible for the cameras and surveillance system because they belong to the Airport Authority.

However, TSA provided the funding for the JFK CCTV cameras and surveillance systems to the New York Airport Authority. The funding was an estimated $7.2 million to design, install, and maintain the JFK CCTV intrusion detection systems and other surveillance equipment. The Airport Authority Selected Surveillance Systems (Security System) includes CCTV cameras, detection systems, other surveillance hardware, storage equipment, and associated electrical cabling, and

support facilities monitored at JFK. The Airport Authority sets the conditions for shared use of these systems throughout JFK. Figure 9 shows the TSA's Security System.

Figure 9-Security System at JFK

According to the agreement between the Airport Authority and TSA, the Security System provides greater surveillance of TSA areas to enhance security at JFK and assists in resolution of law enforcement issues. The Airport Authority is the owner of the Security System and is responsible for the repairs and maintenance. All media generated from the Security System remains with the Airport Authority. Although, the Airport Authority owns the systems, TSA controls the system design, identification of milestones, and who has allowable access to the system data. TSA officials also have unlimited ability to access information from the Security System to conduct TSA administrative or Top Secret criminal investigations.

The Security System collects images from all cameras to a video management system that stores the information for a minimum of 31 days. Since information that DHS uses is being stored, transmitted, and monitored on this system, and the Port Authority is operating this system on behalf of TSA, then TSA has the requirement to designate the Security System as a DHS IT system. However, TSA officials stated that because this system belongs to the Airport Authority it did

not need to conduct required security authorization processes, a privacy threshold analysis (PTA), or a privacy impact assessment (PIA).[3]

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

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

DHS Sensitive Systems Policy Directive 4300A states that Component Chief Information Security Officers (CISO) shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[3] A privacy threshold analysis is performed to determine if additional privacy compliance documentation is required, such as a privacy impact assessment. A privacy impact assessment is a publicly released assessment of the privacy impact of an information system and includes an analysis of the personally identified information collected, stored, and shared.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, Office of Management and Budget (OMB) M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

TSA has not fulfilled security authorization or privacy requirements for the cameras and surveillance systems at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put this information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Recommendations

We recommend that the TSA Chief Information Officer (CIO):

Recommendation #1:

Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA IT assets.

Recommendation #2:

Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Recommendation # 3:

Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Recommendation #4:

Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #5:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #6:

Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Director, Departmental Government Accountability Office (GAO) OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #1 through #5, but non-concurred with recommendation #6. Additionally, TSA has already taken actions and has submitted supporting documentation to resolve the reported deficiencies for recommendations #1, #3, and #5. We consider these recommendations resolved, but open pending verification of corrective and planned actions and supportive documentation.

Recommendation #1:

DHS concurred with recommendation 1. TSA officials recognize the need to comply with DHS policies on physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring that all uninterrupted power supplies are operational. TSA took several corrective actions and submitted supporting documentation. We agree that the steps TSA is taking, and plans to take, will satisfy this recommendation. Our recommendation will remain open and resolved until we receive and review supporting documentation for the corrective actions.

Recommendation #2:

DHS concurred with recommendation 2. TSA officals recognize the need to comply with the DHS policy concerning fire protection. TSA plans to take corrective actions to ensure that all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. Additionally, TSA plans to verify the presence of other required fire protection equipment at all of its locations at JFK. TSA estimated that corrective actions would be completed by November 30, 2014.

We agree that the steps that TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #3:

DHS concurred with recommendation 3. TSA's response outlines corrective actions for the removal of the excess items and the assurance to refrain from using IT equipment rooms as storage areas. We agree that the steps TSA is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until we receive and review the corrective actions and supporting documentation.

Recommendation #4:

DHS concurred with recommendation 4. TSA recognizes that temperature and humidity levels in computer storage areas should be between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent, respectively. TSA plans to coordinate with facilities management to ensure that the Airport Authority complies with these requirements. TSA estimated that the corrective actions would be completed by October 31, 2014. We recognize these actions as positive steps and look forward to learning more about the continued progress in the future. This recommendation will remain open and resolved pending receipt and verification of planned actions and supporting documentation

Recommendation #5:

DHS concurred with recommendation 5. TSA stated that it remediated the identified vulnerabilities. TSA also stated that another subsequent security scan of the JFK servers was conducted to ensure vulnerabilities identified previously were no longer present on the servers. TSA provided supporting documentation for this recommendation. This recommendation will remain open and resolved pending verification of corrective actions and supporting documentation.

Recommendation #6:

DHS did not concur with recommendation 6. Instead of addressing directly our recommendation to designate detection and surveillance systems as DHS IT systems and to initiate appropriate IT security and privacy controls, TSA indicated it does not have a relationship at the JFK Airport that meets the definition of DHS 4300A Sensitive Systems Handbook for DHS IT systems. In TSA's

response, it stated that, because the intrusion detection and surveillance security systems are owned and operated by the Airport Authority, it had no responsibility to ensure that IT security and privacy controls were met.

