

# Department of Homeland Security **Office of Inspector General**

## Technical Security Evaluation of DHS Activities at Hartsfield-Jackson Atlanta International Airport



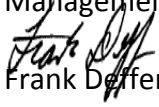


**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

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

July 12, 2013

MEMORANDUM FOR: Jeffrey Eisensmith  
Chief Information Security Officer  
Management Directorate

FROM:   
Frank Deffer  
Assistant Inspector General  
Office of Information Technology Audits

SUBJECT: *Technical Security Evaluation of DHS Activities at  
Hartsfield-Jackson Atlanta International Airport*

Attached for your action is our final report, *Technical Security Evaluation of DHS Activities at Hartsfield-Jackson Atlanta International Airport*. We incorporated the formal comments from U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Transportation Security Administration in the final report.

The report contains 20 recommendations aimed at improving information security at Hartsfield-Jackson Atlanta International Airport. Your office concurred with 20 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. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Based on information provided in your response to the draft report, we consider the 20 recommendations resolved. The Department has already taken actions to resolve reported deficiencies, including providing documentation to support the resolution and closure of recommendations 5 and 20. Once your office has fully implemented the remaining resolved but open recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.



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

---

Consistent with our responsibility under the *Inspector General Act*, we are providing 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, at (202) 254-5451.

Attachment



## Table of Contents

Executive Summary.....	1
Background .....	2
Results of Review .....	7
CBP Did Not Comply Fully With DHS Sensitive System Policies .....	7
Recommendations .....	15
Management Comments and OIG Analysis .....	16
ICE Did Not Comply Fully With DHS Sensitive System Policies .....	18
Recommendations .....	26
Management Comments and OIG Analysis .....	27
TSA Did Not Comply Fully With DHS Sensitive System Policies .....	29
Recommendations .....	34
Management Comments and OIG Analysis .....	34

## Appendixes

Appendix A: Objectives, Scope, and Methodology.....	37
Appendix B: Management Comments to the Draft Report.....	39
Appendix C: Major Contributors to This Report .....	44
Appendix D: Report Distribution.....	45

## Abbreviations

AAG	Atlanta Airport Group
AO	Authorizing Official
ATL	Hartsfield-Jackson Atlanta International Airport
BIA	business impact assessment
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CVE	Common Vulnerabilities and Exposures
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DHS OneNet	DHS One Network



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

DHS Directive 4300A	<i>DHS Sensitive Systems Policy Directive 4300A</i>
DHS 4300A Handbook	<i>DHS 4300A Sensitive Systems Handbook</i>
FAMS	Federal Air Marshal Service
FAMSNet	Federal Air Marshal Service Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002, as amended
GAO	Government Accountability Office
GSS	general support system
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
ICON	ICE Communication Over Networks
ICS	Infrastructure Core System
ISA	interconnection security agreement
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVM	Information Security Vulnerability Management
IT	information technology
LAN	local area network
LAX	Los Angeles International Airport
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OIG	Office of Inspector General
OWFPS	OCIO Workstations with File and Print Servers
PALS	Portable Automated Lookout System
SAC	Special Agent in Charge
SAP	System Availability Project
SOC	Security Operation Center
SP	Special Publication
STIP	Security Technology Integrated Program
TSA	Transportation Security Administration
TSANet	Transportation Security Administration Network
TSE	transportation security equipment
WAN	wide area network
WFPS	Windows File and Print System



## **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 Hartsfield-Jackson Atlanta International Airport. U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Transportation Security Administration operate information technology systems that support homeland security operations at this airport.

Our evaluation focused on how these components had implemented computer security technical, management, and operational controls 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 internal controls. We also reviewed applicable policies, procedures, and other relevant documentation.

The information technology security controls implemented at these sites have deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' respective information technology systems. For example, a technical control includes regularly scanning servers for vulnerabilities. However, not all departmental servers were being scanned for vulnerabilities.

Also, these components were not always resolving known technical vulnerabilities in a timely fashion. Additionally, there were deficiencies in physical security and environmental controls at departmental server rooms. Further, information systems security officers for 6 of the 10 identified systems in use at the airport were not reviewing system audit logs. For example, some of these officers did not have access to the files where the audit logs were kept.

We have briefed the components, and the Department's Chief Information Security Officer, on the results of our audit. We have also made 20 recommendations to resolve the control deficiencies identified in this report. Management comments and Office of Inspector General analysis are included at appendix B.



## Background

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security (DHS) officials with timely information on whether they had properly implemented DHS information technology (IT) security policies at critical sites. Our program is based on *DHS Sensitive Systems Policy Directive 4300A*, version 9.1 (DHS Directive 4300A), which applies to all DHS components. It provides direction to managers and senior executives regarding the management and protection of sensitive systems. DHS Directive 4300A also describes policies relating to the operational, technical, and management controls that are necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation within the DHS IT infrastructure and operations. A companion document, the *DHS 4300A Sensitive Systems Handbook*, version 9.1 (DHS 4300A Handbook), provides detailed guidance on the implementation of these policies. For example, according to the DHS 4300A Handbook:

Components shall categorize systems in accordance with FIPS [Federal Information Processing Standards] 199, *Standards for Security Categorization of Federal Information and Information Systems* and shall apply the appropriate NIST SP 800-53 controls.<sup>1</sup>

DHS IT security policies are organized under operational, technical, and management controls. According to DHS Directive 4300A, these controls are defined as follows:

- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. These controls are designed to improve the security of a particular system or group of systems, and often rely on management and technical controls.
- **Technical Controls** – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations, and support security requirements for applications and data.
- **Management Controls** – Focus on managing both the system information security controls and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.

---

<sup>1</sup> This refers to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

Our evaluation focused on U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA), which have activities at Hartsfield-Jackson Atlanta International Airport (ATL) and rely on a range of IT assets to support their respective missions. As a Category X airport, ATL is one of the airports with the largest number of enplanements in North America, processing approximately 92 million passengers in 2011.<sup>2</sup>

### U.S. Customs and Border Protection

At ATL, CBP Officers and Agricultural Specialists staff 101 primary passenger lanes, review flight data for terrorist-related activities, collect duties, and process 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 reviewed the following CBP locations:

- Port Office, Atlanta, GA
- Office of Field Operations, College Park, GA
- St. George Warehouse, Forest Park, GA
- ATL Concourse E
- ATL Concourse F

CBP staff at these locations use the following systems:

- **The DHS One Network (OneNet).** This general support system (GSS) provides all wide area network (WAN) communications for the service-wide DHS sensitive but unclassified environment. Although the DHS Management Directorate's Enterprise Services is the system owner, CBP serves as the DHS OneNet steward. CBP is also responsible for daily operations and management of the enterprise-wide DHS OneNet. In 2005, DHS began to consolidate components' existing infrastructures into a single WAN, known as the DHS OneNet. The DHS OneNet supports communication and interaction among many organizational entities within and outside DHS. The Department's goal for the DHS OneNet is to facilitate the ability of all DHS components to share data by integrating component networks into a shared network infrastructure to include network operations, security operations, architecture, and management.

---

<sup>2</sup> There are five categories of airports: X, I, II, III, and IV. Category X airports have the largest number of enplanements and Category IV airports have the smallest number.





## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

- **The Southeast Field Local Area Network (LAN).** This network provides the General Support Network Infrastructure and end points for DHS/CBP users and electronic communications tools that enables the execution of official duties. The Southeast Field LAN consists of 174 geographically dispersed sites using more than 6,800 devices connected to the DHS OneNet to provide application services to CBP field offices.
- **The Network Operations Center (NOC).** This center maintains the performance, management, and administration capabilities of the CBP core network and all CBP field site locations and the underlying supporting environment. In addition, the CBP NOC deploys and maintains a network management system and a suite of network devices that collect and report real-time information related to the overall health of the network. Further, the system enforces approved 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.
- **The Windows File and Print System (WFPS).** This system provides CBP with file and printing services using the Microsoft Windows Server 2008 x64 platform.
- **TECS.**<sup>3</sup> This system is key for border enforcement and the sharing of information about people who are inadmissible or may pose a threat to the security of the United States. TECS plays an essential role in the assessment and inspection of travelers entering the United States and in supporting the requirements of other Federal agencies. TECS supports over 80,000 users from more than 20 Federal agencies. TECS interfaces with many law enforcement systems and Federal agencies interactively, including the Federal Bureau of Investigation's National Crime Information Center and the International Justice & Public Safety Network. Disclosure of information in TECS may be provided to Federal, State, local, tribal, and foreign law enforcement, counterterrorism, and border security agencies on a case-by-case basis where DHS determines such disclosure is appropriate and otherwise consistent with U.S. law, including in the enforcement of certain civil or criminal laws.

---

<sup>3</sup> 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.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### U.S. Immigration and Customs Enforcement

ICE's Office of the Special Agent in Charge (SAC) identifies and investigates security issues with a foreign nexus at ATL. The SAC's areas of responsibility at ATL include the following:

- Investigations of internal criminal conspiracies involving employees of companies doing business at ATL;
- Identification, interdiction, and apprehension of currency smugglers traveling through ATL;
- Enforcement activities on international drug-smuggling carriers arriving at ATL;
- Enforcement actions that center on the interception of parcels containing illegal narcotics and initiation of controlled deliveries on these parcels if appropriate;
- Investigations of illegal workers having unescorted access to secure areas of the airport; and
- Investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack, or exploitation.

The SAC Atlanta Airport Group (AAG) staff supports the ICE Office of Investigations mission by providing access to law enforcement data processing resources available through DHS OneNet. Interconnectivity with DHS OneNet further enhances the mission support capabilities of the SAC AAG by allowing remote access to their users through secure virtual private networking and access to the public Internet. Local data processing resources directly supported by the SAC AAG are file sharing and print services. The ICE locations of the AAG facility at College Park, GA, and the SAC Atlanta facility at East Point, GA, were reviewed. ICE staff at these locations use the following systems:

- **Office of the Chief Information Officer Workstations with File and Print Servers (OWFPS).** The purpose of the OWFPS system is to provide workstations, laptops, print services, and file services to all ICE program areas nationwide. Print servers allow ICE users to utilize networked printing. The file servers provide a networked file repository for all groups and users. OWFPS reflects all nationwide workstations, laptops, file servers, printers, and print servers managed by the ICE OCIO IT Field Operations Branch.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

- **ICE Communication over Networks (ICON).** ICON is a GSS that provides support for all network devices and data communications that employ the infrastructure throughout ICE and 287 sites in the continental United States. The authorization boundary for the ICON consists of ICE Operations managed switches, firewalls, intrusion detection sensors and packet shapers, and ICE Engineering–managed WAN optimization appliances. The ICON is connected to the DHS OneNet.
- **A communication surveillance and analysis system.** The system helps Homeland Security Investigations (HSI) staff with intelligence gathering and live collection of data in support of its law enforcement mission. Specifically, the system assembles historical telephone records and permits searches of warrant data from online providers. Additionally, this system is connected to the DHS OneNet.
- **A standalone electronic surveillance system as part of HSI’s undercover operations.** The system is not attached to the DHS OneNet. Specifically, the system 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 satellite transmissions (in some cases). The system is authorized for use in accordance with the *Wire and Electronic Communications Interception and Interception of Oral Communication Act* (formally known as the "Title III" Wiretap Act, 18 U.S.C §§ 2510-2520).

### Transportation Security Administration

TSA’s activities include screening passengers and baggage on all departing flights at ATL. To support these activities, TSA has operations in each of the ATL terminals and at a nearby office building. We reviewed the following TSA locations:

- Office of the Federal Security Director, Atlanta, GA
- Domestic Terminals (ATL Concourse E and T)
- International Terminal (ATL Concourse F)
- Office of Federal Air Marshal Service (FAMS), College Park, GA

TSA staff at these locations use the following systems:

- **Federal Air Marshal Service Network (FAMSNet).** The purpose of FAMSNet GSS is to provide an IT infrastructure that supports the FAMS mission. Federal Air Marshals are law enforcement officers that help to detect, deter, and defeat



hostile acts targeting U.S. air carriers, airports, passengers, and crews. The FAMSNet GSS supports the FAMS' overall critical mission by providing an IT infrastructure that facilitates Internet access as well as internal access to FAMS information systems including but not limited to email, database access, file sharing, printing, and a number of critical administrative and enforcement related programs. FAMSNet GSS also provides a communication pathway to third-party and government networks such as DHS, TSA, the Federal Aviation Administration, Sabre Travel Network, and other State and local law enforcement entities. Additionally, this system is connected to the DHS OneNet.

- **Infrastructure Core System (ICS).** This system provides core services, including file and print services, to the entire TSA user community.
- **The Security Technology Integrated Program (STIP).** The STIP combines many different types of components. The STIP components include transportation security equipment (TSE), servers and storage, software/application products, and databases. A user physically accesses the TSE to perform screening or other administrative functions.
- **The Transportation Security Administration Network (TSANet).** Owing to its geographically dispersed topology, the TSANet GSS is considered a WAN. The TSANet GSS consists of the WAN backbone and LAN at each site that connects to the backbone. The TSANet GSS provides connectivity for airports and their users. The TSANet is connected to the DHS OneNet.

## Results of Review

### **CBP Did Not Comply Fully With DHS Sensitive System Policies**

---

CBP did not comply fully with DHS technical, management, and operational policies for its servers, routers, and switches operating at ATL. For example, CBP and DHS OneNet Information Systems Security Officers (ISSOs) were not reviewing audit logs on a weekly basis. CBP also had not implemented corrective action plans for high vulnerabilities identified by technical scans of its servers at ATL.<sup>4</sup>

---

<sup>4</sup> The severity level used by the scanning software is derived from the open framework common vulnerability scoring system, which is under the custodial care of the Forum of Incident Response and Security Teams. The common vulnerability scoring system uses a numerical score from zero to 10 that is used by the scanning software to assign a severity level. When the associated score is zero, the severity level is "Info." When the associated score is less than four, the severity level is "Low." When the associated score is less than seven, the severity level is "Moderate." When the associated score is less than 10, the severity level is "High." When the associated score is 10, the severity level is "Critical."



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Additionally, CBP had not updated security documentation to include the risks associated with the use of out-of-band modems on the DHS OneNet routers operating at ATL.<sup>5</sup>

CBP's server rooms contained excess storage and were not always within the humidity range established by DHS policies. Additionally, CBP had not specifically assigned the responsibility to review audit logs to prevent a network outage. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at ATL.

#### Technical Controls

CBP's implementation of technical controls for systems operating at ATL did not conform fully to DHS policies. Specifically, CBP ISSOs were not reviewing audit logs on a weekly basis and were not receiving adequate real-time alerts. Additionally, identified vulnerabilities on CBP servers were not being resolved in a timely fashion.

#### Audit Logs and Real-Time Security Alerts

CBP's implementation of technical controls for systems operating at ATL did not conform fully to DHS policies. For example, while the ISSO for the WFPS was reviewing the audit logs and receiving real-time alerts, the ISSOs for the Southeast Field LAN and NOC were not reviewing the audit logs on a weekly basis. These ISSOs reviewed the audit logs only when there was a problem. These ISSOs relied on the Security Operation Center (SOC)/NOC engineers and analysts to review the audit logs. Additionally, these ISSOs received real-time security alerts from the SOC/NOC.

