Department of Homeland Security
Office of Inspector General

DHS' Progress in Addressing Technical Security Challenges at Washington Dulles International Airport (Redacted)

Notice: The Department of Homeland Security, Office of the Inspector General has redacted this report for public release. A review under the Freedom of Information Act (5 U.S.C. 552), will be conducted upon request.

OIG-09-66

May 2009

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

May 7, 2009

Preface

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 report addresses DHS' progress in strengthening technical and information security policies and procedures at Washington Dulles International Airport in Virginia. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
DHS 4300A Handbook	DHS Sensitive Systems Handbook
DHS Directive 4300A	DHS Sensitive Systems Policy Directive 4300A
IAD	Washington Dulles International Airport
IT	Information Technology
LAN	Local Area Network
OIG	Office of Inspector General
POA&M	Plan of Action and Milestones
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TSA	Transportation Security Administration
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply

Executive Summary

We initiated a program to determine the extent to which critical Department of Homeland Security sites comply with the department's technical and information security policies and procedures. In January 2007, we reported that information technology security controls implemented by U.S. Customs and Border Protection and the Transportation Security Administration at Washington Dulles International Airport had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the automated systems used to perform their mission-critical activities. We also identified actions that these components could take to improve information technology security.

We conducted a follow-up evaluation to determine whether corrective actions for the reported weaknesses had been implemented, and whether those actions comply with the department's and components' technical and information security policies and procedures. We performed onsite verification of the corrective actions, interviewed department staff, and conducted technical tests of internal controls.

The department has made significant progress in improving technical security for information technology assets at Dulles. However, further work is needed to comply with government policies and procedures. For example, both components need to make additional improvements in their operational controls over the physical security of their information technology. We are also recommending improvements in technical controls, including updating servers with the latest release of the operating system software. Implementation of these additional measures will increase the technical security of departmental information technology assets at Dulles.

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* (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 outlines policies relating to the operational, technical, and management controls that are necessary for ensuring confidentiality, integrity, availability, authenticity, and no repudiation within the DHS IT infrastructure and operations. A companion document—*DHS 4300A Sensitive Systems Handbook* (DHS 4300A Handbook)—provides detailed guidance on the implementation of these policies.

DHS IT security policies are organized under management, operational, and technical 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. These controls require technical or specialized expertise and often rely on management and technical controls.

****

- **Technical Controls** – Focus on security controls executed by IT 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 IT security system and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.

U.S. Customs and Border Protection (CBP) and the Transportation Security Administration (TSA) each have activities at Washington Dulles International Airport (IAD), a port of entry located in Chantilly, VA. Both CBP and TSA rely on a range of IT assets to support their respective missions.

CBP processes passengers and baggage on arriving international flights at IAD by using information systems that include United States Visitor and Immigrant Status Indicator Technology, Automated Biometric Identification Systems, Custom Modernization Prime Integration, and other secondary systems. The CBP activities at IAD are conducted at the Main Terminal-International Arrivals, C Terminal/Midfield, B Terminal, Cargo Inspections, and two private terminals.

TSA also has operations at various buildings at IAD, including the main terminal and a commercial office building. TSA activities include screening passengers and baggage on all departing flights at IAD.

In January 2007, we reported that the IT security controls implemented by CBP and TSA at IAD had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the IT systems on which CBP and TSA rely to perform their mission-critical activities.[1] Specifically, we reported that CBP and TSA needed to improve operational, technical, and management controls for their IT assets at IAD. Based on these findings, we recommended that the DHS Chief Information Security Officer instruct CBP and TSA to:

- Strengthen operational controls at CBP and TSA facilities at IAD.
- Apply necessary software upgrades in a timely and expeditious manner.
- Prepare the necessary plan of action and milestones (POA&M) to resolve known and reported deficiencies in IT Security.
- Ensure that all systems, wireless communications, and group users' ID are appropriately authorized to operate.

The objective of this evaluation was to determine whether corrective actions for the reported weaknesses had been implemented, and whether those actions comply with the department's and components' technical and information security policies and procedures.

[1] *Technical Security Evaluation of DHS Activities at Dulles International Airport*, OIG-07-25, January 2007.