According to the DHS Sensitive Systems Policy Directive 4300A, however, a DHS IT system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on its behalf. The systems at JFK transmit, store, and process data on behalf of DHS. Based on the Department's definition, these systems are IT systems and need to be treated as such by DHS. Because TSA has refused to define the detection and surveillance systems as DHS IT systems, TSA did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

We do not agree with DHS's response to this recommendation. The response does not provide for corrective actions to address the security and privacy concerns identified. DHS needs to perform security and privacy reviews of the surveillance systems at JFK airport. By not peforming these reviews, vulnerabilitilies may exist that may put the information collected at risk and lead to security breaches, and violations of DHS policy, and U.S. privacy laws. To assist in this process, we have added additional recommendations, #15 and #16, to our report that will need to be addressed before we can resolve the status of this recommendation.

We look forward to reviewing TSA's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

CBP Did Not Comply Fully with DHS Sensitive Systems Policies

CBP did not comply fully with DHS operational, technical, and management controls. Specifically, several CBP servers and telecommunication rooms did not contain humidity and temperatures sensors. Additionally, the temperature of several of the rooms reviewed with sensors had room temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these rooms were within the ranges set by DHS policy. Also, CBP had an unlocked and open switch device in an open storage area allowing the potential for unauthorized access. In addition, CBP had not implemented known information security software patches to its servers at JFK. Finally, CBP did not designate the CCTV cameras and surveillance room as DHS IT systems nor did they implement the applicable, operational, technical, and managerial controls for these JFK systems. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at JFK.

Operational Controls

CBP server rooms and communication closets at JFK were clean and well maintained. However, onsite implementation of operational controls did not conform fully to DHS policies. For example, temperatures in CBP JFK server rooms were not within the temperature range recommended by the DHS 4300A Sensitive Systems Handbook. Additionally, one of the CBP sites did not have adequate equipment to prevent unauthorized access to CBP communication switches.

Humidity and Temperature Controls

Six out of 21 CBP switch rooms at JFK did not have humidity and temperature sensors. Five rooms with sensors had temperatures that exceeded temperature ranges established by DHS policy. The humidity control readings for these five rooms were within the ranges set by DHS policy.

According to the *DHS 4300A Sensitive Systems Handbook*:

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

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Inadequate Equipment

CBP did not have a large enough box in the office storage area to contain one of its telecommunication switches. As a result, the box could not properly close. Figure 10 shows the box and the telecommunication switches mounted unprotected, beside the box.

Figure 10- Unlocked Switch Box

According to DHS Sensitive System Policy Directive 4300A:

> Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Without adequate physical security controls, unauthorized individuals may gain access to sensitive TSA hardware.

Technical Controls

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

Patch Management

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

Table 3- Critical, High, and Medium Vulnerabilities

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

According to the *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 message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of CBP data. CBP IT Security officials reviewed the technical results for the three servers and immediately began corrective actions to resolve the two critical vulnerabilities.

Management Controls

CBP's implementation of management controls for the CCTV cameras and surveillance room systems operating at JFK did not conform fully to DHS policies. For example, CBP had not designated the CCTV cameras and surveillance room systems as DHS IT systems. As a result, CBP had not performed the security authorization processes and privacy requirements over the newly installed physical security measures at JFK terminals.

CCTV Cameras and Surveillance Room

CBP did not designate the JFK CCTV cameras and surveillance monitoring room systems as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. CBP failed to designate the cameras and surveillance monitoring room equipment as DHS IT systems, as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

We observed several CCTV cameras in the Terminal 4 area of the CBP passenger processing primary and secondary locations.[4] Figure 11 shows CBP's primary passenger processing area.

[4] Primary processing is the first point of examination of passengers by a CBP officer. Those passengers selected for further examination are referred to a secondary processing point for a more thorough inspection.

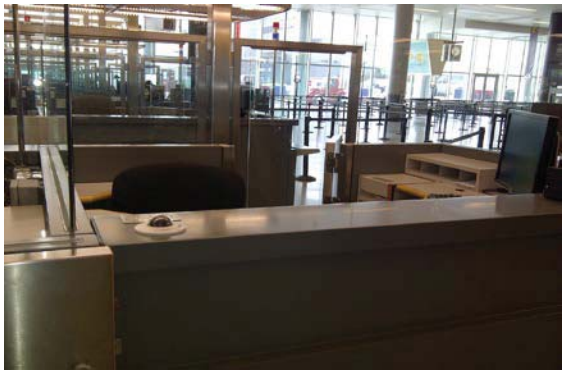

Figure 11-Primary Processing

In 2013, CBP acquired newly renovated space at JFK that included CCTV cameras and a CBP surveillance monitoring room containing IT equipment. The CBP Command and Control Center employees use the cameras to assess threats signaled by alarm events and for surveillance by CBP airport security to monitor activity both inside and outside the terminal.[5] CBP requires a secondary CCTV system that allows officers to monitor detainees in the secondary processing areas, interview rooms, holding rooms, and expedited voluntary removal rooms. CBP officials estimate that approximately 300 cameras are throughout viewable areas within CBP primary passenger processing, secondary passenger processing, interview rooms, and holding rooms. CBP officials operate and monitor the cameras from a CBP secured surveillance monitoring room. Only CBP officials have permission to view cameras observing operations in secondary processing areas. Figure 12 shows the CBP surveillance monitoring room.