CBP stores system event notification message logs, or syslogs, for system and network security events on a syslog server that aggregates the logs and facilitates auditing.<sup>6</sup> However, the Southeast Field LAN and NOC ISSOs did not have access to the syslog server. According to CBP staff, they are in the process of providing access to the syslog server.

---

<sup>5</sup> Out-of-band devices provide access to information systems through network paths that are physically separate from those used for operational traffic.

<sup>6</sup> According to NIST SP 800-92, *Guide to Computer Security Log Management*: Syslog provides a simple framework for log entry generation, storage, and transfer, that any OS [Operating System], security software, or application could use if designed to do so. Many log sources either use syslog as their native logging format or offer features that allow their log formats to be converted to syslog format.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Additionally, the DHS OneNet ISSO was not reviewing audit logs. Specifically, the DHS OneNet ISSO did not have the tools to be able to perform weekly reviews of audit logs generated by network routers. Further, the DHS OneNet ISSO was not receiving adequate real-time alerts to address identification and resolution of possible security events affecting the system.

The DHS OneNet ISSO team indicated that they received real-time alerts for security incidents. However, according to the DHS OneNet ISSO team, the threshold used by the SOC for determining which alerts were to be provided was not adequate. For example, repeated invalid login attempts, which might indicate a possible attack, would not result in a real-time alert from the SOC.

According to the DHS 4300A Handbook:

The DHS ISVM [Information Security Vulnerability Management] Program, managed through the SOC, provides Component CISOs [Chief Information Security Officer]/ISSMs [Information Systems Security Manager] and operational support personnel (e.g., ISSOs, System Administrators) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats.

Also, according to the DHS 4300A Handbook, ISSOs should—

Review audit records at least weekly, or in accordance with the SP [Security Plan].

The SOC reviewed DHS OneNet audit logs on a limited basis. However, these reviews were performed on a case-by-case basis, such as when audit events require correlation among numerous network devices. Additionally, the SOC did not perform reviews of the audit logs on a weekly basis. Further, the DHS OneNet ISSO was not provided access to the log aggregation tool to perform independent audit log review.

CBP and the DHS Management Directorate are making progress toward providing the necessary tools for the DHS OneNet ISSO to perform weekly audit log review. However, full deployment of the centralized audit log review tool has been delayed pending availability of sufficient backup storage area network infrastructure to ensure redundancy.

The ISSOs for Southeast Field LAN and the NOC will be able to better identify weaknesses and develop corrective action plans by having access to the audit



logs. Specifically, weekly reviews of audit logs will help identify whether problems exist and if corrective actions are required.

### Patch Management

We scanned CBP’s three servers at ATL for vulnerabilities in November 2012. This technical scan identified 13 high vulnerabilities on the three servers. (See table 1 for details.) Additionally, patch information for three vulnerabilities was published more than 6 months before the scans were performed.

**Table 1. Total Number of High and Critical Vulnerabilities and Instances by Common Vulnerabilities and Exposures (CVEs) and Vulnerability Name**

CBP Server Name	Total Number of CVEs <sup>7</sup>	Total Number of Unique Vulnerabilities <sup>8</sup>	Date of Last Vulnerability Scan Report to DHS <sup>9</sup>
Server 1	9	3	06/2012
Server 2	31	5	06/2012
Server 3	31	5	Not reported.
Total:	71	13	

According to DHS 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 CBP data. These risks include allowing remote code execution on CBP’s information systems.

<sup>7</sup> According to NIST Interagency Report 7298, Revision 1, *Glossary of Key Information Security Terms*, CVE is a dictionary of common names for publicly known information system vulnerabilities.

<sup>8</sup> 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.”

<sup>9</sup> The Information Security Scorecard used by DHS to determine compliance with reporting requirements obtains eight measures on operational systems, including vulnerability management. For fiscal year 2012, the vulnerability management metric was based upon the percentage of systems reporting vulnerability scanning results from the total number of reported inventory of operational systems. This column lists the date when a vulnerability scan was last reported to the Department for the listed system.



## Management Controls

CBP's implementation of management controls for systems operating at ATL did not conform fully to DHS policies. Specifically, CBP did not include the risk associated with the use of out-of-band modems in the DHS OneNet security documentation.

## Out-of-Band Modems

DHS OneNet service providers use out-of-band devices to provide access to information systems through network paths that are physically separate from those used for operational traffic. Specifically, these out-of-band devices can be used in delivery of router configuration information, firmware, and updates for malicious code protection. Additionally, the time necessary to restore network connectivity of the DHS OneNet at a field site may be reduced through the use of an out-of-band device.

Figure 1 illustrates an out-of-band device attached to a DHS OneNet router used to provide maintenance access in the event of a network failure.



**Figure 1. Out-of-Band Modem Device Attached to a DHS OneNet Router**

According to CBP and DHS Management Directorate staff, the out-of-band access to DHS OneNet routers is controlled and monitored by the telecommunications service providers. However, the DHS OneNet Security Plan does not document





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

the responsibilities and expected behavior of all individuals who use these devices to access the DHS OneNet.

According to the DHS 4300A Handbook:

The SP [Security Plan] provides a complete description of an information system, including purposes, functions, system boundaries, architecture, user groups, interconnections, hardware, software, encryption techniques, transmissions, and network configuration. It also provides an overview of the system's security requirements, describes the controls in place or planned, and delineates the responsibilities and expected behavior of all individuals who access the system.

Further, the out-of-band modems attached to DHS OneNet routers at ATL were observed ready to accept incoming connections. As a result, DHS OneNet availability for mission-critical activities may be vulnerable to disruption by unauthorized use of these devices.

According to the DHS 4300A Handbook:

Components shall ensure that maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.

The always-on status of the out-of-band modems during normal system operation creates a risk of misuse of these devices. Misuse of the out-of-band devices by telecommunications service provider employees could include attacks that affect the availability of critical resources such as email servers, web servers, routers, gateways, or other communications infrastructure.

### **Operational Controls**

Onsite implementation of operational controls that did not conform fully to DHS policies included inadequate humidity controls and excess storage in server rooms.

### **Environmental Controls**

CBP has three server rooms at ATL. Based on CBP's humidity reading at the time of our test, only one of the three server rooms was within the humidity range recommended by the DHS 4300A Handbook. Additionally, CBP did not have a



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

device to measure humidity in one of the server rooms. Further, according to our humidity and temperature measurements, all three server rooms did not meet DHS humidity standards and two did not meet DHS temperature standards. See table 2 for details.

**Table 2. CBP Server Room Humidity and Temperature**

Location	Humidity		Temperature	
	CBP	OIG <sup>10</sup>	CBP	OIG
157 Tradeport Drive	23%	18.5%	70°	77.7°
Field Office – Phoenix Blvd.	No device	23.4%	70°	76.9°
Concourse E	45%	24.1%	70°	68.7°

According to CBP staff, the Office of Inspector General (OIG) temperature and humidity readings were taken within the IT racks and were not indicative of the room conditions as a whole. However, CBP will work with the General Services Administration to control the temperature and humidity in the server and network rooms at ATL. In addition, CBP staff stated that server rooms at the Field Inspection Service are owned by the City of Atlanta and installation of temperature and humidity sensors require coordination with the City of Atlanta. CBP and the Port Office are in the process of working with the City of Atlanta to get permission to install these devices in the server rooms located at the airport.

According to the DHS 4300A Handbook:

The following should be considered when developing a strategy for temperature and humidity control:

- 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.

Also, several server and network rooms were being used for excess storage. Specifically, some rooms had shelves with supplies, including cleaning solutions.

