Department of Homeland Security

Office of Inspector General

Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport

OIG-14-132

September 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 5, 2014

MEMORANDUM FOR: Luke J. McCormack
Chief Information Officer

FROM: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport*

Attached for your information is our final report, *Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport*. We incorporated the formal comments from the Transportation Security Administration, the U.S. Customs and Border Protection, and the U.S. Immigration and Customs Enforcement in the final report.

The report contains 19 recommendations aimed at improving security controls for the department's information systems. Your office concurred with 18 of the recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

The OIG considers recommendation #6 as unresolved and open. Based on information provided in your response to the draft report, we consider recommendations #2, #15, and #18 resolved and closed. We consider the other recommendations in this report to be resolved, but open. Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

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

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

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

Attachment

Table of Contents

Executive Summary 1

Background 2

Results of Audit 3

TSA Did Not Comply Fully with DHS Sensitive Systems Policies 3
Recommendations 12
Management Comments and OIG Analysis 13

CBP Did Not Comply Fully with DHS Sensitive Systems Policies 16
Recommendations 20
Management Comments and OIG Analysis 21

ICE Did Not Comply Fully with DHS Sensitive Systems Policies 22
Recommendations 29
Management Comments and OIG Analysis 30

Appendixes

Appendix A: Objectives, Scope, and Methodology 34
Appendix B: Management Comments to the Draft Report 36
Appendix C: DHS Activities at Dallas/Fort Worth International Airport 42
Appendix D: Major Contributors to This Report 47
Appendix E: Report Distribution 48

Abbreviations

CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CVE	Common Vulnerabilities and Exposures
DFW	Dallas/Fort Worth International Airport
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
EDS	Explosive Detection System
FAMS	Federal Air Marshall Service
FAMSNet	Federal Air Marshall Service Network

FISMA	Federal Information Security Management Act of 2002
GAO	Government Accountability Office
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
ICS	Infrastructure Core System
ISSO	Information System Security Officer
ISVM	Information Security Vulnerability Management
IT	information technology
LAN	local area network
NOC	Network Operations Center
OCIO	Office of the CIO
OIG	Office of Inspector General
OneNet	DHS One Network
OSC	Office of Security Capabilities
OWFPS	Office of the Chief Information Officer Workstations with File and Print Servers
SAC	Special Agent in Charge
SOC	Security Operations Center
STIP	Security Technology Integrated Program
TSA	Transportation Security Administration
TSANet	Transportation Security Administration Network
UPS	uninterruptable power supply
WFPS	Windows File and Print System

Executive Summary

We audited security controls for Department of Homeland Security information technology systems at Dallas/Fort Worth International Airport. Four Department components—the Management Directorate, Transportation Security Administration, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement—operate information technology systems that support homeland security operations at this airport.

Our audit focused on how these components have implemented computer security operational, technical, and management controls for their systems at the airport and nearby locations. We performed onsite inspections of the areas where information technology systems and 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 information technology security controls implemented at these sites had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' information technology systems. We identified numerous deficiencies in the information technology security controls associated with the Transportation Security Administration's Security Technology Integration Program system. For example, physical security and environmental controls for rooms containing this system's information technology assets need improvement. Further, onsite servers for this system were not being scanned regularly for vulnerabilities. Lastly, technical security controls for Customs and Border Protection and Immigration and Customs Enforcement information technology resources also need improvement.

We have briefed the components, and the Department's Chief Information Systems Security Officer, on the results of our audit. We have also made 19 recommendations addressing the control deficiencies identified in this report. We have included a copy of the Department's comments to the draft report in their entirety in appendix B.

Background

We designed our audits of information technology (IT) security controls to provide senior Department of Homeland Security (DHS) officials with timely information on whether they had properly implemented DHS IT security policies at critical sites. Our program is based on *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 operational, technical, and management controls necessary to ensure confidentiality, integrity, and availability within the DHS IT infrastructure and operations. These controls are defined as follows:

- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. 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 a password system which performs an authentication process.

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

We audited security controls for IT systems that support homeland security operations of DHS Management Directorate, Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE) at Dallas/Fort Worth International Airport (DFW). As a Category X airport, DFW has a large number of passenger boardings, processing approximately 58 million passengers (158,375 passengers daily) in 2011.[1]

See appendix C for specific details of DHS activities at DFW by component.

[1] There are five categories of airports—X, I, II, III, and IV. Category X airports have the largest number of passenger boardings and category IV airports have the smallest number.

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 DFW. Specifically, physical security and environmental controls for numerous TSA server rooms were deficient. Additionally, TSA did not have redundant data telecommunications lines providing service to its DFW facilities. Further, TSA had not documented the IT assets or interconnections related to the Security Technology Integrated Program (STIP). Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by TSA at DFW.

Operational Controls

We audited the security controls for TSA server rooms and communications closets containing IT assets at DFW and at the shared TSA/Federal Air Marshall Service (FAMS) facility in Coppell, TX. We determined that onsite implementation of operational controls did not conform fully to DHS policies. These deficiencies exist in physical security, housekeeping and storage, electronic power supply protection, and temperature controls. Additionally, TSA's IT assets at DFW did not have redundant data telecommunications.

Physical Security

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

Figure 1a.
Duct Tape on STIP EDS Server Room

Figure 1b.
Blankets Stored in STIP Rack

Figure 1c.
Non-DHS Equipment in STIP EDS Server Room

Figure 1d.
Smartphone Powered by a STIP Rack

Figure 1e.
STIP EDS Server Room with Access from Baggage Conveyer Belt

Figure 1f.
STIP EDS Server Cabinet Used for Non-DHS storage

According to the *DHS 4300A Sensitive Systems Handbook*, version 10:

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

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

TSA has taken actions to resolve these reported deficiencies. According to TSA, the airline employees' access to the two STIP EDS server rooms has been removed. Additionally, TSA has created a key/lock management process for these STIP EDS server rooms.

Housekeeping and Storage

TSA server rooms and communications closets contained excess storage items, paint, and cleaning supplies. During our fieldwork, TSA staff removed paint cans from a FAMS location. Additionally, the STIP EDS server rooms contained trash, and work areas were dusty. (See figures 2a through 2c for details.)

Figure 2a.
Paint Cans in Server Room

Figure 2b.
Dust Covered STIP Workstation

Figure 2c.
Trash in STIP EDS Server Room

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

- Dusting of hardware and vacuuming of work areas should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware.

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

Electronic Power Supply Protection

Uninterruptible power supply (UPS) for Transportation Security Administration Network (TSANet), Infrastructure Core System (ICS), STIP, and Federal Air Marshal Service Network (FAMSNet) systems at four of 12 server rooms

reviewed showed warning lights signaling that the battery needed to be replaced or that the battery was being bypassed.

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

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

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

According to TSA, 22 failing UPS devices were replaced across three systems (FAMSNet, TSANet, and ICS) to improve power protection and ensure policy compliance.

Environmental Controls

All TSA server rooms exceeded the temperature ranges established by DHS policies. Additionally, several of the server rooms did not contain temperature or humidity sensors. However, the TSA server rooms were within humidity ranges established by DHS policies. Table 1 provides the temperature and humidity readings for each location.