Results of Review

CBP's IT Security Controls Improve, But More Work Is Needed

CBP's IT security controls have improved at IAD, but more work is needed to comply with DHS policies and procedures. Specifically, CBP improved its operational, technical, and management controls for IT equipment. For example, CBP implemented adequate POA&Ms to effectively address previously reported IT deficiencies at IAD. Additionally, group user accounts were disabled and all CBP systems were authorized to operate. Further, CBP disabled inactive physical ports on its routers and switches at IAD.

However, more work is needed to address physical and environmental control deficiencies. CBP also needs to implement technical controls to ensure that it is using the most current version of operating systems. Further, CBP should ensure that system documentation includes information concerning vulnerabilities and accepted risks.

Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at IAD.

Operational Controls

CBP improved operational controls to comply with DHS policies. Specifically, CBP implemented temperature and humidity sensors, added a second telecommunications circuit for path redundancy, and disabled unused physical ports on the routers and switches at IAD. However, CBP needs to do more to address operational control deficiencies. For example, physical security control improvements are needed to prevent unauthorized access to telecommunications equipment. CBP also needs to improve business continuity capabilities for times when power or telecommunications outages affect IAD.

Physical Security Controls

CBP needs to improve physical security controls to prevent unauthorized access to IT resources. For example, CBP has telecommunications equipment in a room shared with non-DHS tenants. While this room is locked, it is not under the control of CBP officials, non-CBP staff has access keys, and the CBP telecommunications equipment is not in a locked cabinet.

CBP telecommunications equipment in a waiting room is not properly secured in a locked cabinet. This room is used by international passengers waiting for CBP personnel to process them for entry into the country. See figure 1.

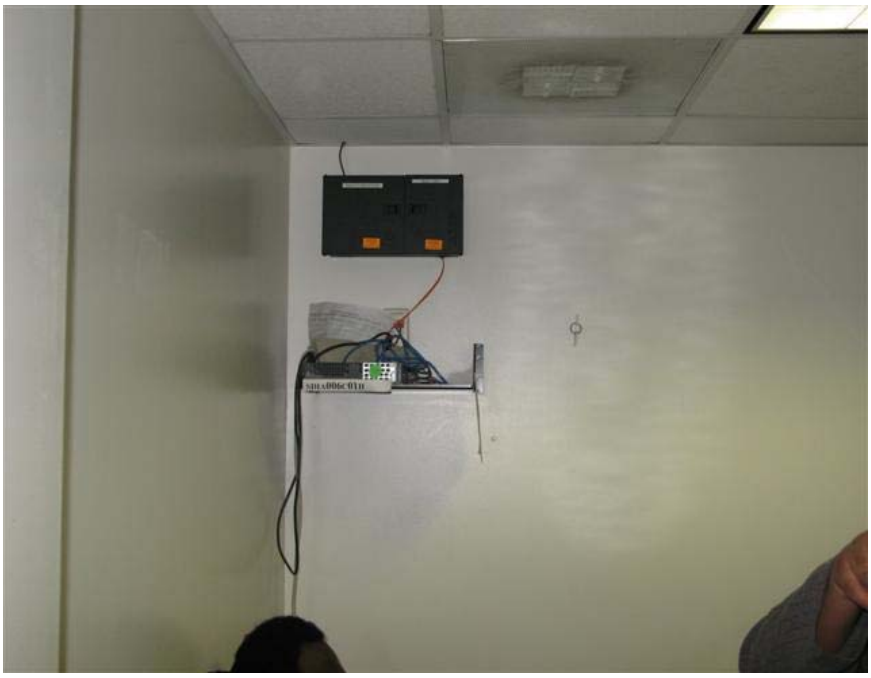


Figure 1: Unsecured CBP telecommunications equipment on a wall in an international passenger waiting room.

[redacted].

Further, CBP is not using the visitors' sign-in logs that are now installed in all of its local area network (LAN) and telecommunications rooms.

According to the DHS 4300A Handbook:

> "Access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data shall be limited to authorized personnel."
>
> "Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and will be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions and natural disasters."
>
> "Visitors log should be maintained and available for one year."

Business Continuity Capability

CBP has taken steps to ensure continued passenger processing during communications or power outages. For example, CBP improved its business continuity capability by installing new telecommunications lines and circuits at IAD. Specifically, two circuits were installed, each with a different end point and each from a different vendor. Routers at the two end-point locations will be load-balanced and will provide redundancy for each other. These actions are in response to our January 2007 report concerning the lack of data communication redundancy.