<sup>10</sup> OIG staff measured the humidity and temperature at the front of racks containing information technology equipment in the identified DHS server rooms.



**Figures 2a and 2b. Before and After Pictures of Storage in a CBP Server Room**

According to the DHS 4300A Handbook:

In addition to the physical security controls... facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:

- Housekeeping protection from dirt and dust
- Combustible cleaning supplies protection (not to be kept in computer areas).

According to CBP staff, CBP is in the process of modifying space at ATL. CBP expects to have the server and network rooms cleaned within the next 30 days. For example, CBP has cleaned up excess debris, boxes, and hazardous items at two of its server rooms.

### **Systems Availability Project**

On August 11, 2007, Los Angeles International Airport (LAX) experienced a network outage that hindered operation at LAX for approximately 10 hours and affected more than 17,000 passengers. We reported in May 2008 that the outage occurred because CBP devices at LAX were flooded with electronic messages, a “broadcast storm,” from within the CBP LAN at LAX.<sup>11</sup> We recommended actions that CBP could implement to manage network outages more effectively. These recommendations included enhancing router logs and establishing automatic error notification messages. We also recommended that CBP determine whether their actions taken at LAX should also be taken at other ports of entry.

---

<sup>11</sup> *Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport*, May 2008, OIG-08-58.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

According to CBP staff, they have taken a number of steps to implement these recommendations. These actions included the development of the System Availability Project (SAP), which was established in order to implement corrective action at other CBP Ports of Entry. SAP-related actions at ATL included upgrades to switches, cable, and fiber. CBP also upgraded connectivity at ATL by installing redundant telecommunications lines with increased bandwidth.

CBP also has 20 Portable Automated Lookout System (PALS) laptops at ATL that can be used to process passengers if an outage occurs. Additionally, CBP has ordered additional laptop batteries and 30 more PALS laptops to increase its passenger processing capability during outages. Further, CBP passenger processing areas are part of ATL's emergency generator circuit. This emergency generator can provide power for up to 48 hours.

Although CBP has made improvements and upgrades at ATL to prevent future outages, it has not fully implemented the recommendations from our report. For example, CBP is not reviewing automated Dynamic Host Configuration Protocol (DHCP) server messages.<sup>12</sup> According to CBP staff, they are not reviewing these messages because there is no specific policy requiring the monitoring of DHCP messages. Additionally, the SOC is not monitoring ATL LAN audit logs to prevent a similar network outage as occurred at LAX. According to SOC staff, reviewing of the LAN audit logs is not their primary responsibility.

### **Recommendations**

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

#### **Recommendation #1:**

Provide ISSOs with real-time security alerts and the capability to review audit logs.

#### **Recommendation #2:**

Resolve high system vulnerabilities in a timely fashion.

---

<sup>12</sup> According to NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, "The DHCP service assigns IP addresses to hosts on a network as needed."



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### **Recommendation #3:**

Update the DHS OneNet Security Plan to document the risks associated with the use of out-of-band modems attached to DHS OneNet routers.

### **Recommendation #4:**

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

### **Recommendation #5:**

Maintain ATL server and network rooms free of excess storage and hazardous items that may cause damage to the system.

### **Recommendation #6:**

Assign the responsibility to review DHCP server automatic messages and ATL LAN audit logs.

### **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 at appendix B. DHS concurred with recommendations 1 through 6. Additionally, CBP has already taken actions to resolve reported deficiencies. Further, CBP has provided documentation to support the resolution and closure of recommendation 5. Recommendations 1 through 4 and recommendation 6 are considered resolved, but open pending verification of all planned actions.

### **Recommendation #1:**

CBP concurs and agrees to provide the ISSOs with access to the appropriate logs. Additionally, a standard operating procedure for reviewing logs on a weekly basis is being developed.



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

---

CBP's actions satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until CBP provides documentation to support that the planned corrective actions have been completed.

**Recommendation #2:**

CBP concurs and agrees to continue to patch system vulnerabilities in a timely manner, and also to ensure that outstanding patches are implemented.

CBP's actions satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until CBP provides documentation to support that the planned corrective actions have been completed.

**Recommendation #3:**

CBP concurs and has updated the DHS OneNet Security Plan to include the use of out-of-band modems. CBP will also document the risks associated with the use of out-of-band modems attached to DHS OneNet routers.

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

**Recommendation #4:**

CBP concurs and has procured a device that measures humidity. CBP has already tested this device at one location and plans to complete similar installations in all server rooms. The estimated completion date for this recommendation is August 30, 2013.

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

**Recommendation #5:**

CBP concurs and has removed excess storage and hazardous items from each of the identified server and network rooms. CBP also began inspecting the rooms for clutter and hazardous items and will continue doing so on a monthly basis. In addition, CBP is using a checklist to document the inspections. Network rooms



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

maintained by others are also being checked periodically. CBP requested that the OIG close recommendation 5.

Following receipt of the draft report, CBP provided all requested documentation to support actions taken. CBP's actions satisfy the intent of this recommendation. This recommendation is considered resolved and closed.

#### **Recommendation #6:**

CBP concurs and will research, clarify, monitor, and enforce responsibilities for the review of the DHCP server automatic messages and ATL LAN audit logs.

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

#### **ICE Did Not Comply Fully With DHS Sensitive System Policies**

---

ICE did not comply fully with DHS technical, management, and operational policies for its servers, routers, and switches operating at ATL. For example, the ISSO for the ICON system was not reviewing audit logs on a weekly basis. ICE also had not implemented software patches for critical and high vulnerabilities and was not regularly scanning its servers at ATL. Additionally, ICE had not completed the process to authorize the ICON system to operate. Further, not all ICE servers at ATL were accounted for as part of a *Federal Information Security Management Act of 2002 (FISMA)*, as amended, inventoried system.

ICE did not have escort procedures in place for its multiuse server room. Additionally, ICE's server rooms were not always within the temperature range established by DHS policies. Further, ICE had not determined whether redundant data telecommunications lines at these locations were warranted. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at ATL.

#### **Technical Controls**

ICE's implementation of technical controls for systems operating at ATL did not conform fully to DHS policies. For example, the ICON ISSO was not receiving real-time security alerts and was not reviewing audit logs on a weekly basis. Also, identified vulnerabilities on ICE servers were not being resolved in a timely



fashion. Further, not all ICE servers at ATL were being regularly scanned for vulnerabilities.

### **Audit Logs and Real-Time Security Alerts**

The OWFPS ISSO reviews system audit logs on a weekly basis and receives real-time security alerts. The ICON ISSO was not reviewing the audit logs and was not receiving real-time security alerts. Specifically, the ICON ISSO did not have access to the system directory, which contains the real-time security alerts.

According to the DHS 4300A Handbook, ISSOs should:

Review audit records at least weekly, or in accordance with the SP [Security Plan].

Additionally, according to the DHS 4300A Handbook:

The DHS ISVM Program, managed through the SOC, provides Component CISOs/ISSMs and operational support personnel (e.g., ISSOs, System Administrators) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats.

According to ICE staff, upon completion of the ICON security authorization, they will develop procedures to capture specific events in the audit logs. ICE staff will then review the audit logs on a weekly basis. Additionally, the ICON ISSO is taking steps to acquire access to the real-time security alerts.

Reviewing audit logs and receiving real-time alerts would provide the ICON ISSO with early warning advisories on security attacks, along with information on the most recent viruses.

### **Patch Management**

We scanned ICE's three servers at ATL for vulnerabilities in December 2012. This technical scan identified 1 critical and 28 high vulnerabilities on the three servers. (See table 3 for details.)