[5] Command and Control Center is a station centrally located within the airport's Federal Inspection Service Areas, where CBP systems are monitored.

Figure 12- Views of CBP Surveillance Monitoring

The cameras record audio and visual interactions between CBP officers and passengers. However, the Airport Authority owns the CCTV cameras. Since CBP information is being stored, transmitted, and monitored on this system, CBP has the requirement to designate the cameras and surveillance monitoring room as DHS IT systems. By not designating the cameras and surveillance monitoring room as an IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A.

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

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

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The

PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Among other things, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when it uses IT to collect new information.

CBP has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and may lead to violations of U.S. privacy laws and DHS policy.

Recommendations:

We recommend that the CBP CIO

Recommendation #7:

Maintain the temperatures of servers and switch rooms within the established temperature ranges.

Recommendation #8:

Secure CBP information technology equipment from unauthorized access.

Recommendation #9:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #10:

Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #7 through #10 and has provided details on corrective actions to address each recommendation.

Recommendation #7:

DHS concurred with recommendation 7. CBP's response outlines its plans to install humidity and temperatures sensors. CBP agrees to set humidity and temperatures to the recommended range per the DHS 4300A Sensitive Systems Handbook. These corrective actions are expected to be completed by December 31, 2014. We believe that such efforts are good steps toward addressing our recommendation. We look forward to receiving additional documentation on CBP's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #8:

DHS concurred with recommendation 8. CBP's response outlines its plans to obtain a lockable rack large enough to secure the identified telecommunication switch from unauthorized access. This corrective action is expected to be completed by January 31, 2015. We look forward to receiving notification from

CBP that the lockable rack has been installed and in use. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #9:

DHS concurred with recommendation 9. CBP officials plan to review the OIG reported vulnerabilities to ensure that all critical and high vulnerabilities are addressed. CBP's review is expected to be completed by February 28, 2015. Although, this response appears to address critical and high vulnerabilities, it does not address any corrective actions for the remaining vulnerabilities identified in our report. We look forward to learning more about CBP's actions on this recommendation in the near future. This recommendation will remain open and unresolved pending verification of corrective actions and supporting documentation for all vulnerabilities identified.

Recommendation #10:

Although DHS concurred with recommendation 10, it does not appear that its concurrence addressed all of the concerns noted in our recommendation. Specifically, CBP does not take full ownership of all of the CCTV cameras. CBP agrees that it needs to perform a PTA for CBP's collection and use of the CCTV information. Additionally, CBP plans to determine whether further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV PIA.

However, CBP only plans to perform the PTA and PIA on the cameras it owns. Although the Port Authority owns some of the cameras in CBP's areas, these cameras and surveillance systems also store, transmit, and monitor CBP information. As a result, CBP has the requirement to designate the cameras and surveillance monitoring room systems as DHS IT systems and to perform required security and privacy reviews. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, CBP did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

DHS/CBP did not provide sufficient corrective actions for our review. We look forward to reviewing CBP's progress in the future. However, this recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

ICE Did Not Comply Fully with DHS Sensitive Systems Policies

ICE did not comply fully with DHS operational, technical and management policies for its servers and switches operating at JFK. Specifically, ICE server and telecommunication rooms did not contain humidity and temperature sensors. Also, ICE had not implemented identified information security patches to its servers. Additionally, ICE did not designate the CCTV cameras and surveillance monitoring equipment as DHS IT systems nor did it implement the applicable, operational, technical, and managerial controls for these JFK systems. Finally, ICE CCTV cameras and surveillance system did not function properly or reliably. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at JFK.

Operational Controls

ICE server rooms and communications closets at JFK were clean and well maintained. However, onsite implementation of operations controls did not conform fully to DHS policies. For example, the ICE servers and switch rooms did not have the appropriate humidity and temperature control devices to measure and record humidity and temperature ranges as required by DHS policies.

Humidity and Temperature Controls

The ICE servers and switch rooms did not contain any humidity and temperature sensors.

According to the *DHS 4300A Sensitive Systems Handbook*:

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

High humidity and temperature can damage sensitive elements of computer systems. Therefore, the monitoring of humidity readings and the maintenance of proper temperatures are important to ensure that availability and preservation of IT equipment.

Technical Controls

Patch Management

ICE implementation of technical controls for systems operating at JFK did not conform fully to DHS policies. For example, vulnerabilities identified on ICE servers were not being resolved in a timely fashion. Table 4 provides the number of critical, high, and medium level vulnerabilities identified for each server.