CBP also has allocated funding to critical border sites to purchase computers for emergency conditions. The IAD allocation allowed for the purchase of 17 computers that can be used to process passengers during a power failure or if the telecommunications connection to the CBP data center is not available. In April 2008, CBP staff cited the emergency computers as a compensating control in an exception request for accepting the risk associated with a cutoff of telecommunications services at IAD.[2]

However, CBP currently has 65 Primary Passenger Processing Lanes at IAD for 100% passenger-processing capacity. Going from 65 lanes for processing passengers to 17 lanes with emergency computers would reduce CBP's passenger-processing capability by 74%.

[2] The CBP information systems security manager has not approved any of the exception or waiver requests for IAD that are cited in this report.

Additionally, CBP has not completed all corrective actions to comply with DHS policies and procedures. For example, each [redacted] (see Appendix D). In April 2008, CBP staff prepared a 6-month waiver request to accept this risk while CBP installed the equipment to resolve this deficiency.

Further, CBP has not developed plans to resolve all reported deficiencies. For example, CBP does not have a backup power supply for any of its buildings at IAD. Although CBP has installed uninterruptible power supply (UPS) devices for all of its servers, routers, and switches at IAD, these devices provide power only for a limited period. UPS devices are not sufficient for the purpose of operating CBP workstations following a power failure. However, according to CBP staff, a backup power supply is unnecessary as IAD receives power from two separate power substations.

CBP also does not have plans to remediate other operational control deficiencies at IAD. For example, in April 2008, CBP staff prepared policy exception requests accepting the risk [redacted]

According to the DHS 4300A Handbook:

> "DHS must have the capability to ensure continuity of essential function under all circumstances."
>
> "For larger and more critical systems it may be appropriate to have an electrical generator available for the most critical of operational requirements."

Environmental Controls

CBP does not regularly maintain and monitor the temperature and humidity levels within its LAN rooms and telecommunications closets at IAD. Specifically, many of CBP's telecommunications rooms had temperatures that exceeded 70 degrees Fahrenheit. Additionally, on our June 2008 walk-through, we observed some ad hoc ventilation methods in use, including floor fans and a portable air conditioning unit.

According to the DHS 4300A Handbook:

> "Temperature in computer storage areas should be held between 60 and 70 degrees Fahrenheit."

Inadequate heating, ventilation, and air conditioning capability in these telecommunications closets increases the risk of damage to CBP IT assets.

CBP purchased and installed several temperature and humidity sensors at IAD in response to our January 2007 report. CBP also provided information on plans to install IT cabinets that contain fans. In April 2008, CBP staff prepared an exception request accepting the risk associated with a lack of environmental monitoring.

Technical Controls

We determined that CBP has improved its technical controls for servers at IAD, but more work is needed to comply with DHS policies. For example, CBP disabled inactive physical ports on its routers and switches at IAD. However, CBP also needs to improve its technical controls by:

- [redacted]

Additionally, CBP Novell servers had open logical ports with known vulnerabilities that were not documented in the site risk assessment. Unnecessary open ports and services increase the risk that malicious users may compromise CBP systems or allow external attacks.

[redacted] CBP personnel told us that they recognize the vulnerabilities associated with these open ports and that they used the firewall as a compensating control to block the threats associated with these ports.[3] However, CBP has not documented the acceptance of this risk and the associated compensating controls in the site-specific security plans or risk assessments.

According to DHS Directive 4300A:

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

Management Controls

CBP resolved the management control deficiencies we reported in January 2007. We did not identify any additional management control deficiencies.

Recommendations

We recommend that the CBP Chief Information Officer (CIO) take the following actions for CBP activities at IAD:

Recommendation #1: Implement physical security and environmental controls to compensate for reported deficiencies.

Recommendation #2: Implement business continuity capabilities to compensate for reported deficiencies.

Recommendation #3: Implement and document technical controls and processes to compensate for reported deficiencies.

[3] CBP staff provided evidence that the firewalls block these ports. However, we did not independently test these firewalls.

Management Comments and OIG Analysis

CBP concurred with recommendations 1 through 3. These recommendations will be considered resolved but open pending verification of all planned actions.