**Table 3. Total Number of High and Critical Vulnerabilities and Instances by CVEs and Vulnerability Name**

<b>ICE Server Name</b>	<b>Total Number of CVEs</b>	<b>Total Number of Unique Vulnerabilities</b>	<b>Date of Last Vulnerability Scan Report to DHS</b>
Server 1	15	6	12/2012
Server 2	29	15	01/2012
Server 3	47	8	12/2012
Total:	91	29	

These vulnerabilities place ICE systems at risk of malicious code execution, buffer overflows, and unauthorized access.<sup>13</sup> Additionally, some of the identified vulnerabilities date back to 2009.

According to DHS 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 ICE staff, the critical vulnerability identified was resolved during our audit fieldwork. Additionally, ICE staff has informed us that they have taken steps to resolve the identified high vulnerabilities. For example, as of February 2013, only two high vulnerabilities had not been resolved.

Server vulnerabilities that are not mitigated place at risk the confidentiality, integrity, and availability of ICE data. These risks include allowing remote code execution on ICE's information systems.

<sup>13</sup> NIST defines a buffer overflow as a condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or insert specially crafted code that lets them gain control of the system.



### **ICE Servers Were Not Regularly Scanned for Vulnerabilities**

The HSI SAC Atlanta electronic surveillance system servers had not been scanned for vulnerabilities. Specifically, the ICE SOC does not perform vulnerability assessments on these servers, as they are not connected to the DHS OneNet. Although this 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.

Additionally, ICE officials had experienced difficulties performing vulnerability scans on the three other ICE servers at ATL. Specifically, vulnerability scans performed since February 2012 were not always completed. According to ICE staff this issue was resolved during our fieldwork.

According to the DHS 4300A 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.

ICE officials are actively working with CBP to resolve the identified vulnerability scanning problem. Additionally, ICE officials have also submitted a request to their SOC to remediate all critical and high SAC Atlanta and AAG server vulnerabilities identified in December 2012.

### **Management Controls**

ICE's implementation of management controls for systems operating at the SAC Atlanta and AAG facilities did not conform fully to DHS policies. Specifically, ICE had not completed the security authorization activities for the ICON system. Additionally, ICE had not updated its interconnection security agreement (ISA) with the DHS OneNet to include the OWPFS and ICON systems. Further, ICE had not accounted for each server at ATL as part of a FISMA-inventoried system.



### **Security Authorization of ICON**

ICE had not completed the security authorization activities for the ICON network infrastructure system. As we reported in March 2012, ICE officials are in the process of establishing a security authorization package for their network infrastructure.<sup>14</sup> ICON security assessment review activities began in November 2012 and the authorization to operate is expected to be issued in January 2013.

According to DHS 4300A Handbook:

Components shall authorize systems at Initial Operating Capability and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first.

Without performing security authorization activities, ICE officials cannot ensure that they are aware of the vulnerabilities and threats to the system. Additionally, appropriate information security controls might not be established for ICON.

### **Interconnection Security Agreements**

ICE had not updated its ISA with the DHS OneNet to include the OWFPS and ICON systems.

According to DHS Directive 4300A:

Components shall document all interconnections to the DHS OneNet with an ISA signed by the OneNet AO [Authorizing Official] and by each appropriate AO.

As we reported in March 2012, ICE officials are establishing security authorization packages for their workstations, file and print servers, and network infrastructure.<sup>15</sup> However, the ISAs had not been completed. An updated ISA will help ICE officials more effectively document the security protections that must operate on interconnected systems.

---

<sup>14</sup> *Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport – Sensitive Security Information*, OIG-12-45, March 2012.

<sup>15</sup> *Ibid.*



### **The HSI Server Is Not Part of the FISMA System Inventory**

ICE had not individually accounted for the server hosting HSI's communications analysis and surveillance system as part of a recognized system in the Department's FISMA inventory. According to ICE staff, ICE officials decided in 2006 that this server was part of the component network infrastructure and that separate security authorization activities were not necessary for this application. However, ICE now plans to include the HSI servers as part of the ICE Subpoena System, a FISMA-inventoried system.

According to DHS Directive 4300A:

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

### **Operational Controls**

Onsite implementation of operational controls that did not conform fully to DHS policies included escort procedures for its multiuse server room, inadequate temperature and humidity controls in ATL server rooms, and redundant data telecommunications.

### **Physical Security**

ICE's HSI server room at ATL houses several sensitive IT devices, including a wire-tapping system, a tactical communication system, the building closed-circuit television security system, a contractor-serviced office telephone system (e.g., Private Branch exchange), a U.S. State Department digital subscriber line, and two computer network switches that link various devices in the SAC Atlanta offices. However, ICE does not have procedures to restrict access to the room to authorized personnel.

According to DHS Directive 4300A:

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

According to ICE staff, HSI controls physical access to the server room by electronic entry through the facility security system. Access to the server room



is limited to 10 full-time employees. Additionally, HSI officials agreed with our concerns on the need for improved physical security controls. Unauthorized access to sensitive law enforcement information systems could cause disclosure, disruption, modification, or destruction of information and information systems that support agency operations and assets.

### Environmental Controls

ICE has three server rooms at ATL. According to our temperature and humidity measurements, all three server rooms did not meet DHS temperature and humidity standards. (See table 4 for details.)

**Table 4. ICE Server Rooms Humidity and Temperature**

Location	Humidity		Temperature	
	ICE	OIG	ICE	OIG
SAC Atlanta HSI Computer Room	25%	31.3%	70	75.5
AAG – Main Computer Room	N/A <sup>16</sup>	31.3%	73	75.4
SAC Atlanta Computer Room	41%	13%	71	77

According to the DHS 4300A Handbook:

The following should be considered when developing a strategy for temperature and humidity control:

- 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.

According to ICE staff, the temperature in the HSI server room can be high as 90 degrees in the summer. Additionally, according to ICE staff, this server room includes more IT equipment from other entities than was originally intended. ICE is in negotiations with the facility landlord to make improvements.

Additionally, one server room did not have a smoke detector. Further, a server room was being used for storage of non-IT assets. However, during our review fieldwork, ICE removed the excess storage from this location. (See figures 3a and 3b for details.)

<sup>16</sup> We could not confirm the AAG computer room sensor humidity reading as we did not have access to the device.



**Figures 3a and 3b. Before and After Pictures of Storage in Room With ICE IT Equipment**

According to the DHS 4300A Handbook:

In addition to the physical security controls...facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:

- Housekeeping protection from dirt and dust
- Combustible cleaning supplies protection (not to be kept in computer areas).

ICE officials agree that non-IT assets should not be stored in rooms with IT assets and have agreed to clean the rooms.

### **Redundant Data Telecommunications Services**

ICE had not established redundant telecommunications services at its SAC Atlanta facility. Specifically, only one data telecommunications line services the SAC Atlanta server rooms and approximately 200 users at the facility. As a result, performance of mission-critical activities at this location is vulnerable to disruptions in the event of a data telecommunications line failure.



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

---

According to DHS 4300A Handbook *Attachment M, Tailoring the NIST SP 800-53 Security Controls*:

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.

**Recommendations**

We recommend that the ICE CIO:

**Recommendation #7:**

Provide ISSOs with real-time security alerts and the capability to review audit logs.

**Recommendation #8:**

Resolve high system vulnerabilities in a timely fashion.

**Recommendation #9:**

Scan all ICE servers at the SAC Atlanta and AAG sites annually.

**Recommendation #10:**

Complete security authorization activities for the ICON system.

**Recommendation #11:**

Update the ICE ISA with the DHS OneNet to include the OWFPS and ICON systems.

**Recommendation #12:**

Complete activities to include the HSI communications analysis and surveillance system server as part of a recognized FISMA-inventoried system.



**Recommendation #13:**

Obtain smoke detectors for the server rooms at ATL, and also maintain the server rooms within the temperature and humidity ranges established by the DHS 4300A Handbook.