Table 1. TSA Server Rooms Temperature and Humidity Averages

Location	Recommended Temperature: 60 – 70 Degrees Fahrenheit*		Recommended Humidity: 35% – 65%	
	Office of Inspector General (OIG) Average	TSA Reading	OIG Average	TSA Reading
FAMS Coppell	70.7	68	56.5%	No Sensor
ICS Coppell	75.1	72	40.7%	41%
ICS/STIP Terminal B	73.3	74	43.2%	38%
STIP Terminal B Room 2	75.2	66	49.7%	No Sensor
STIP Terminal A	77.9	No Sensor	41.3%	No Sensor
STIP Terminal C Room 1	78.8	76	51%	No Sensor
STIP Terminal C Room 2	78.73	75	57.8%	No Sensor
STIP Terminal E Room 1	84.8	No Sensor	54.9%	No Sensor
STIP Terminal E Room 2	77.6	75	54.1%	59%
STIP Terminal E Room 3	76.9	83	50.6%	No Sensor
STIP Terminal D Room 1	75.6	No Sensor	49.6%	No Sensor
STIP Terminal D Room 2	75.8	No Sensor	42.0%	No Sensor

* Temperature readings in red exceeded the DHS recommended temperature.

Further, one STIP EDS server room contained a non-DHS heater inside a server rack. (See figure 3 for details.)

Figure 3. Non-DHS Heater in STIP EDS Rack

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

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

High temperatures can damage sensitive elements of computer systems. Therefore, TSA should monitor and adjust server room temperature accordingly.

Redundant Data Telecommunications Services

TSA had not established redundant telecommunications services at its Coppell facility or at DFW. Specifically, while there was a data telecommunications circuit for each server room at the Coppell facility and each terminal at DFW, TSA had not configured these circuits to provide redundancy. As a result, performance of mission activities at these locations was vulnerable to disruptions in the event of a data telecommunications circuit failure.

According to *DHS 4300A Sensitive Systems Handbook Attachment M, Tailoring National Institute of Standards and Technology (NIST) SP 800-53 Security Controls, v9.1.xls*:

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

Redundant data telecommunications services vulnerabilities that are not mitigated place at risk the availability of TSA data. For example, if there is a service disruption on the one telecommunications line, IT systems may not be available for TSA's passenger and baggage screening processes.

According to TSA staff, TSA determined it is not necessary to install redundant data circuits for each of the individual circuits already at DFW because TSA has seven telecommunications data circuits providing connectivity to the FSD Office, FAMS Field Office, and five DFW terminals.

Technical Controls

TSA's implementation of technical controls for systems operating at DFW did not conform fully to DHS policies. For example, Office of Security Capabilities (OSC) had not implemented a process to report STIP-related computer security incidents to the TSA Security Operations Center (SOC). Additionally, TSA had not resolved in a timely manner identified patch management vulnerabilities on FAMSNet and ICS servers at DFW. Further, TSA was not scanning STIP EDS servers at DFW for vulnerabilities.

STIP Computer Security Incidents

OSC had not established procedures to report STIP-related computer security incidents to TSA SOC. According to TSA staff, if STIP users identify a problem, they report it to a contractor-operated TSA Service Response Center. There were no procedures in place for this center to report computer security incidents to TSA SOC.

According to *DHS 4300A Sensitive Systems Handbook, Attachment F, Incident Response and Reporting*:

> All users of DHS information systems, including system and network administrators and security officers, have the following responsibilities:
>
> - Report incidents to Component SOCs immediately upon suspicion or recognition.

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

response and initiate incident evaluation processes to a STIP-related computer security incident.

Patch Management

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

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

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

According to *DHS 4300A Sensitive Systems Handbook*:

> Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction

[2] The scanning software provides a description of the vulnerabilities. Several CVEs may have the same vulnerability description. Additionally, the vulnerability may not have an associated CVE, such as "AntiVirus Software Check."

[3] According to National Institute of Standards and Technology Interagency Report 7298, Revision 1, *Glossary of Key Information Security Terms*, CVE is a dictionary of common names for publicly known information system vulnerabilities.

> stated in the Information Security Vulnerability Management (ISVM) message.

According to *DHS 4300A Sensitive Systems Handbook, Attachment O, Vulnerability Management Program*:

> Detailed vulnerability assessment scan schedules and results must be provided to the DHS Vulnerability Management Branch in order to satisfy *Federal Information Security Management Act* requirements for enterprise-wide security situational awareness of assets and risks.

Further, TSA was not scanning for vulnerabilities on the STIP EDS servers at DFW. According to TSA staff, STIP EDS servers, similar to those at DFW, were scanned in June 2013. Those scans determined that the vendor did not support some system software, and other software did not contain the latest security patches. Those scans also reported more than 79 high vulnerabilities on the STIP devices.

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. For example, one of the unpatched vulnerabilities would allow arbitrary code execution on TSA's information systems.

According to TSA staff, several of the identified vulnerabilities were considered to be 'false-positive' or duplicates.[4] For example, according to TSA staff one false-positive was a result of identifying an application that was not in use. Additionally, TSA has resolved several of the identified vulnerabilities and has remediation plans for the remaining.

Management Controls

TSA's management controls for systems operating at DFW did not conform fully to DHS policies. Specifically, OSC had not established interconnection security agreements to document the STIP connections to non-DHS baggage handling

[4] A false-positive is a vulnerability that does not actually exist but is counted in a measurement.

systems. According to TSA, if the STIP software or a TSA screener determines that an individual bag is not considered hazardous, the STIP EDS device sends a signal to the baggage handling system to allow the bag to continue onto the baggage handling system. Additionally, the STIP system security plan, which is a security authorization process document, did not describe the servers, switches, and workstations associated with the system.

According to *DHS 4300A Sensitive Systems Handbook, Attachment N, Preparation of Interconnection Security Agreements*:

> An ISA [Interconnection Security Agreement] is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same Authorizing Official.

According to *DHS 4300A Sensitive Systems Handbook*, the Authorizing Official:

> Ensures new hardware and software products have been approved and documented in the Security Authorization Process documentation.

Undocumented interconnection security agreements place at risk the confidentiality, integrity, and availability of TSA data. For example, the security protections that must operate on interconnected systems may not be established without an interconnection security agreement.

Security authorization is the official management decision to authorize operation of an information system. Security authorization involves comprehensive testing and evaluation of security features and addresses software and hardware security safeguards. The Authorizing Official will not be able to make an informed decision about the security of a system if the system's hardware inventory is incomplete.

Recommendations

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

Recommendation #1:

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

Recommendation #2:

Determine whether it is necessary and cost effective to establish redundant data telecommunications services at TSA's Coppell facility and DFW terminal locations.

Recommendation #3:

Establish a process to report STIP computer security incidents to TSA SOC.

Recommendation #4:

Scan TSA servers annually and resolve identified vulnerabilities within the timeframe or direction stated in the Information Security Vulnerability Management message published by DHS SOC.

Recommendation #5:

Provide required vulnerability assessment reports to the DHS Vulnerability Management Branch.

Recommendation #6:

Establish interconnection security agreements to document the interconnection between STIP and non-DHS baggage handling systems.

Recommendation #7:

Document in the system security plan the STIP servers, switches, and workstations.

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, and #7. DHS non-concurred with recommendation #6. Additionally, TSA provided documentation to support the resolution and closure of recommendation #2. Further, TSA has already taken actions to resolve reported deficiencies with

recommendations #1, #3 through #5, and #7. We consider these recommendations resolved, but open pending verification of planned actions.

Recommendation #1:

TSA concurred and initiated a project at DFW in 2013 to replace failing UPS devices. TSA has remediation plans to resolve the electrical supply deficiency. The remaining six UPSs were refreshed. Additionally, FAMS temperature/humidity sensors are in place and functional. Documentation illustrating remediation of several housekeeping concerns was provided to OIG. However, to complete the recommendation, TSA must secure the cooperation of third parties at DFW. TSA will work with these third parties to close the recommendation.