TSA's IT Security Controls Improve, But More Work Is Needed

TSA's IT security controls have improved at IAD, but more work is needed to comply with DHS policies and procedures. Specifically, TSA improved its operational, technical, and management controls for IT equipment. For example, operational controls at IAD were strengthened with the installation of locked cabinets, camera surveillance, and card readers for doors. TSA also reinforced its technical security controls by updating the secure socket layer (SSL) certificate for its servers at IAD. Additionally, TSA strengthened management controls by streamlining the TSANet system POA&Ms. Further, TSA updated the TSANet system boundaries to include the Office of Emergency Preparedness' server at IAD.

However, more work is needed to address our previously reported deficiencies. Specifically, TSA needs to take steps to restrict access to IT equipment at IAD and to strengthen technical security controls.

Operational Controls

We reported previously that TSA had not provided sufficient physical security to prevent unauthorized access to TSA telecommunications closets and desktop computers at IAD. Since then, TSA has improved physical security controls by implementing the use of locked cabinets, camera surveillance, and entry/exit card readers. However, additional physical security controls are still needed in several areas at IAD. For example, TSA could strengthen controls to restrict access to its telecommunications closet and a workstation in a passenger screening area. Additionally, TSA should remove excess IT equipment and boxes in its IAD LAN room. See figure 2.

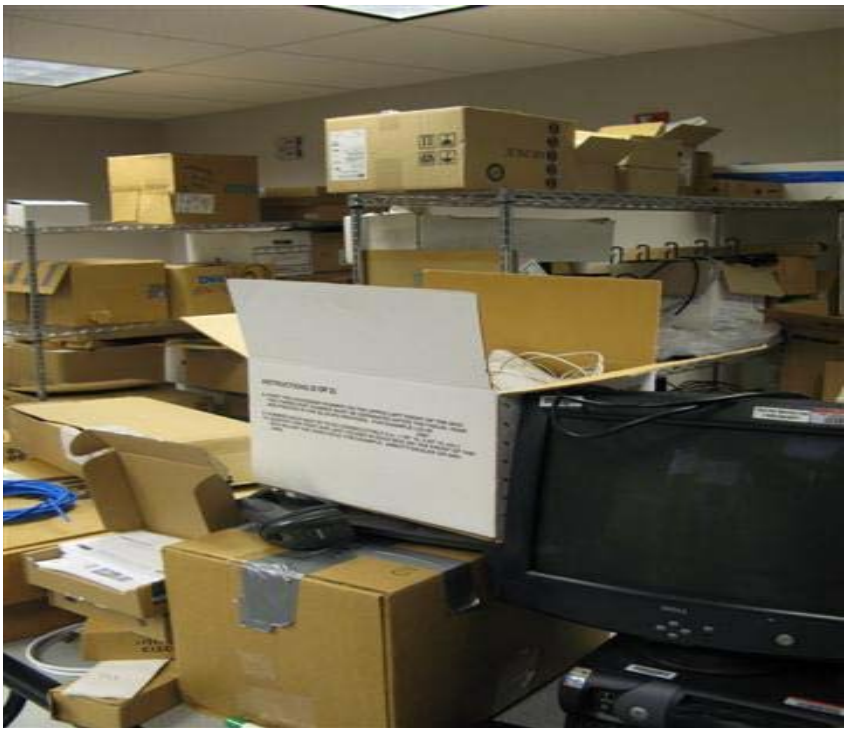


Figure 2: Excess equipment stored in LAN room.

TSA has moved some of the excess equipment and restacked or relocated boxes. Additionally, TSA has added a visitor log to the room. Further, TSA provided detailed plans, flooring diagrams, and pictures of a "cage structure" that TSA plans to purchase to protect its IT equipment from harm. However, actual construction of the cage has not started.

TSA telecommunications equipment located in a commercial office building basement at IAD was not properly secured in a locked cabinet [redacted] Access to this room and to TSA's telecommunications equipment should be controlled and limited.

Further, a workstation at IAD was not properly secured. (See figure 3.) This workstation was adjacent to a TSA passenger screening exit area, and its computer terminal connections were clearly visible and accessible to the public.