**Recommendation #14:**

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

**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 at appendix B. DHS concurred with recommendations 7 through 14. Additionally, ICE has already taken actions to resolve reported deficiencies. Recommendations 7 through 14 are considered resolved, but open pending verification of all planned actions.

**Recommendation #7:**

ICE concurs and will provide ISSOs with the capability to review audit logs. Specifically, ICE's Information Assurance Division is working with the ICE NOC to implement this capability.

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

**Recommendation #8:**

ICE concurs and has published the Plan of Action and Milestone Management Process, which describes the steps taken by an ISSO to proactively monitor and manage the remediation of system vulnerabilities. In addition, ICE OCIO is in the process of developing an Enterprise Level Configuration Management Plan that will address resolution of high system vulnerabilities.

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





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

---

**Recommendation #9:**

ICE concurs and will scan their servers prior to the end of the fiscal year. In addition, information about the vulnerability scans for the SAC Atlanta and AAG will be addressed in ICE's Vulnerability Assessment Test Program. The estimated completion date for this recommendation is September 30, 2013.

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

**Recommendation #10:**

ICE concurs and will initiate the security controls assessment for ICON in May 2013 in order to obtain an Authority to Operate. ICE's actions satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until ICE provides documentation to support that the planned corrective actions are completed.

**Recommendation #11:**

ICE concurs and has agreed to update the ICE ISA with the DHS OneNet once the Authorization to Operate for ICON is in place. The estimated completion date for this recommendation is September 30, 2013.

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

**Recommendation #12:**

ICE concurs and will complete activities to include the HSI communications analysis and surveillance system server as part of the ICE Subpoena System Security Authorization package.

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



**Recommendation #13:**

ICE concurs and will obtain and install smoke detectors for the server rooms at ATL, as well as maintain the server rooms within the temperature and humidity ranges established by the DHS 4300A Handbook.

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

**Recommendation #14:**

ICE concurs and will conduct an internal assessment of current telecommunications and data systems to determine if a redundant system is necessary and cost-effective for this facility.

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

**TSA Did Not Comply Fully With DHS Sensitive System Policies**

TSA did not comply fully with DHS technical, management, and operational policies for its servers, routers, and switches operating at ATL. For example, three TSA ISSOs were not receiving real-time security alerts and were not reviewing audit logs on a weekly basis. TSA also had not implemented software patches for high vulnerabilities and was not regularly scanning all its servers at ATL. Additionally, TSA had not updated security documentation to include business impact assessments (BIAs) for the IT systems operating at ATL.

TSA's FAMS server room did not have a smoke detector and contained excess storage. Further, TSA did not have redundant data telecommunications lines providing service to its ATL facilities. Collectively, these deficiencies place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by TSA at ATL.

**Technical Controls**

TSA's implementation of technical controls for systems operating at ATL did not conform fully to DHS policies. For example, three TSA ISSOs were not reviewing audit logs on a weekly basis and were not receiving real-time alerts.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Additionally, identified vulnerabilities on TSA servers had not been resolved in a timely fashion. Further, not all TSA servers at ATL were being regularly scanned for vulnerabilities.

#### **Audit Logs and Real-Time Alerts**

The FAMSNet ISSO reviews audit logs on a weekly basis and receives real-time security alerts.<sup>17</sup> However, TSA ISSOs for the TSANet, ICS, and STIP were not receiving real-time security alerts. In addition, these ISSOs were not performing weekly monitoring of system audit logs.

According to TSA staff, the SOC is responsible for monitoring the audit logs. Incidents are reported to the ISSOs when the incident is escalated from the SOC. Additionally, the audit logs are sent to a platform to which the TSANet ISSO does not have remote access.

According to the DHS 4300A Handbook, ISSOs should—

Review audit records at least weekly, or in accordance with the SP [Security Plan].

Additionally, according to the DHS 4300A Handbook:

The DHS ISVM Program, managed through the SOC, provides Component CISOs/ISSMs and operational support personnel (e.g., ISSOs, System Administrators) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats.

Access to real-time alerts would provide the TSA ISSOs with early warning advisories on security attacks, along with information on the most recent viruses.

---

<sup>17</sup> According to the FAMSNet ISSO, the real-time alerts are limited to “all or nothing” alerting, and a more scalable solution providing specific alerts based on criticality would be more efficient and useful.



**Patch Management**

We scanned TSA FAMS' two servers at ATL for vulnerabilities in December 2012. This technical scan identified a high vulnerability on one of the servers. (See table 5 for details.)

**Table 5. Total Number of High Vulnerabilities and Instances by CVEs and Vulnerability Name**

<b>TSA FAMS Server Name</b>	<b>Total Number of CVEs</b>	<b>Total Number of Unique Vulnerabilities</b>	<b>Date of Last Vulnerability Scan Report to DHS</b>
Server 1	1	1	Not reported.

According to DHS Directive 4300A:

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

In February 2013, TSA FAMS staff informed us that the identified high vulnerability has been partially resolved, and will be completely resolved shortly.

**Vulnerability Scans**

STIP devices at ATL include servers that are used to facilitate image transfer to remote viewing stations. These STIP servers are not connected to TSANet and have not been scanned for vulnerabilities.

According to TSA staff, the first scan for STIP devices is tentatively scheduled for May 2013. These scans will provide a baseline after their initial hardening.<sup>18</sup> Any findings will be tracked and checked during integration testing, tentatively scheduled for July 2013. All findings must be adjudicated before placing the machines onto the TSANet.

<sup>18</sup> According to the DHS 4300 Handbook, "The DHS CISO has published secure baseline configuration guides for several operating systems, the Oracle 9i database management system, and CISCO routers, and will provide additional configuration guides as required. Hardening guides provide system and database administrators with a clear, concise set of procedures that shall ensure a minimum baseline of security in the installation and configuration of the hardware and software."



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

According to the DHS 4300A 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.

#### **Management Controls**

TSA's implementation of management controls for systems operating at ATL did not conform fully to DHS policies. Specifically, TSA had not completed BIAs for these systems, in that only TSANet contains a BIA in its Continuity Plan.

According to DHS 4300A Handbook:

The Business Impact Assessment (BIA) is essential in the identification of critical DHS assets.

The BIA helps to identify and prioritize critical IT systems and components. BIAs are also essential for contingency planning. For example, a BIA would allow TSA to identify maximum tolerable downtime, the resources required to resume mission/business processes, and recovery priorities for system resources. Without performing a BIA, TSA cannot ensure that its backup and recovery plans meet the needs of the business owners (e.g., recovery time objective and recovery point objective).

#### **Operational Controls**

Onsite implementation of operational controls that did not conform fully to DHS policies included excess storage, inadequate temperature and humidity controls, and the need for a smoke detector in the TSA server room at ATL. Additionally, TSA's IT assets at ATL do not have redundant data telecommunications.

#### **Environmental Controls**

TSA's FAMS server room at ATL did not have a smoke detector. Additionally, there was excess storage in this room. However, after our fieldwork, TSA took actions to clean up the server room. (See figures 4a and 4b for details.)



**Figures 4a and 4b. TSA FAMS Server Room**

According to the DHS 4300A Handbook:

In addition to the physical security controls...facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:

- Housekeeping protection from dirt and dust
- Combustible cleaning supplies protection (not to be kept in computer areas)

### **Redundant Data Telecommunications Services**

TSA has not established redundant telecommunications services at the terminals at ATL. Specifically only one data telecommunications circuit services TSA users at the North, South, and International Terminals. As a result, performance of mission activities at these locations is vulnerable to disruptions in the event of a data telecommunications circuit failure.