Table 4- Critical, High, and Medium Vulnerabilities

ICE Server Name	Total Number of Critical Vulnerabilities	Total Number of High Vulnerabilities	Total Number of Medium Vulnerabilities
1	0	1	6
2	0	2	4
3	0	0	2
4	0	1	2
Total	0	4	14

According to the DHS 4300A Sensitive Systems Handbook:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction as stated in the Information Security Vulnerability Management message published by the DHS Security Operations Center.

Server vulnerabilities that are not mitigated could compromise the confidentiality, integrity, and availability of ICE data. If the identified security vulnerabilities are not addressed, they could lead to the introduction of malicious code or unauthorized access to ICE information systems.

Management Controls

CCTV and Surveillance Systems

ICE's implementation of management controls over its CCTV cameras and surveillance systems for the physical security requirements at JFK did not conform fully to DHS policies. Specifically, in April 2010, ICE acquired space at Terminal 4, JFK for the Joint Narcotics and Smuggling Unit. This space includes CCTV cameras, a surveillance monitor, and a digital video receiver. Figure 13 shows the ICE surveillance monitor.

Figure 13- ICE's Surveillance Monitor

However, ICE failed to designate the cameras and surveillance monitor as a DHS IT system as required by *DHS Sensitive Systems Policy Directive 4300A,* sections 1.4.7 and 1.4.8.

ICE officials stated that they did not designate the cameras and surveillance monitor as a DHS IT system because the Airport Authority owned the system. Since ICE information is being stored, transmitted, and monitored on this system, then ICE has the requirement to designate the cameras and surveillance monitor as a DHS IT system. By not designating the cameras and surveillance monitoring room systems as a DHS IT system, ICE did not perform the security authorization process as required by DHS Sensitive Systems Policy Directive 4300A or the privacy reviews as required by U.S. privacy laws. By not peforming

these reviews, vulnerabilitilies may exist that may put the information at risk and lead to security breaches, violations of DHS policy, and U.S. privacy laws.

Additionally, two of four CCTV cameras at the Terminal 4 Joint Narcotics and Smuggling Unit communication room were not working during our site visit. The surveillance system monitor connected to the CCTV cameras did not properly display all captured images. ICE officials stated that the cameras had not worked for a period of time but the surveillance system monitor was operating properly 3 days prior to our visit. The ICE officials indicated that they would request camera repairs.

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

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

DHS Sensitive Systems Policy Directive 4300A states that the CISO shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.

Section 208 of the E-Government Act of 2002 requires all Federal Government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII. Section 222 of the Homeland Security Act, as amended, requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate.

DHS' *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010) states that a PIA should be completed for any program, system, technology, or rulemaking that involves PII. This guide defines PII as:

> Information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII includes photographic facial images and any other unique identifying number or characteristic.

Also, OMB M-03-22 directs agencies to conduct reviews of how information about members of the public is handled within their agency when they use IT to collect new information.

ICE has not fulfilled security authorization or privacy requirements for the cameras and surveillance equipment at JFK. Since the JFK cameras and surveillance system have not undergone the required security and privacy reviews, vulnerabilities may exist that may put the information at risk, and lead to violations of U.S. privacy laws and DHS policy.

Lastly, the identified vulnerabilities on ICE CCTV cameras and surveillance monitor degrade physical security for ICE and law enforcement staff members.

Recommendations

We recommend that the ICE CIO:

Recommendation #11:

Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Recommendation #12:

Resolve identified information security vulnerabilities within the timeframe or published direction.

Recommendation #13:

Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Recommendation #14:

Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #11 through #14 and has already taken actions to resolve reported deficiencies.

Recommendation #11:

DHS concurred with recommendation 11. The ICE OCIO plans to to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Sensitive Systems Handbook. ICE estimated the corrective actions would be completed by October 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #12:

DHS concurred with recommendation 12. The ICE OCIO plans to remediate vulnerabilities as they are identified, or within timeframes specified by the DHS Security Operations Center messages. ICE expects this process to be an ongoing effort, however, with an estimated completion date of December 31, 2014. We look forward to receiving additional documentation on ICE's progress on this recommendation. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #13:

DHS concurred with recommendation 13. ICE agreed with the intent of this recommendation for the the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE's OCIO and Homeland Security Investigations plans to coordinate and designate the surveillance systems as ICE/DHS IT systems. ICE also plans to implement applicable DHS management, technical, operational controls, and privacy controls and reviews. ICE anticipates completing corrective actions for this recommendation by June 30, 2015. This recommendation will remain open and resolved pending verification of planned actions and supporting documentation.

Recommendation #14:

DHS concurred with recommendation 14. ICE's Homeland Security Investigations, with assistance from the ICE OCIO, plans to assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ICE officials estimate the completion date of the feasibility study by June 30, 2015. Although this response addresses part our recommendation, it does not outline any corrective actions for the repair of the inoperable CCTV cameras and surveillance system. We look forward to reviewing ICE's progress in the future. This recommendation will remain open and unresolved pending verification of planned actions and supporting documentation.