TSA's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until TSA provides documentation to support that the planned corrective actions are completed.

Recommendation #2:

TSA concurred with this recommendation. TSA has determined that it would not be cost effective to implement the redundancies. TSA requested that OIG close recommendation #2.

TSA's actions satisfy the intent of this recommendation. We consider this recommendation resolved and closed.

Recommendation #3:

TSA concurred with this recommendation. TSA's Cybersecurity Awareness and Outreach Support Team will reach out to the DFW TSA staff to appropriately train those personnel on the correct incident reporting process. The estimated completion date is June 30, 2015.

TSA's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until TSA provides documentation to support that the planned corrective actions are completed.

Recommendation #4:

TSA concurred with this recommendation. According to TSA, servers are scanned on a monthly basis and the results or data feeds are submitted to the DHS Vulnerability Management Branch. Evidence of reports can be provided as requested. TSA supports the DHS Information Security Vulnerability Management program by resolving vulnerabilities as directed by DHS SOC to Alerts and Bulletins. Additionally, TSA requested that OIG consider this recommendation resolved and closed.

However, TSA has not provided documentation that the STIP EDS servers at DFW are being scanned on a monthly basis. Additionally, TSA has not provided documentation that actions have been taken to resolve the vulnerabilities identified on the ICS servers.

TSA's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until TSA provides documentation to support that the planned corrective actions are completed.

Recommendation #5:

TSA concurred with this recommendation. According to TSA, servers are scanned on a monthly basis and the results or data feeds are subsequently submitted to the DHS Vulnerability Management Branch. Evidence of reports will be provided to OIG, upon request. TSA requested that OIG consider this recommendation resolved and closed.

However, TSA has not provided documentation that vulnerabilities associated with the STIP EDS servers at DFW are being reported. TSA's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until TSA provides documentation to support that the planned corrective actions are completed.

Recommendation #6:

TSA non-concurred with this recommendation. According to TSA, the STIP does not have an interconnection with non-DHS baggage handling systems, and therefore, an interconnection security agreement is not needed. TSA requested that OIG consider this recommendation resolved and closed.

However, during the audit TSA provided documentation that these connections do occur. The documentation details the types of connections between STIP EDS and the Baggage Handling System, as well as the data transmitted between the two systems. We consider this recommendation unresolved and open; it will remain unresolved and open until TSA provides a corrective action plan.

Recommendation #7:

TSA concurred with this recommendation. According to TSA, the STIP EDS server and endpoint inventory will be assessed during the Security Authorization process during 2014–2015 and shall be added as an artifact in the DHS information Assurance Compliance System, where the Security Plan is also stored. The estimated completion date is June 30, 2015.

TSA's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until TSA provides documentation to support that the planned corrective actions are completed.

CBP Did Not Comply Fully with DHS Sensitive Systems Policies

CBP did not comply fully with DHS operational, technical, and management controls. Specifically, the two CBP server rooms audited exceeded temperature ranges established by DHS policies. Additionally, CBP had not implemented known patches to its servers at DFW. CBP also had not appointed an information system security officer (ISSO) for the Windows File and Print System (WFPS). Collectively, these deficiencies place at risk the confidentiality, integrity, and availability, of the data stored, transmitted, and processed by CBP at DFW.

Operational Controls

CBP server rooms and communications closets at DFW and the Port Office of Dallas were clean and well maintained. Further, CBP had implemented additional physical security for IT assets in public areas. However, onsite implementation of environmental controls that did not conform fully to DHS policies included inadequate temperature and humidity controls for CBP's two servers' rooms at DFW.

Physical Security Controls

During our audit fieldwork, we observed that CBP had taken additional steps to secure their IT assets in areas that could be accessible by the public. Specifically,

CBP had secured the ports connecting to these devices with a hardware lock. (See figure 4 for details.)

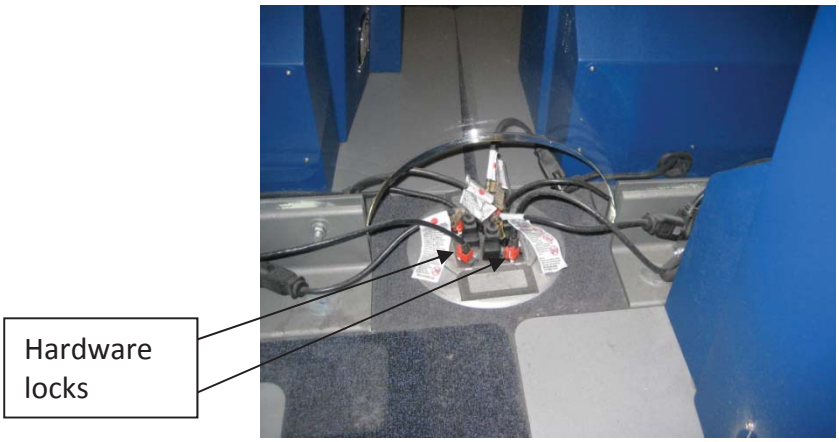

Figure 4. Hardware Locks on LAN Ports

Environmental Controls

The two CBP server rooms exceeded the temperature ranges established by DHS policies. Additionally, one of the two CBP server rooms did not contain temperature or humidity sensors. However, CBP server rooms were within humidity ranges established by DHS policies. Table 3 provides the temperature and humidity readings for each location.

Table 3. CBP Server Rooms Temperature and Humidity Averages

Location	Recommended Temperature: 60 – 70 Degrees Fahrenheit		Recommended Humidity: 35% – 65%	
	OIG Average	CBP Reading	OIG Average	CBP Reading
Concourse D	73.8	No Sensor	44.01%	No Sensor
Port Office of Dallas	72.3	66	48.3%	53%

According to CBP officials, repairs were made to the air conditioner at the Port Office server room, resolving this deficiency. Additionally, based upon a request by CBP, the DFW Airport Authority resolved the temperature deficiency in the Concourse D server room. Further, CBP is working with DFW Airport to establish monitoring and alerting for temperatures that fall outside established ranges.

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

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

High temperatures can damage sensitive elements of computer systems. Therefore, CBP should monitor and adjust the server room accordingly.

Technical Controls—Patch Management

In October 2013, we observed CBP staff scan servers located at DFW for vulnerabilities.[5] These technical scans detected critical and high vulnerabilities on the five servers. Table 4 provides the number of vulnerabilities for each server.

Table 4. Critical and High Vulnerabilities by CVE

CBP Server Name	Total Number of Critical Vulnerabilities	Total Number of Unique High Vulnerabilities	Total Number of High or Critical CVEs	Date of Last Vulnerability Scan Report to DHS
Server 1	2	2	11	12/19/2013
Server 2	2	6	23	12/19/2013
Server 3	2	7	23	12/19/2013
Server 4	5	9	200	12/19/2013
Server 5	2	8	60	12/19/2013

According to *DHS 4300A Sensitive Systems Handbook*:

> 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 CBP data. These risks allow arbitrary code execution on CBP's information systems.

[5] According to the DHS Office of the Chief Information Security Officer, CBP had provided reports of vulnerabilities for five of the servers at DFW.

During the course of our audit, CBP took actions to correct many of the identified vulnerabilities. For example, CBP removed server #4 from the network and installed the necessary patches to resolve the critical vulnerabilities except for one that CBP considers a 'false-positive.' According to CBP staff, this false-positive was the result of the scanning software not properly identifying the version of the target system.