According to DHS 4300A Handbook *Attachment M, Tailoring the NIST SP 800-53 Security Controls*:

**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.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

According to TSA staff, adequate redundancy at ATL includes alternate means to access email and a separate voice circuit for their phones. Additionally, their continuity of operations plans contain detailed information on the continuity of mission-essential functions in the event that normal operations are severely disrupted.

### **Recommendations**

We recommend that the TSA CIO:

#### **Recommendation #15:**

Provide ISSOs with real-time security alerts and the capability to review audit logs.

#### **Recommendation #16:**

Continue efforts to resolve the identified high system vulnerability according to its associated plans of actions and milestones.

#### **Recommendation #17:**

Scan all TSA servers annually.

#### **Recommendation #18:**

Prepare the BIAs for the identified TSA systems operating at ATL.

#### **Recommendation #19:**

Obtain a smoke detector for the FAMS server room at ATL.

#### **Recommendation #20:**

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

### **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 at appendix B. DHS concurred with



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

recommendations 15 through 20. Additionally, TSA has already taken actions to resolve reported deficiencies. Recommendations 15 through 19 are considered resolved, but open pending verification of all planned actions. Further, TSA has provided documentation to support the resolution and closure of recommendation 20.

#### **Recommendation #15:**

TSA concurs with this recommendation. According to TSA (1) their SOC receives system log entries, all of which are correlated into audit logs of system events; (2) the SOC acts as an agent for the ISSOs to perform this function; and (3) all TSA ISSOs have full access to the SOC to observe system events in real time. Further, TSA ISSOs have the capability to perform historical queries on their systems. TSA requested OIG closure of recommendation 15.

However, during audit fieldwork, TSA ISSOs for the TSANet, ICS, and STIP were not receiving real-time security alerts. In addition, these ISSOs were not performing weekly monitoring of system audit logs as they did not have access to the ATL LAN audit logs. This recommendation is considered resolved, but will remain open until TSA provides documentation that the ISSOs are receiving real-time security alerts and have the audit log access required.

#### **Recommendation #16:**

TSA concurs with this recommendation. According to TSA, the one vulnerability noted required two steps to remediate and both steps were completed as of April 10, 2013. TSA requested that OIG close recommendation 16.

TSA provided documentation supporting that corrective actions had been taken for step 1 of this recommendation. However, TSA has not provided adequate supporting documentation to allow us to verify that step 2 was completed.

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

#### **Recommendation #17:**

TSA concurs and will include scanning of TSA multiplexed servers as part of the scheduled Technical Vulnerability Audits conducted at airports annually. The





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

---

Technical Vulnerability Audits will begin June 2013 and continue on a scheduled basis.

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

**Recommendation #18:**

TSA concurs and will prepare BIAs for the identified systems operating at ATL. Additionally, BIA templates have been distributed to system owners and ISSOs. The estimated completion date for this recommendation is April 30, 2014.

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

**Recommendation #19:**

TSA concurs and has implemented environmental monitoring for temperature and humidity thresholds for the FAMS server room. However, according to TSA, adding smoke detectors will require additional research and coordination to determine the impact on the office lease, funding sources, and local building and fire codes. TSA will begin work with facilities management immediately, and the completion date will be contingent upon the complexity of implementation.

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

**Recommendation #20:**

TSA concurs with this recommendation. In response to it, TSA performed an analysis to determine whether it is necessary and cost-effective to establish redundant data telecommunications services at TSA's ATL terminal location. TSA has determined that it would not be cost-effective to implement the redundancies. TSA requested that OIG close recommendation 20.

TSA's actions satisfy the intent of this recommendation. This recommendation is considered resolved and closed.



## **Appendix A**

### **Objectives, Scope, and Methodology**

The Department of Homeland Security (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 review is part of an ongoing program to evaluate 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 Directive 4300A and its companion document, the DHS 4300A Handbook. Our primary focus was on evaluating the security controls over the servers, routers, switches, and telecommunications circuits of the DHS IT infrastructure at this site.

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

We reviewed documentation contained in the Trusted Agent-FISMA system to ensure that it is current. We reviewed documentation such as the authority-to-operate letter, contingency plans, and BIAs. 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 component 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.<sup>19</sup>

We conducted this performance audit between September 2012 and February 2013 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.

---

<sup>19</sup> During our audit fieldwork, we identified additional data telecommunications lines. We are still working with CBP and ICE to determine whether these lines are still necessary.



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

---

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 Frank Deffer, 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 C.



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

Appendix B  
Management Comments to the Draft Report

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



May 16, 2013

MEMORANDUM FOR: Frank Deffer  
Assistant Inspector General  
Office of Inspector General

FROM: *Christopher T. Brothers*  
Christopher T. Brothers  
Assistant Director  
Departmental GAO-OIG Liaison Office

SUBJECT: Technical Security Evaluation of DHS Activities at Hartsfield-Jackson Atlanta International Airport (OIG Project No. 12-031-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 to note OIG's positive acknowledgement that U.S. Customs and Border Protection (CBP) has made improvements and upgrades at Hartsfield-Jackson Atlanta International Airport (ATL) to reduce network outages. CBP will continue to work toward improving areas of technical security in the CBP information technology (IT) infrastructure. U.S. Immigration and Customs Enforcement (ICE) and Transportation Security Administration (TSA) are also committed to strengthening technical controls to address the weaknesses identified in the report, and have already begun developing plans of actions and milestones to facilitate timely closure of recommendations.

The draft report contained 20 recommendations with which the Department concurs. Of these, the Department is requesting closure of four recommendations.

Specifically, OIG recommended that the CBP Chief Information Officer (CIO):

**Recommendation 1:** Provide ISSOs with real-time security alerts and the capability to review audit logs.

**Response:** Concur. CBP Office of Information Technology (OIT) will provide Information System Security Officers (ISSOs) with access to the appropriate logs regarding network changes such as router and switch configuration updates as well as user access information. The DHS security team is developing a Standard Operating Procedure for reviewing logs weekly. Estimated Completion Date (ECD): June 30, 2013.



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

---

**Recommendation 2:** Resolve high system vulnerabilities in a timely fashion.

**Response:** Concur. CBP OIT will continue to patch system vulnerabilities in a timely manner and will make sure that the outstanding patches are implemented.  
ECD: June 30, 2013.

**Recommendation 3:** Update the DHS OneNet Security Plan to document the risks associated with the use of out-of-band modems attached to DHS OneNet routers.

**Response:** Concur. The DHS OneNet Security Plan has been updated to include the use of out-of-band modems. The Plan will be further updated to document the risks associated with the use of out-of-band modems attached to DHS OneNet routers. ECD: July 31, 2013.

**Recommendation 4:** Obtain temperature and humidity sensors for the ATL server rooms, and maintain them within the temperature and humidity ranges established by the DHS 4300A Handbook.

**Response:** Concur. The Port of Atlanta procured a device which measures humidity and will call up to four telephone numbers if it detects data outside of the set parameters. It was installed and tested in the Phoenix Parkway location during the week of April 22, 2013. Funding permitted and with no additional restrictions on procurement, the Port of Atlanta plans to complete installation of the device in all server rooms. ECD: August 30, 2013.

**Recommendation 5:** Maintain ATL server and network rooms free of excess storage and hazardous items that may cause damage to the system.

**Response:** Concur. CBP OIT and CBP Office of Field Operations (OFO) removed excess storage and hazardous items from each of the Port of Atlanta's server and network rooms (completed March 26, 2013). Pictures of the cleaned rooms have been sent to the OIG. On April 1, 2013, the CBP OFO ATL began inspecting the rooms for clutter and hazardous items and will continue doing so on a monthly basis. A checklist is being used to document the inspections. Network rooms maintained by others are also being checked periodically. ECD: Complete.