USSS Fully Complied with DHS Sensitive Systems Policies

USSS fully complied with DHS operational, technical, and management operational policies for its telecommunication room at JFK. We audited IT security controls of the USSS telecommunication room located at the JFK on-site building number 75. This location had a DHS OneNet connection and a network switch device. The telecommunications room was clean and well maintained. Visitor's logs were also maintained. Humidity and temperature sensor readings were within DHS policy guidelines. Since, the JFK location did not have an on-site server, vulnerability scans were not applicable.

Department's Nonconcurrence

Based on the Department's nonconcurrence with recommendation #6, we have added two additional recommendations that were not part of our draft report. Specifically, we recommend that the DHS CIO:

Recommendation #15:

Coordinate steps with DHS components located at JFK, to ensure their compliance with DHS Sensitive Systems Policy Directive 4300A, Section 1.4.8, and to designate the JFK CCTV cameras and surveillance systems as DHS IT systems.

We also recommend that the DHS Chief Privacy Officer:

Recommendation #16:

Require DHS components located at JFK to prepare PTAs and, as applicable, PIAs for the JFK CCTV cameras and surveillance systems as directed by privacy laws and policy.

Appendix A
Objectives, Scope, and Methodology

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

This audit is part of a program to evaluate, 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 evaluating the security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS IT infrastructure at this site. For example, we recorded humidity and temperature at different locations in the server rooms, and then averaged these readings. We also recorded humidity and temperature readings obtained from component sensors that existed in the rooms during fieldwork. We then compared these readings with DHS guidance.

We coordinated the implementation of this technical security evaluation program with the DHS Chief Information Security Officer. We interviewed TSA, CBP, ICE, and USSS, and other staff. We conducted site visits of TSA, CBP, ICE, and USSS facilities at and near JFK. We compared the DHS IT infrastructure that we observed onsite with the documented standards provided by the auditees.

We reviewed the Information Assurance Compliance System documentation, such as the authority-to-operate letter, contingency plans, and system security plans. Additionally, we reviewed guidance provided by DHS to its components in the areas of system documentation, patch management, and wireless security. We also reviewed applicable DHS and components' policies and procedures, as well as Government-wide guidance. We gave briefings and presentations to DHS staff concerning the results of fieldwork and the information summarized in this report.

We conducted this performance audit between November 2013 and April 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 audit. The principal OIG points of contact for the audit are Richard Harsche, Acting Assistant Inspector General for Information Technology Audits, (202) 254-4100, and Sharon Huiswoud, Director, Information Systems Division, (202) 254-5451. Appendix D contains a major OIG contributors listing.

Appendix B
Management Comments to the Draft Report

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

Homeland Security

October 20, 2014

MEMORANDUM FOR: Richard Harsche
Acting Assistant Inspector General
Information Technology Audits

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

SUBJECT: OIG Draft Report: "Technical Security Evaluation of DHS Activities at John F. Kennedy International Airport" (Project No. 14-082-ITA-MGMT)

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) work in planning and conducting its review and issuing this report.

DHS is pleased the OIG noted that the United States Secret Service (USSS) fully complied with DHS operational, technical, and management policies for its telecommunication room at the John F. Kennedy International Airport (JFK). DHS is committed to resolving the information technology (IT) issues identified in the report and has already begun developing plans of actions and milestones to facilitate the timely closure of OIG's recommendations.

The draft report contained fourteen recommendations with which DHS concurs with thirteen, and non-concurs with one. The Department has already fully implemented three recommendations and is requesting closure of those.

Specifically, OIG recommended that the [Transportation Security Administration] TSA Chief Information Officer (CIO):

Recommendation 1: Comply with DHS policy concerning physical security, housekeeping and electronic power supply protection at all locations at JFK that contain TSA [Information Technology] IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning physical security, housekeeping, and electrical power supply protection by conducting quarterly cleaning of all IT equipment cabinets as well as ensuring all uninterrupted power supplies are operational. The doors to the On Screen Resolution room will remain shut to prevent unauthorized access. Supporting documentation for recommendation closure has

been sent by the TSA Office of Security Operations (OSO) to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 2: Comply with DHS policy concerning fire protection at all locations at JFK that contain TSA IT assets.

Response: Concur. TSA recognizes the need to comply with DHS policy concerning fire protection and will ensure all locations at JFK that contain TSA IT assets are equipped with fire extinguishers. TSA OSO is currently verifying the presence of required fire protection equipment. Estimated Completion Date (ECD): November 30, 2014.

Recommendation 3: Maintain JFK servers and network rooms free of excess storage that may cause damage to the equipment.