Management Controls

CBP's implementation of management controls for systems operating at DFW did not conform fully to DHS policies. Specifically, since January 2013, the WFPS has been without an ISSO to receive and manage IT system security matters. Additionally, CBP does not have centralized storage for Southwest Field local area network (LAN) audit logs because there is insufficient space to store and maintain the audit logs. However, CBP has recognized the audit log storage space issue as a deficiency and has created a plan of actions and milestones to address it.

Further, as part of our DFW fieldwork, we requested the implementation status of our previous Dynamic Host Configuration Protocol (DHCP) audit log recommendation.[6] Specifically, we reported in July 2013 that CBP was not reviewing the automated DHCP server messages. We recommended that CBP assign the responsibility to review DHCP server automatic messages and LAN audit logs. According to CBP staff, the Network Operations Center (NOC) and the DHS One Network (OneNet) Security teams are verifying that the audit logs are being sent to the National Data Center. In addition, the OneNet Security team had created a standard operating procedure for the review and was performing weekly reviews. Furthermore, the NOC ISSO and the OneNet security team plan to review the audit logs.

However, the tool used for collecting, unifying, storing, and automating security logs and events for analysis and reporting was not receiving the required data. According to the CBP staff, hardware and software need to be upgraded to assure that the events are sent to the NOC and OneNet Security Teams. Also, according to CBP staff, while a new logging solution has been identified, the solution has not received funding and has been placed on the 2014 unfunded requirements lists. CBP submitted a waiver request to the DHS Chief Information Security Officer (CISO) to accept the risk. In March 2014, DHS CISO approved this

[6] *Technical Security Evaluation of DHS Activities at Hartsfield-Jackson Atlanta International Airport* (OIG-13-104), July 2013.

waiver.

According to *DHS 4300A Sensitive Systems Handbook*:

> An ISSO shall be designated for every information system and serve as the point of contact for all security matters related to that system.
>
> Components shall ensure that audit logs are recorded and retained in accordance with the Component's Record Schedule or with the DHS Records Schedule. At a minimum, audit trail records shall be maintained online for at least ninety (90) days. Audit trail records shall be preserved for a period of seven (7) years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.

Management control vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of CBP data. For example, without assigning the responsibility to an ISSO, components may not adequately implement and maintain system security controls in accordance with the DHS policies.

Recommendations:

We recommend that CBP CIO:

Recommendation #8:

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

Recommendation #9:

Address and resolve identified vulnerabilities within the timeframe or direction stated in the Information Security Vulnerability Management message published by DHS SOC.

Recommendation #10:

Designate an ISSO for WFPS.

Recommendation #11:

Store, maintain, and review as recommended by the *DHS 4300A Sensitive Systems Handbook*:

- WFPS audit logs, and
- DHCP audit logs.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Director, Departmental GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #8 through #11 and has already taken actions to resolve reported deficiencies. We consider these recommendations resolved, but open pending verification of planned actions.

Recommendation #8:

CBP concurred with this recommendation. CBP corrected the temperature in the Dallas Port Office LAN Room. CBP also corrected the temperature in the DFW Airport LAN Room by asking DFW Airport to lower the set point of the room to 68 degrees Fahrenheit. CBP is working with DFW Airport Authority to establish monitoring and alerting for temperatures that fall outside established ranges within the LAN Room. The estimated completion date is October 31, 2014.

CBP's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that the planned corrective actions are completed.

Recommendation #9:

CBP concurred with this recommendation. CBP plans to continue to patch system vulnerabilities in a timely manner and will ensure that outstanding patches are implemented. The estimated completion date is December 31, 2014.

CBP's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that the planned corrective actions are completed.

Recommendation #10:

CBP concurred with this recommendation. CBP plans to provide ISSO duties to WFPS initially through existing ISSO resources, while a contract ISSO is added to the existing contract. Other options are being reviewed related to WFPS boundaries. The estimated completion date is November 30, 2014.

CBP's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that the planned corrective actions are completed.

Recommendation #11:

CBP concurred with this recommendation. CBP plans to store, maintain, and review WFPS audit logs when an ISSO is assigned. Regarding the DHCP audit logs, CBP has submitted a funding request and is pursuing the capability to meet this requirement. Remediation of this part of the finding will depend upon funding approval which is expected to be determined by the end of fiscal year 2014.

CBP's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that the planned corrective actions are completed.

ICE Did Not Comply Fully with DHS Sensitive Systems Policies

ICE did not comply fully with DHS operational, technical, and management operational policies for its servers and switches operating at DFW. For example, ICE had not implemented known patches to its Special Agent in Charge (SAC) Dallas and DFW Airport Group servers and was not regularly scanning its servers at DFW. Also, ICE had not included the Homeland Security Investigations (HSI) servers at DFW as part of a recognized *Federal Information Security Management Act* (FISMA) inventoried system.[7]

Additionally, one ICE server room did not comply with temperature ranges established by DHS policies. Further, ICE did not implement redundant data telecommunications lines to avoid single points of failure at DFW and SAC Dallas sites. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability, of the data stored, transmitted, and processed by ICE at DFW.

[7] The *Federal Information Security Management Act of 2002* (P.L. 107-347)

Operational Controls

ICE server rooms and communications closets at DFW and SAC Dallas Office were clean and well maintained. However, onsite implementation of operations controls did not conform fully to DHS policies. For example, the temperature in the DFW server room was not within the temperate range as recommended by the *DHS 4300A Sensitive Systems Handbook*. Additionally, the ICE site at DFW did not have redundant data telecommunications capability to avoid single points of failure.

Environmental Controls

One of the two ICE server rooms exceeded temperature ranges established by DHS policies. Additionally, one of the two ICE server rooms did not contain temperature or humidity sensors. However, the ICE server rooms were within humidity ranges established by DHS policies. Table 5 provides the temperature and humidity readings for each location.

Table 5. ICE Server Rooms Temperature and Humidity Averages

Location	Recommended Temperature: 60 – 70 Degrees Fahrenheit		Recommended Humidity: 35% – 65%	
	OIG Average	ICE Reading	OIG Average	ICE Reading
SAC Dallas Server Room	73[8]	69	38.3%	51%
DFW Storage Area / Server Cabinet	77.5	No Sensor	42.5%	No Sensor

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

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

[8] We measured the average temperature for the SAC Dallas Server Room as 72.8 degrees Fahrenheit. However, the heating, ventilation, and air conditioning (HVAC) system was momentarily shut off to facilitate the audit team site visit accounting for the temperature variation.

The average temperature for the DFW area containing the ICE server cabinet did not meet DHS temperature requirements at 77.5 degrees Fahrenheit. Further, ICE did not have temperature or humidity sensors present in the room. According to ICE staff, the temperature in the DFW storage area location where the server cabinet is located was managed by the DFW Airport Board.

High temperatures can damage sensitive elements of computer systems. Therefore, ICE should monitor and adjust the server room temperature accordingly.

Data Telecommunications Services

ICE had not established redundant telecommunications services at its SAC Dallas or DFW facilities. Specifically, only a single telecommunications line serves the HSI Airport Group. Additionally, while the SAC Dallas office is served by multiple circuits, the circuits are from a single vendor and may lack diverse routing to provide sufficiently alternate telecommunications service. As a result, mission-critical activities at these locations are vulnerable to disruption in the event of a data telecommunications failure.

According to *DHS 4300A Sensitive Systems Handbook, Attachment M, Tailoring NIST SP 800-53 Security Controls, v9.1.xls*:

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

Additionally, we observed an ICE data telecommunications line at DFW located in a shared wiring closet with an existing connection of DHS OneNet for CBP. The monthly cost for this circuit is approximately $330. There may be potential cost savings if the DHS OneNet connection were used by both CBP and ICE.