CBP requests OIG closure of recommendation 5.

**Recommendation 6:** Assign the responsibility to review DHCP server automatic messages and ATL LAN audit logs.

**Response:** Concur. CBP OIT will research, clarify, monitor, and enforce responsibilities for the review of the Dynamic Host Configuration Protocol (DHCP) server automatic messages and ATL LAN (Local Area Network) audit logs. ECD: June 30, 2013.

OIG recommended that the ICE Chief Information Officer (CIO):

**Recommendation 7:** Provide ISSOs with real-time security alerts and the capability to review audit logs.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

**Response:** Concur. The ICE Network Operations Center (NOC) is monitoring the ICE Communication Over Networks (ICON) devices on a constant basis. If a security risk or incident is found, the NOC will notify the ICE Secure Operations Center (SOC). ICE will provide ISSOs with the capability to review audit logs. ICE (Information Assurance Division) IAD is working with the NOC to implement this capability. ECD: To Be Determined (TBD).

**Recommendation 8:** Resolve high system vulnerabilities in a timely fashion.

**Response:** Concur. In April 2013, ICE Office of the Chief Information Officer (OCIO) published the Plan of Action and Milestone management process. This process describes the steps taken by an ISSO to proactively monitor and manage the remediation of system vulnerabilities. In addition, ICE OCIO is in the process of developing an Enterprise Level Configuration Management Plan that includes Patch Management that will address timely management of resolution of high system vulnerabilities. ECD: June 30, 2013.

**Recommendation 9:** Scan all ICE servers at the SAC Atlanta and AAG sites annually.

**Response:** Concur. Vulnerability scans for the Special Agent in Charge (SAC) Atlanta and Atlanta Airport Group (AAG) are covered in the ICE Security Operations Center Vulnerability Assessment Test (VAT) Program and will be scanned prior to the end of the fiscal year. ECD: September 30, 2013.

**Recommendation 10:** Complete security authorization activities for the ICON system.

**Response:** Concur. ICE OCIO will initiate the security controls assessment for ICON in May 2013 in order to obtain an Authority to Operate (ATO). ECD: August 30, 2013.

**Recommendation 11:** Update the ICE ISA with the DHS OneNet to include the OWFPS and ICON systems.

**Response:** Concur. ICE will update the ICE Interconnection Security Agreement (ISA) with the DHS OneNet to include the OCIO Workstations with File and Print Servers (OWFPS) and ICON systems once the ATO for ICON is in place. ECD: September 30, 2013.

**Recommendation 12:** Complete activities to include the HSI communications analysis and surveillance system server as part of a recognized FISMA-inventoried system.

**Response:** Concur. ICE OCIO in coordination with ICE Homeland Security Investigation (HSI) will complete activities to include the HSI communications analysis and surveillance system server as part of the ICE Subpoena System (ISS) Security Authorization package, a recognized Federal Information Security Management Act (FISMA)-inventoried system. ECD: May 31, 2013.

**Recommendation 13:** Obtain smoke detectors for the server rooms at ATL, and also maintain the server rooms within the temperature and humidity ranges established by the DHS 4300A Handbook.



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

---

**Response:** Concur. ICE OCIO in coordination with ICE HSI will obtain and install smoke detectors for the server rooms at ATL, as well as, maintain the server rooms within the temperature and humidity ranges established by the DHS 4300A Handbook. ECD: June 30, 2013.

**Recommendation 14:** Determine whether it is necessary and cost-effective to establish redundant data telecommunications services at the SAC Atlanta facility.

**Response:** Concur. SAC Atlanta will conduct an internal assessment of current telecommunications and data systems to determine if a redundant system is necessary and cost-effective for this facility. ECD: June 28, 2013.

OIG recommended that the TSA Chief Information Officer (CIO):

**Recommendation 15:** Provide ISSOs with real-time security alerts and the capability to review audit logs.

**Response:** Concur. TSA has made significant investments in a state-of-the-art Security Operations Center (SOC). The SOC receives system log entries all of which are correlated into audit logs of system events. The SOC acts as an agent for the ISSOs to perform this function. All TSA ISSO's have full access to the SOC to observe system events in real time. In addition, ISSO's have the capability to perform historical queries on the systems they are interested in. ECD: Complete.

TSA requests OIG closure of recommendation 15.

**Recommendation 16:** Resolve high system vulnerabilities according to their associated plans of actions and milestones.

**Response:** Concur. The one vulnerability noted had already been identified by TSA and partially addressed at the time of the OIG testing on December 12, 2012. The particular vulnerability required two steps to remediate; step-1 was completed prior to the OIG testing, and step-2 was completed on April 10, 2013. TSA provided to OIG during the active audit phase and the period after, documents detailing the Office of Information Technology/Federal Air Marshal Service Information Technology Division active system monitoring and compliance. ECD: Complete.

TSA requests OIG closure of recommendation 16.

**Recommendation 17:** Scan all TSA servers annually.

**Response:** Concur. TSA IAD will include scanning of TSA multiplexed (MUX) servers as part of the scheduled Technical Vulnerability Audits conducted at airports annually. TSA MUX Servers are the servers that act as hub devices connecting various Transportation Security Equipment (TSE) in an Airport Environment. The Technical Vulnerability Audits will begin June 2013 and continue on a scheduled basis. ECD: June 30, 2013.

**Recommendation 18:** Prepare the BIAs for the identified TSA systems operating at ATL.



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

---

**Response:** Concur. TSA will prepare business impact assessments (BIAs) for the identified systems operating at ATL. BIA templates have been distributed to System Owners and ISSOs. ECD: April 30, 2014.

**Recommendation 19:** Obtain a smoke detector for the FAMS server room at ATL.

**Response:** Concur. Environmental monitoring for temperature and humidity thresholds is established for the FAMS server room. However, adding smoke detectors will require additional research and coordination to determine the impact on the office lease, funding sources, and local building and fire codes. TSA will begin work with Facilities Management immediately. The completion date will be contingent upon the complexity of implementation. ECD: TBD.

**Recommendation 20:** Determine whether it is necessary and cost-effective to establish redundant data telecommunications services at TSA's ATL terminal locations.

**Response:** Concur. TSA performed an analysis to determine whether it is necessary and cost-effective to establish redundant data telecommunications services at TSA's ATL terminal location. TSA determined it would not be cost effective to implement the redundancies. In the event of an unforeseen network interruption, TSA will continue to provide screening services without any impact to the mission due to the following redundant telecommunication services that are in place at ATL:

- The Blackberry service is on a separate network that provides email services if TSANet at ATL is not operational.
- Users can access their email via TSA Outlook Web Access Portal.
- ATL has MiFi access for users to VPN to the network.
- Internal and external calls on the TSA VoIP phones would not be affected, since they are connected via separate voice Primary Rate Interface (PRI) circuits. Checkpoint and baggage screening operations would continue un-impacted. Additionally, on-going training, would not be impacted since training could continue in an offline manner.

ECD: Complete.

TSA requests OIG closure of recommendation 20.

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitivity comments have been sent under separate cover. We look forward to working with you in the future.





## **Appendix C**

### **Major Contributors to This Report**

Sharon Huiswoud, Director  
Kevin Burke, Supervisory Auditor  
Matthew Worner, Senior Auditor  
Charles Twitty, Senior Auditor  
Pamela Chambliss-Williams, Senior Program Analyst  
Steven Tseng, IT Specialist  
Philip Greene, Referencer



## **Appendix D**

### **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  
Acting 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 obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov).

For additional information, visit our website at: [www.oig.dhs.gov](http://www.oig.dhs.gov), or follow us on Twitter at: [@dhsoig](https://twitter.com/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](http://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: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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