Response: Concur. TSA has removed excess items and will refrain from utilizing IT equipment rooms as storage. Supporting documentation for recommendation closure has been sent by TSA OSO to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 4: Obtain humidity and temperature sensors for the JFK server rooms, and maintain them within the humidity and temperature ranges established by the ["DHS 4300A Sensitive Systems Handbook"] DHS 4300A Handbook.

Response: Concur. Based on the DHS 4300A Handbook, TSA's Federal Security Director's Staff and Office of Information Technology (OIT) representatives onsite at JFK recognize that temperature and humidity levels in computer storage areas should be held between 60 and 70 degrees Fahrenheit and at a level between 35 percent and 65 percent respectively. TSA representatives at JFK will coordinate with facilities management to ensure the Airport Authority complies with TSA related requests. ECD: October 31, 2014.

Recommendation 5: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. TSA has remediated the identified vulnerabilities. A security scan of the JFK servers was conducted to ensure identified vulnerabilities are no longer present on the servers. Supporting documentation for recommendation closure has been sent by the TSA OIT to OIG under separate cover. TSA requests that OIG consider this recommendation resolved and closed.

Recommendation 6: Designate the intrusion detection and surveillance Security Systems as DHS IT systems and implement applicable management, technical, operational, and privacy controls and reviews.

Response: Non-Concur. TSA has no relationships at JFK that meet the definition within the DHS 4300A Handbook for a DHS IT system. TSA leases space [via the General Services Administration (GSA) or using TSA's own leasing authority] for non-checkpoint space areas like break rooms, Federal Security Director office space, and storage rooms. All operational space, including both passenger and checked baggage screening space, is provided to TSA

"rent free" from the airport pursuant to Section 511 of the DHS Appropriations Act, 2005, Pub. Law 108-334, 118 Stat. 1298 (Oct. 18, 2004).

That law continued the requirement for Airports to provide rent-free necessary security checkpoint space to TSA. Additionally, the Act requires TSA to pay for certain activities associated with its checkpoint activities:

> "For fiscal year 2005 and thereafter, none of the funds appropriated or otherwise made available by this Act shall be used to pursue or adopt guidelines or regulations requiring airport sponsors to provide to TSA without cost building construction, maintenance, utilities and expenses, or space in airport sponsor-owned buildings for services relating to aviation security: Provided, That the prohibition of funds in this section does not apply to-
>
> (1) negotiations between the agency and airport sponsors to achieve agreement on ``below-market'' rates for these items, or
> (2) space for necessary security checkpoints."

Accordingly, the space in which the closed circuit televisions (CCTVs) are located (checkpoint space, operational space, terminals) is not leased by TSA or GSA but rather is owned completely by the airport authority or airline running the particular terminal. TSA's use of checkpoint space is often the subject of a Reimbursable Agreement for services like utilities and janitorial, but ownership and control of the space remains with the terminal owner.

Fundamentally, the intrusion detection and surveillance security systems operated at JFK, as with other airports, are owned and operated by the airport operating authority. Further, there are camera systems at JFK that are owned and operated by individual terminal operators, typically the airlines. While TSA has provided limited reimbursement for some portions of the system, that reimbursement reflects only a small percentage of the airport's investment. The reimbursement is reflected as a stewardship investment on the DHS Agency Financial Report, which is audited annually by DHS OIG. Stewardship investments are investments made by the federal government for the long-term benefit of the Nation. Physical property purchased with such funds is considered non-federal physical property owned by the airport authorities, consistent with federal generally accepted accounting principles.

As noted in OIG's draft report, the "Airport Authority sets the conditions for shared use of these systems throughout JFK." TSA has access to feeds for only 348 of the approximately 1,726 cameras at JFK. While the report states that TSA funded the JFK CCTV system, in actual fact the Airport Authority and the airlines operated such systems at JFK long before TSA even existed, and it would be significant over-reach for TSA to assert ownership of the system based on its reimbursement of a small portion of the overall system.

Finally, it is unclear what information is at risk by the JFK Airport Authority's operation of security cameras at the airport in general, or more specifically at TSA checkpoints or entrance queues. TSA provided the airport with a best-practices guidance document on CCTV policy

development to assist the airport with development of its own CCTV policies, and reflecting that the Airport Authority is the owner and operator of the CCTV system. Even if it were assumed, as the OIG report does, that the anonymous images are Personally Identifiable Information (PII), they are not Sensitive PII under DHS or TSA policy such that there is any substantial risk of harm associated with them. Indeed, they show nothing more than what is seen by the general public. It is unclear what vulnerabilities the OIG believes could exist that would put the images at risk or lead to violations of law or policy.

OIG recommended that the [U.S. Customs and Border Protection] CBP CIO:

Recommendation 7: Maintain the temperature of server and switch rooms within the established temperature ranges.

Response: Concur. CBP OIT/Field Support Directorate (FSD) is working with JFK to install humidity and temperatures sensors. Humidity and temperatures will be set to the recommended range per the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 8: Secure CBP information technology equipment from unauthorized access.