Redundant data telecommunications services vulnerabilities that are not mitigated place at risk the availability of ICE data. For example, if there is a service disruption on the one telecommunications line, IT systems may not be available for ICE's passenger screening processes.

Technical Controls

ICE implementation of technical controls for systems operating at DFW did not conform fully to DHS policies. For example, identified vulnerabilities on ICE servers were not being resolved in a timely fashion. Also, ICE was not regularly scanning for vulnerabilities on ICE HSI servers at DFW. Further, an insecure communications protocol was available on an ICE server.

Patch Management

In October 2013, we observed ICE security operations center staff perform a vulnerability scan on its four servers in use at SAC Dallas and DFW. These scans identified a total of nine high vulnerabilities. Table 6 provides the number of vulnerabilities for each server. Additionally, ICE had provided reports of vulnerabilities to DHS for only three of the four servers identified at DFW.

Table 6. High Vulnerabilities by CVE

ICE Server Name	Total Number of Unique High Vulnerabilities	Total Number of High CVEs	Date of Last Vulnerability Scan Report to DHS
Office of the Chief Information Officer (OCIO) Server 1	1	0	12/19/2013
OCIO Server 2	1	0	12/19/2013
OCIO Server 3	3	2	12/19/2013
HSI Server 1	4	2	Not Reported

According to the *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.

According to *DHS 4300A Sensitive Systems Handbook, Attachment O, Vulnerability Management Program*:

> Detailed vulnerability assessment scan schedules and results must be provided to the DHS Vulnerability Management Branch in order to satisfy *Federal Information Security Management Act* requirements for enterprise-wide security situational awareness of assets and risks.

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.

ICE has taken action and implemented patches to resolve the identified high vulnerabilities.

HSI Servers Were Not Regularly Scanned for Vulnerabilities

ICE had not scanned the HSI electronic surveillance servers that are isolated from the DHS OneNet.[9]

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

> Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or whenever significant changes are made to the information systems.

We reported in July 2013 that ICE was not regularly scanning HSI's electronic surveillance systems for vulnerabilities and recommended that ICE scan servers at Hartsfield-Jackson Atlanta International Airport and the SAC Atlanta office annually.[10] ICE has made progress in vulnerability scanning for the DHS OneNet connected segment of the HSI communication surveillance and analysis system. However, ICE SOC did not perform a vulnerability assessment for HSI servers isolated from the DHS OneNet. Further, ICE had not implemented vulnerability scanning for the standalone electronic surveillance system.

[9] These servers were not included in our observed October 2013 scans of ICE servers.
[10] Ibid.

Proactive vulnerability scanning allows for effective countermeasures for improving security, leads to faster detection of vulnerabilities, and reduces damage to breached systems. As the electronic surveillance system is not connected to the DHS OneNet, the protection of sensitive law enforcement data may be at risk if the servers are not regularly scanned for vulnerabilities.

Insecure Communications Protocol

According to the October 2013 vulnerability assessment scans, the OCIO server at DFW was running an unencrypted telnet protocol.

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

> Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.

Server vulnerabilities that are not mitigated could compromise the confidentiality of ICE data. Specifically, telnet transfers information in "clear text" (unencrypted human-readable text), which allows other users on the LAN to intercept and read the traffic.

According to ICE officials, the insecure protocol was a default setting for the remote administration access that had not been disabled. ICE officials have reported that the telnet vulnerability was resolved during our audit field work by disabling telnet access.

Management Controls

ICE implementation of management controls for systems operating at SAC Dallas and DFW facilities did not conform fully to DHS policies. Specifically, ICE had not individually accounted for the servers hosting HSI's communications analysis and surveillance systems as part of a recognized system in the Department's FISMA inventory. Further, the standalone electronic surveillance system was not included in a FISMA inventory.

We reported in July 2013 that ICE officials planned to include the HSI servers as part of the ICE Subpoena System, a FISMA inventory.[11] In November 2013, ICE

[11] Ibid.

officials reported that they were implementing the recommendation and included the communications analysis and surveillance software as part of the ICE Subpoena System security plan. However, ICE's plan for inclusion of the communications analysis and surveillance software into the ICE Subpoena System security plan is limited to software. ICE officials do not consider the physical servers as part of the ICE Subpoena System. Accordingly, the communications analysis and surveillance servers are not part of a FISMA inventory.

At DFW, the physical servers used for the communications analysis and surveillance system are former OCIO servers that ICE repurposed. Local OCIO staff continue to maintain the physical servers following repurposing, but consider the servers running communications analysis and surveillance software as owned by HSI. (See figure 5 for details.)

Figure 5. An HSI Communications Analysis and Surveillance System Server and OCIO Servers in the Same Rack

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

> Every DHS computing resource (desktop, laptop, server, portable electronic device, etc.) shall be individually accounted for as part of a FISMA-Inventoried information system.

ICE officials reported taking steps to include the surveillance systems servers as part of recognized FISMA-inventory. In addition to the physical servers for the communications analysis and surveillance system, the standalone electronic surveillance system will be added to the FISMA inventory.

Recommendations

We recommend that ICE CIO:

Recommendation #12:

Maintain server rooms at DFW within DHS' recommended temperature ranges.

Recommendation #13:

Determine whether it is necessary and cost effective to establish redundant data telecommunications services at the SAC Dallas facility.

Recommendation #14:

Determine whether it would be cost effective to share the DHS OneNet connection in the shared CBP/ICE communications closet.

Recommendation #15:

Resolve identified vulnerabilities within the timeframe or direction stated in the Information Security Vulnerability Management message published by DHS SOC.

Recommendation #16:

Provide required vulnerability assessment reports to the DHS Vulnerability Management Branch.

Recommendation #17:

Scan the ICE servers at the SAC Dallas sites annually, including HSI systems separated from DHS OneNet.

Recommendation #18:

Use a connection protocol that employs secure authentication, or disable unnecessary ports from the server.

Recommendation #19:

Include the HSI surveillance system servers in a recognized FISMA-inventoried system.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Director, Departmental GAO OIG Audit Liaison. We have included a copy of the comments in their entirety in appendix B. DHS concurred with recommendations #12 through #19. Additionally, ICE has provided documentation to support the resolution and closure of recommendations #15 and #18. Further, ICE has already taken actions to resolve reported deficiencies with recommendations #12, #13, #14, #16, #17, and # 19. We consider these recommendations resolved, but open pending verification of planned actions.

Recommendation #12:

ICE concurred with this recommendation. ICE plans to work with CBP to request and complete changes necessary with DFW parties to maintain the server rooms within DHS' recommended temperature ranges. The estimated completion date is September 30, 2014.

ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until ICE provides documentation to support that the planned corrective actions are completed.

Recommendation #13:

ICE concurred with this recommendation. ICE HSI plans to review the potential mission/business impact if the SAC Dallas Facility loses connectivity. A risk-based decision to establish redundant data telecommunications will be made after the analysis is complete. The estimated completion date for this recommendation is December 31, 2014.

ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until ICE provides documentation to support that the planned corrective actions are completed.

Recommendation #14:

ICE concurred with this recommendation. ICE OCIO plans to work with CBP to determine if it is cost effective to share the DHS OneNet Connection in the DFW shared CBP/ICE communications closet. The estimated completion date for this recommendation is December 31, 2014.

ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until ICE provides documentation to support that the planned corrective actions are completed.

Recommendation #15:

ICE concurred with this recommendation. There were nine vulnerabilities noted in the audit report. ICE SOC remediated and validated these nine identified vulnerabilities by December 16, 2013. On a monthly basis, the ICE Chief Information Security Officer and Authorizing Official meet to review ISVM compliance over the previous 60 days. During this meeting, approval to create a plan of action and milestones for unmet ISVM dates are provided and/or a request is made to patch devices within a specified time period. Scans were sent to OIG on December 16, 2013. ICE requested that OIG consider this recommendation resolved and closed.

ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved and closed.

Recommendation #16:

ICE concurred with this recommendation. An ongoing schedule for scanning OCIO Workstations with File and Print Servers (OWFPS) Organizational Units on a monthly basis, which includes SAC Dallas and DFW, has been developed and implemented. Results of the scans are provided in ICE's monthly report to the DHS vulnerability Management Branch. Evidence of reports can be provided separately. A 6-month forecasted Vulnerability Assessment Test scan schedule was created and implemented as part of the transition to a new vendor. ICE requested that OIG consider this recommendation resolved and closed.

While ICE has provided documentation concerning OWFPS, ICE has not provided documentation concerning vulnerability reporting for HSI systems separated from DHS OneNet. ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until ICE provides documentation to support that the planned corrective actions are completed.

Recommendation #17:

ICE concurred with this recommendation. An ongoing schedule for scanning OWFPS Organizational Units, which includes SAC Dallas and DFW, has been developed and implemented. A 6-month forecasted Vulnerability Assessment Test scan schedule was created and implemented as part of the transition to a new vendor.

ICE OCISO and ICE HSI will determine if scanning the standalone servers is appropriate. The servers contain law enforcement sensitive data; therefore, there is a need to verify that chain of custody rules are not violated by the scan. After the determination is made, either a plan of action and milestones will be opened by ICE HSI to determine procedures for coordinating with ICE SOC to scan ICE HSI systems separate from DHS OneNet, or ICE OCISO will assist ICE HSI with creating a waiver request. The estimated completion date for this recommendation is December 31, 2014.

ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until ICE provides documentation to support that the planned corrective actions are completed.

Recommendation #18:

ICE concurred with this recommendation. The unsecure protocol, telnet, was a default setting for the remote administration access that had not been disabled. OWFPS ISSO submitted a request to manually disable telnet on the SAC and DFW servers. ICE SOC ran scans on December 16, 2013 and validated that the issue was remediated. ICE provided scan results to OIG on December 16, 2013 and this remediation was noted in the audit report. ICE requested that OIG consider this recommendation resolved and closed.

ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved and closed.

Recommendation #19:

ICE concurred with this recommendation. ICE OCISO is currently working with ICE HSI to determine options for including the HSI surveillance system servers into a recognized FISMA package. The estimated completion date for this recommendation is August 31, 2014.

ICE's actions satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until ICE provides documentation to support that the planned corrective actions are completed.

Appendix A
Objectives, Scope, and Methodology

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

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

We coordinated the implementation of this audit of IT security controls with the DHS Chief Information Security Officer. We interviewed CBP, ICE, TSA, and DHS Office of the Chief Information Security Officer staff. We conducted site visits of CBP, ICE, and TSA facilities at and near DFW. We compared DHS IT infrastructure that we observed onsite with the documentation provided by the auditees.

We reviewed 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 the components in the areas of system documentation, patch management, and wireless security. We 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 field work and the information summarized in this report.

We conducted this performance audit between September 2013 and February 2014 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable

basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

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

Appendix B
Management Comments to the Draft Report

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

Homeland Security

August 4, 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 Dallas/Fort Worth International Airport" (Project No. 13-010-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's) work in planning and conducting its review and issuing this report.

DHS is pleased to note OIG's recognition that U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) server rooms and communications closets at the Dallas/Fort Worth International Airport (DFW), the Port Office of Dallas, and the Special Agent in Charge (SAC) Dallas Office were clean and well maintained, and that CBP, ICE, and the Transportation Security Administration (TSA) server rooms were within humidity ranges established by DHS policies. In addition, the report documents that CBP had implemented additional physical security for information technology (IT) assets in public areas; and taken actions to correct and resolve identified vulnerabilities concerning the technical controls over patch management.

The draft report contained 19 recommendations, 18 with which the Department concurs and 1 with which it non-concurs (Recommendation 6). Specifically, OIG recommended that the:

Recommendation 1: TSA Chief Information Officer (CIO) comply with DHS policy concerning physical security, temperature, housekeeping and electronic power supply protection at all locations at DFW that contain TSA IT assets.

Response: Concur. TSA previously recognized the need to improve power protection at DFW and initiated a project in 2013 to replace failing Uninterruptable Power Supply (UPS) devices. In November and December 2013, TSA replaced 22 UPS devices, of which 16 were decommissioned and replaced with surge protectors. The remaining six UPSs were refreshed. Additionally, Federal Air Marshal Service (FAMS) temp/humidity sensors are in place and functional. Documentation illustrating remediation of several housekeeping concerns was provided to OIG. However, in order to complete the recommendation, TSA must secure the

cooperation of third parties at DFW. TSA leases property at DFW. TSA will work with these third parties to close the recommendation. Estimated Completion Date (ECD): To Be Determined (TBD).

Recommendation 2: TSA CIO determine whether it is necessary and cost effective to establish redundant data telecommunications services at TSA's Coppell facility and DFW terminal locations.

Response: Concur. TSA has determined it is not necessary to install redundant data circuits for each of the individual circuits already at DFW, because TSA has seven telecommunications data circuits providing connectivity to the Federal Security Director's Office, FAMS Field Office, and five DFW terminals. These circuits provide connectivity to TSA network for services such as email, online training, and Call Manager for Voice over Internet Protocol (VoIP) directory services and voicemail. Internal and external calls on the TSA VoIP phones would not be affected, since they are connected via separate Primary Rate Interface (PRI) voice circuits. Should a circuit outage be experienced, the Transportation Security Officers can take advantage of the services accessible from another terminal or the Federal Security Director's office. TSA has deployed other types of communication capabilities that use Wi-Fi and cellular broadband technologies that provide employees with additional connectivity. In-Line Baggage screening would not be affected by a circuit outage since these functions do not rely on the telecommunication lines of TSA network.

A review of the current enterprise telecommunication circuits and associated operations and maintenance costs are approximately $30 million annually. TSA determined it is not cost-effective to install redundant circuits considering the multiple communications and connectivity capabilities already available. TSA currently has adequate redundant capabilities which allow for continuity of airport security operations. For example:

- the Blackberry service is on a separate network that provides email services if the TSA network at DFW is not accessible;
- users can access their email via TSA Outlook Web Access Portal through any internet connection;
- DFW has Mobile Wi-Fi (MiFi) access for users to virtual private network to the TSA network;
- cellular broadband access through hotspot capabilities; and
- internal and external calls on the TSA VoIP phones would not be affected since they are connected via separate voice PRI circuits.

Accordingly, we request that OIG consider this recommendation resolved and closed.

Recommendation 3: TSA CIO establish a process to report STIP computer security incidents to the TSA SOC.

Response: Concur. TSA follows the Standard Operating Procedure 1404, "Incident Response for Computer Security Incidents." TSA's Cybersecurity Awareness and Outreach Support Team will reach out to the DFW TSA staff to appropriately train those personnel on the correct incident reporting process. ECD: June 30, 2015.

2

Recommendation 4: TSA CIO scan all TSA servers annually and resolve identified vulnerabilities within the timeframe or direction stated in the Information Security Vulnerability Management message published by the DHS SOC.