Response: Concur. CBP OIT/FSD will obtain a lockable rack large enough to secure the telecommunication switches from unauthorized access. ECD: January 31, 2015.

Recommendation 9: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. CBP OIT/Enterprise Data Management and Engineering (EDME), Enterprise Data Center Operations Group (EDCOG), Windows Server Group, and Security Technology Policy Group will review the vulnerabilities to ensure all of the critical and high vulnerabilities have been addressed, as appropriate. ECD: February 28, 2015.

Recommendation 10: Designate the surveillance systems as CBP/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. The recommendation is overly broad and does not account for the nuanced ownership, use and retention considerations of the surveillance systems used by CBP at JFK.

The cameras in the area of CBP operations at JFK are owned by the terminal operators. CBP agrees with this recommendation for cameras fully operated by CBP under the CCTV system within CBP Controlled Space in the Federal Inspection Station area. The CBP Privacy and Diversity Office will prepare a Privacy Threshold Analysis (PTA) for CBP's capture and use of the CCTV information to determine whether or not further privacy compliance coverage is warranted through an update to DHS/CBP's current CCTV Privacy Impact Assessment. CBP will also conduct an impact analysis and develop a strategy for security authorization and to identify and implement various levels of controls.

4

CBP does not agree that this recommendation applies to the cameras owned by the terminal operators and not operated by CBP. CBP has varying levels of access to the footage from cameras owned by the terminal operators which are not under CBP's operational control. ECD: October 31, 2015.

OIG recommended that the [U.S. Immigration and Customs Enforcement] ICE CIO:

Recommendation 11: Obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300 Handbook.

Response: Concur. The ICE Office of the Chief Information Officer (OCIO) will work to obtain humidity and temperature sensors for the JFK server and switch rooms, and maintain them within the humidity and temperature ranges established by the DHS 4300A Handbook. ECD: December 31, 2014.

Recommendation 12: Resolve identified information security vulnerabilities within the timeframe or published direction.

Response: Concur. The ICE OCIO will work to remediate vulnerabilities as they are identified, or within timeframes specified by the vulnerabilities respective DHS Security Operations Center Vulnerability Assessment Tests Information Security Vulnerability Management message (DHS SOC VAT ISVMs). This will be an ongoing effort for the ICE OCIO Workstation File and Print Server (OWFPS) Information Systems Security Officer (ISSO). ECD: December 31, 2014.

Recommendation 13: Designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews.

Response: Concur. As it relates to the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK, ICE OCIO and ICE Homeland Security Investigations (HSI) will coordinate to designate the surveillance systems as ICE/DHS IT systems and implement applicable management, technical, operational controls, and privacy controls and reviews. ECD: June 30, 2015.

Recommendation 14: Upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit at JFK.

Response: Concur. ICE HSI with assistance from the ICE OCIO will assess the feasibility to upgrade the CCTV system and surveillance monitoring systems for the Joint Narcotics and Smuggling Unit within Terminal 4 at JFK. ECD: June 30, 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.

5

Appendix C
DHS Activities at JFK Airport

Transportation Security Administration

TSA uses technology to screen passengers and baggage on all departing flights at each of the JFK terminals and to support operation management at nearby office buildings.

We audited IT security controls at the following TSA locations:

- JFK Terminals 1, 2, 4, 5, 7, and 8,
- Office of the Federal Security Director, Jamaica, NY, and
- Office of Federal Air Marshal Service (FAMS), Jamaica, NY.

TSA staff at these locations use the following systems:

- Federal Air Marshal Service Network (FAMSNet) – provides the IT infrastructure to support the FAMS law enforcement mission to help detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. FAMSNet provides Internet access as well as internal access to FAMS information systems including, but not limited to, email, databases, 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 other DHS components, the Federal Aviation Administration, and other State and local law enforcement entities.
- Infrastructure Core System – provides electronic file and print capabilities to the entire TSA user community.
- TSA End User Computing System – provides TSA employees and contractors with desktops, laptops, local printers, mobile devices and other end user computing applications.
- Security Technology Integrated Program – combines many different types of components, including transportation security equipment, servers and storage, software/application products, and databases. Users physically access the transportation security equipment to perform screening or other administrative

functions. TSA's Office of Security Capabilities is the owner of the Security Technology Integrated Program.

- Transportation Security Administration Network (TSANet) – provides connectivity in airports for TSA users. TSANet consists of a geographically-dispersed wide area network and each site's local area network. The networks are connected to the DHS One Network (OneNet) and have been designated a mission essential system.

U.S. Customs and Border Protection

CBP employs over 1,600 staff at JFK to protect the United States from drug and human smugglers, agricultural diseases and pests, and terrorists. CBP personnel also:

- review flight data for terrorist-related activities,
- collect duties, and
- assess fines and civil penalties.

Also, CBP staff at nearby locations use IT assets to perform cargo and outbound passenger review and targeting. In addition, JFK CBP employees operate and maintain the international mail facility.