Response: Concur. TSA servers are scanned on a monthly basis and the results or data feeds are submitted to the DHS Vulnerability Management Branch. Evidence of reports can be provided as requested. TSA supports the DHS Information Security Vulnerability Management (ISVM) program by resolving vulnerabilities as directed by the DHS Security Operations Center (SOC) to Alerts and Bulletins. Accordingly, we request that OIG consider this recommendation resolved and closed.

Recommendation 5: TSA CIO provide required vulnerability assessment reports to the DHS Vulnerability Management Branch.

Response: Concur. TSA servers are scanned on a monthly basis and the results or data feeds are subsequently submitted to the DHS Vulnerability Management Branch. Evidence of reports will be provided to OIG, upon request. Accordingly, we request that OIG consider this recommendation resolved and closed.

Recommendation 6: TSA CIO establish interconnection security agreements to document the interconnection between STIP and non-DHS baggage handling systems.

Response: Non-Concur. The Security Technology Integrated Program (STIP) does not have an interconnection with non-DHS baggage handling systems, and therefore an interconnection security agreement is not needed. Accordingly, we request that OIG consider this recommendation resolved and closed.

Recommendation 7: TSA CIO document in the system security plan the STIP servers, switches, and workstations.

Response: Concur. The STIP Explosive Detection System server and endpoint inventory will be assessed during the Security Authorization process during 2014-2015 and shall be added as an Artifact in the DHS Information Assurance Compliance System, where the Security Plan is also stored. ECD: June 30, 2015.

Recommendation 8: CBP CIO maintain the temperature and humidity of the identified server rooms within the temperature and humidity ranges established by the DHS 4300A Sensitive Systems Handbook.

Response: Concur. CBP corrected the temperature in Dallas Port Office local area network (LAN) Room 123. Repairs were made to the existing air conditioner, resulting in cooler temperatures supplied by air conditioning. The temperature in this room is now 66 degrees Fahrenheit. CBP corrected the temperature in DFW Airport LAN Room D22F432 by asking DFW Airport to lower the set point of the room to 68 degrees Fahrenheit. The average temperature is now 65.1 degrees Fahrenheit and supporting documentation for this was provided to OIG on July 15, 2014. CBP is working with DFW Airport to establish monitoring and alerting for temperatures that fall outside established ranges within LAN Room D22F432. ECD: October 31, 2014.

3

Recommendation 9: CBP CIO address and resolve identified vulnerabilities within the timeframe or direction stated in the Information Security Vulnerability Management message published by the DHS SOC.

Response: Concur. CBP will continue to patch system vulnerabilities in a timely manner and will ensure that the outstanding patches are implemented. ECD: December 31, 2014.

Recommendation 10: CBP CIO designate an ISSO for the WFPS.

Response: Concur. CBP will provide Information System Security Officer (ISSO) duties to Windows File and Print System (WFPS) initially through existing ISSO resources while a contract ISSO is brought onto the existing contract. Other options are being reviewed related to WFPS boundaries. ECD: November 30, 2014.

Recommendation 11: CBP CIO store, maintain, and review WFPS and DHCP audit logs as recommended by the DHS 4300A Sensitive Systems Handbook.

Response: Concur. CBP will store, maintain, and review WFPS audit logs when an ISSO is assigned. Regarding the Dynamic Host Configuration Protocol (DHCP) audit logs, CBP has submitted a funding request and is pursuing the capability to meet this requirement. Remediation of this part of the finding will depend upon funding approval which is expected to be determined by the end of fiscal year 2014. ECD: TBD.

Recommendation 12: ICE CIO maintain server rooms at DFW within DHS' recommended temperature ranges.

Response: Concur. ICE will work with CBP to request and complete changes necessary with DFW parties to maintain the server rooms within DHS' recommended temperature ranges. ECD: September 30, 2014.

Recommendation 13: ICE CIO determine whether it is necessary and cost effective to establish redundant data telecommunications service at the SAC Dallas facility.

Response: Concur. ICE Homeland Security Investigations (HSI) will review the potential mission/business impact if the SAC Dallas Facility loses connectivity. A risk-based decision to establish redundant data telecommunications will be made after the analysis is complete. ECD: December 31, 2014.

Recommendation 14: ICE CIO determine whether it would be cost effective to share the DHS OneNet connection in the shared CBP/ICE communications closet.

Response: Concur. ICE Office of the Chief Information Officer (OCIO) will work with CBP to determine if it is cost-effective to share the DHS OneNet Connection in the DFW shared CBP/ICE communications closet. ECD: December 31, 2014.

4

Recommendation 15: ICE CIO resolve identified vulnerabilities within the timeframe or direction stated in the Information Security Vulnerability Management message published by the DHS SOC.

Response: Concur. There were nine vulnerabilities noted in the audit report. The ICE OCIO Workstations with File and Print Servers (OWFPS) ISSO coordinated with the ICE Information Technology Field Office (ITFO) Regional Leads to install the remaining patches. Eight vulnerabilities were remediated and validated by the ICE SOC on December 16, 2013. The one remaining vulnerability was remediated and validated on December 16, 2013. On a monthly basis, the ICE Chief Information Security Officer and Authorizing Official meet to review ISVM compliance over the previous 60 days. During this meeting approval to create plan of action and milestones (POA&Ms) for un-met ISVM dates are provided and/or a request is made to patch devices in a specified time period. Scans were sent to OIG on December 16, 2013. Accordingly, we request that OIG consider this recommendation resolved and closed.

Recommendation 16: ICE CIO provide all required vulnerability assessment reports to the DHS Vulnerability Management Branch.

Response: Concur. An ongoing schedule for scanning OWFPS Organizational Units (OUs) on a monthly basis, which includes the SAC Dallas and the DFW, has been developed and implemented. Results of the scans are provided in ICE's monthly report to the DHS vulnerability Management Branch. Evidence of reports can be provided separately. A 6-month forecasted Vulnerability Assessment Test (VAT) scan schedule (artifact will be provided separately) was created and implemented as part of the ICE Office of the Chief Information Security Officer's (OCISO's) SOC transition to a new vendor. Accordingly, we request that OIG consider this recommendation resolved and closed.

Recommendation 17: ICE CIO scan all ICE servers at the SAC Dallas sites annually, including HSI systems separated from DHS OneNet.

Response: Concur. An ongoing schedule for scanning OWFPS OUs, which includes the SAC Dallas and DFW, has been developed and implemented. Evidence of scanning completion can be provided separately. A 6-month forecasted VAT scan schedule (artifact will be provided separately) was created and implemented as part of the ICE OCISO's SOC transition to a new vendor.

The ICE OCISO and ICE HSI will determine if scanning the stand-alone servers is appropriate. The servers contain law enforcement sensitive data; therefore there is a need to verify that chain of custody rules are not violated by the scan. After the determination is made, either a POA&M will be opened by ICE HSI to determine procedures for coordinating with the ICE SOC to scan the ICE HSI systems separate from DHS OneNet or the ICE OCISO will assist ICE HSI with creating a waiver request. ECD: December 31, 2014.

Recommendation 18: ICE CIO use a connection protocol that employs secure authentication, or disable unnecessary ports from the server.

Response: Concur. The unsecure protocol, telnet, was a default setting for the remote administration access that had not been disabled. The OWFPS ISSO submitted a request to the

5

ICE ITFO Regional Leads to manually disable telnet on the SAC and DFW servers. The ICE SOC ran scans on December 16, 2013 and validated that the issue was remediated. This remediation was noted in the audit report. Scan results were provided to OIG on December 16, 2013. Accordingly, we request that OIG consider this recommendation resolved and closed.