We audited IT security controls at the following CBP locations:

- JFK Terminals 1, 4, 5, 7, and 8, and
- CBP buildings Number 77 and 250, located in Jamaica, NY.

CBP staff at these locations use the following systems:

- Northeast Field Local Area Network – provides the general support network infrastructure for DHS/CBP users and electronic communications tools, which enables the execution of official duties. The Northeast Field Local Area Network includes 290 geographically dispersed sites using 9,000 devices connected to the OneNet to provide application services to CBP field offices.

- CBP Network Operations Center – maintains the performance, management, and administration of the core network and underlying supporting environment at CBP field site locations. In addition, the center deploys and maintains a network management system and a suite of network devices that collect and report real-time network security information. Further, the center manages the flow of information within interconnected systems in accordance with DHS Sensitive Security Policy.

- Windows 7 PC Client 6.1 – used as the Windows 7 standard desktop image for CBP workstations. Windows 7 PC Client 6.1 consists of a set of standard configurations and installs application software and configures systems according to DHS and CBP technical standards.

- The Windows File and Print System – provides CBP with file and printing services using the Microsoft Windows Server 2008 x 64 platforms.

- Treasury Enforcement Communication System (TECS) – supports enforcement and inspection operations for several components of DHS and is a vital tool for local, State, tribal, and Federal Government law enforcement and intelligence communities.[6] TECS includes several subsystems for enforcement, inspection, and intelligence records relevant to the antiterrorist and law enforcement mission of CBP and other Federal agencies.

[6] 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.

U.S. Immigration and Customs Enforcement

The New York ICE Office of the Special Agent in Charge is responsible for the administration and management of all investigative and enforcement activities within its geographical boundaries. Within the New York Special Agent in Charge office, the Homeland Security Investigations Airport Group is responsible for the identification, disruption, and dismantlement of transnational criminal organizations attempting to exploit vulnerabilities within the air transportation system at JFK. The Homeland Security Investigations Airport Group's areas of concern at JFK include:Contraband smuggling,

- Currency smuggling,
- National security,
- Human smuggling/trafficking,
- Sexual tourism,
- Insider threat, and
- Theft and trafficking of cultural heritage and art.

The JFK Office of Professional Responsibility investigates criminal and administrative misconduct committed by ICE and CBP employees and contractors. This office also addresses complaints of people pretending to be ICE and CBP employees or attempted bribery.

We audited IT security controls at the following ICE locations:

- The Special Agent in Charge New York Office, located in Building No. 75,
- Office of Professional Responsibility, located in Building No. 75, and
- Joint Narcotics and Smuggling Unit, located in JFK Terminal 4.

ICE staff at these locations use the following systems:

- Office File and Print Servers – provide workstation, laptop, print services, and file capability to all ICE employees. File servers provide a networked file repository and print servers allow networked printing.

- ICE Communication over Networks – provides support for all network devices and data communications used by ICE and at 287(g) sites.[7]
- A communication surveillance and analysis system that helps Homeland Security Investigations staff to gather intelligence and collect live data in support of ICE's law enforcement mission. Specifically, the system assembles historical telephone records, monitors telephone and Internet communications, and permits searches of warrant data from online providers. The communication surveillance and analysis system connects to the ICE network infrastructure or on a separate standalone network. This is not a designated mission essential system.

U.S. Secret Service

USSS have nine agents and two administrative personnel located at JFK that report directly to the USSS New York Field Office in Brooklyn, NY. This office is the only USSS office located at an airport.

The agents assigned to the office handle between 750 and 800 arrivals and departures of USSS protected individuals/groups, including Prime Ministers and current and former U.S. Presidents and immediate family members, at JFK and LaGuardia Airports. Each September, the United Nations General Assembly in New York City impacts the JFK Resident Office with over 300 arrivals and departures at JFK and LaGuardia Airports and an additional 42 temporarily assigned agents/officers.

The office also works closely with CBP to seize counterfeit United States currency entering JFK Airport at the passenger and cargo terminals. Since May 2010, DHS seized United States currency totaling over $4 million. The employees of the USSS office use Windows 7, Office 2010, and web—based applications. The service's New York Field Office Technical Operations Squad performs all IT updates, equipment repairs, and installation of new equipment.

[7] The 287(g) program, under the *Immigration and Nationality Act*, as amended, allows a state and local law enforcement entity to receive delegated authority for immigration enforcement within its jurisdiction.

Appendix D
Major Contributors to This Report

Sharon Huiswoud, IT Audit Director
Sharell Grady, IT Audit Manager
Beverly Dale, IT Senior Auditor
Robert Durst, Senior Program Analyst
Frederick Shappee, Senior Program Analyst
Daniel McGrath, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
DHS CISO
DHS CISO Audit Liaison
CBP CIO
CBP Audit Liaison
ICE CIO
ICE Audit Liaison
TSA CIO
TSA Audit Liaison
USSS CIO
USSS Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

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