Recommendation 19: ICE CIO include the HSI surveillance system servers in a recognized FISMA [Federal Information Security Management Act]-inventoried system.

Response: Concur. ICE OCISO is currently working with ICE HSI to determine options for including the HSI surveillance system servers into a recognized FISMA package.
ECD: August 31, 2014.

Again, thank you for the opportunity to review and provide comments 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.

6

Appendix C
DHS Activities at Dallas/Fort Worth International Airport

Management Directorate

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

- DHS OneNet – provides network communications for the DHS sensitive but unclassified environment. The Department's goal for the DHS OneNet is to facilitate the ability of DHS components to share data by integrating component networks into a shared network infrastructure to include network operations, security operations, architecture, and management. DHS OneNet supports communication and interaction among many organizational entities within and outside of DHS and has been designated as a DHS mission-essential system to perform one or more of the components' mission-essential functions.

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

Transportation Security Administration

TSA's activities include screening passengers and baggage on departing flights at DFW. To support these activities, TSA has operations in each of the DFW terminals and at a nearby office building. We audited IT security controls at the following TSA locations:

- Office of the Federal Security Director, Coppell, TX
- Office of FAMS, Coppell, TX
- DFW Terminals A, B, C, D, and E

TSA staff at these locations use the following systems:

- FAMSNet – provides the IT infrastructure to support the FAMS mission. FAMS staff includes law enforcement officers that help to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. FAMSNet supports FAMS' overall critical mission by providing Internet access as well as internal access to FAMS information systems including, but not limited to, email, database(s), file sharing, printing, and a number of critical administrative and enforcement related programs. FAMSNet also provides a communication

pathway to third-party and government networks, such as those used by DHS, TSA, the Federal Aviation Administration, and other State and local law enforcement entities. FAMSNet has been designated a mission-essential system.

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

- STIP – combines many different types of components, including transportation security equipment, servers and storage, software/application products, and databases. A user physically accesses the transportation security equipment to perform screening or other administrative functions. STIP-enablement of transportation security equipment encompasses Explosive Trace Detectors, EDS, Advanced Technology X-ray, Advanced Imaging Technology, and Credential Authentication Technology. TSA's OSC is the owner of STIP. STIP has not been designated a mission-essential system.

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

U.S. Customs and Border Protection

At DFW, CBP personnel staff up to 45 primary passenger lanes, review flight data for terrorist related activities, collect duties, and when CBP discovers a violation of law, assess fines and civil penalties. Additionally, CBP staff at nearby locations use IT assets to perform cargo manifest review and targeting, as well as outbound passenger review and targeting.

We audited IT security controls at the following CBP locations:

- Port Office of Dallas, Dallas/Fort Worth, TX
- DFW Concourse D

CBP staff at these locations use the following systems:

- Southwest Field LAN – provides the general support network infrastructure and end points for DHS/CBP users and electronic communications tools, which enables the execution of official duties. The Southwest Field LAN consists of 331 geographically dispersed sites using 3,423 devices connected to the DHS OneNet

to provide application services to CBP field offices. The Southwest Field LAN boundary spans the Southwest and East Texas Office of Information Technology Field Support Regions to include Arizona, New Mexico, Texas and Oklahoma. The Southwest Field LAN has been designated a mission-essential system.

- CBP NOC – maintains the performance, management, and administration capabilities of the CBP core network and CBP field site locations and the underlying supporting environment. In addition, CBP NOC deploys and maintains a network management system and a suite of network devices that collect and report real-time information on the network. Further, CBP NOC system enforces authorizations for controlling the flow of information within the system and between interconnected systems (DHS OneNet and CBP Field Sites) in accordance with CBP/DHS Sensitive Security Policy. CBP NOC has been designated a mission-essential system.

- Windows 7 PC Client 6.1 – used as the Windows 7 standard desktop image for CBP workstations. The image does not store any personally identifiable information. The Windows 7 PC Client 6.1 consists of a set of standard configurations to build the client for Windows 7, install the application software and configure the system according to DHS and CBP technical standards. Windows 7 PC Client 6.1 has not been designated a mission-essential system.

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

- TECS – supports enforcement and inspection operations for several components of DHS and is a vital tool for the law enforcement and intelligence communities on the local, State, tribal, and Federal Government levels.[12] TECS comprises several subsystems that include enforcement, inspection, and intelligence records relevant to the antiterrorist and law enforcement mission of CBP and the other Federal agencies it supports. TECS has been designated a mission-essential system.

[12] 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

ICE's Office of SAC, Dallas, Texas, is responsible for the administration and management of investigative and enforcement activities within its geographical boundaries. Within the SAC Dallas office, the HSI Airport Group is responsible for the identification, disruption, and dismantlement of transnational criminal organizations attempting to exploit vulnerabilities within the air transportation system at DFW. The HSI Airport Group's areas of concern at DFW include:

- contraband smuggling,
- currency smuggling,
- national security,
- human smuggling/trafficking,
- sexual tourism,
- insider threat, and
- the theft and trafficking of cultural heritage and art.

The HSI Airport Group also covers investigations for the Addison, Alliance, Love Field, Meacham, and McKinney airports, as well as smaller general aviation landing fields and facilities within the HSI Dallas area of responsibility.

We audited IT security controls at the following ICE locations:

- DFW International Airport Group facility, DFW Terminal D
- SAC Dallas Office, Irving, TX

ICE staff at these locations use the following systems:

- OWFPS – provides workstation, laptop, print services, and file services to ICE program areas nationwide. Print servers allow ICE users to use networked printing. The file servers provide a networked file repository for groups and users. OWFPS includes workstations, laptops, file servers, printers, and print servers at each field site managed by the ICE OCIO IT Field Operations Branch. OWFPS has not been designated a mission-essential system.

- ICE Communication over Networks – a general support system that provides support for network devices and data communications that employ the

infrastructure throughout ICE and 287(g) sites in the Continental United States.[13] The authorization boundary for ICE Communication over Networks includes ICE Operations managed switches, firewalls, and intrusion detection sensors. ICE Communication over Networks has not been designated a mission-essential system.

- A communication surveillance and analysis system that helps HSI staff with intelligence gathering and live collection of 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 may be installed and connected to the ICE network infrastructure or on a separate standalone network. This has not been designated a mission-essential system.

- A standalone electronic surveillance system that is part of HSI's undercover operations. The system, which is not attached to the DHS One Network, intercepts cell phones, voice mail, and voice pagers, as well as traditional landline telephones. The system also intercepts electronic communication, such as text messages, email, non-voice computer and Internet transmissions, faxes, communications over digital-display paging devices, and, in some cases, satellite transmissions. The system is authorized for use in accordance with Title III of the *Omnibus Crime Control and Safe Streets Act of 1968*, as amended. This has not been designated a mission-essential system.

[13] The 287(g) program, under the *Immigration and Nationality Act*, allows a state and local law enforcement entity to enter into a partnership with ICE, under a joint Memorandum of Agreement, in order to receive delegated authority for immigration enforcement within their jurisdiction.

Appendix D
Major Contributors to This Report

Sharon Huiswoud, Director
Kevin Burke, Audit Manager
Charles Twitty, Senior Auditor
Steven Tseng, IT Specialist
Craig Adelman, 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
Commissioner, CBP
CBP CIO
CBP Audit Liaison
Director, ICE
ICE CIO
ICE Audit Liaison
Administrator, TSA
TSA CIO
TSA Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

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 (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

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

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.