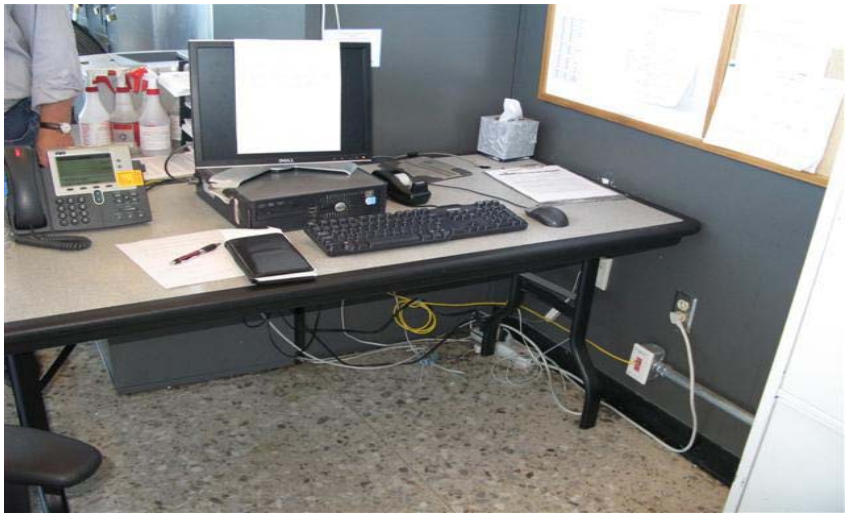


Figure 3: Unsecured workstation in TSA passenger screening area.

According to the DHS 4300A Handbook:

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

Technical Controls

TSA strengthened its technical controls at IAD, but additional work is needed. For example, TSA corrected three of the six technical control deficiencies that we reported in January 2007.

Unnecessary open ports and services increase the risk that malicious users may compromise TSA systems or allow external attacks. Additionally, operating systems that do not receive required updates or patches are vulnerable and can be easily exploited.

[redacted].

According to the DHS Directive 4300A:

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

Management Controls

TSA resolved the management control deficiencies we reported in January 2007. We did not identify any additional management control deficiencies.

Recommendations

We recommend that the TSA CIO take the following actions for TSA activities at IAD:

Recommendation #4: Implement physical security and environmental controls to compensate for reported deficiencies in TSA's LAN rooms, telecommunications closets, and airport passenger screening workstation desks.

Recommendation #5: Implement and document technical controls and processes to compensate for reported deficiencies.

Recommendation #6: Apply the necessary operating system updates to systems operating at IAD.

[4] TSA staff provided evidence that the firewalls block these ports. However, we did not independently test these firewalls.

Management Comments and OIG Analysis

TSA concurred with recommendations 4 through 6. These recommendations will be considered resolved but open pending verification of all planned actions.

As part of our program to evaluate, on an ongoing basis, the implementation of DHS technical and information security policies and procedures at DHS sites, we conducted a follow-up review of DHS' efforts to strengthen IT security controls at IAD. The objectives of this review were to determine whether:

- The DHS components had implemented action plans to correct the weaknesses we reported, and
- Those action plans complied 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 entrance and exit conferences were held with CBP and TSA officials. Follow-up technical evaluations were conducted. DHS components and OIG staff monitored security scans of the servers using various software packages. Additionally, OIG staff conducted scans to determine whether DHS components at IAD were using wireless devices.[5]

We reviewed applicable DHS and DHS component policies and procedures, previously reported deficiencies, and corrective action plans for the OIG reported weaknesses. Before performing our onsite review, we used the components' action plans and status updates to identify the applicable locations for the IT assets, the appropriate staff to interview, and where to conduct the technical test for internal controls. Our onsite review included a physical review of CBP and TSA space and interviews with the appropriate staff. Our technical review included onsite reviews of server security policies. Additionally, we reviewed guidance provided by DHS to the components regarding patch management, operation systems, and wireless security.

We provided both CBP and TSA with briefings concerning the results of fieldwork and the information summarized in this report. We conducted this review between June and October 2008.

We performed our work according to the *Quality Standards for Inspection* of the President's Council on Integrity and Efficiency and pursuant to the *Inspector General Act of 1978*, as amended.

We appreciate the efforts of DHS management and staff to provide the information and access necessary to accomplish this review.

[5] We did not find any wireless devices being used by CBP or TSA at IAD.

Our points of contact for this report are Frank Deffer, Assistant Inspector General for Information Technology, (202) 254-4100, and Sharon Huiswoud, Director for Information Systems (202) 254-5441. Major OIG contributors to the review are identified in Appendix E.

Appendix B
CBP's Management Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and Border Protection

April 30, 2009

MEMORANDUM FOR: DIRECTOR
DHS OIG/GAO AUDIT LIAISON

FROM: Acting Director
Office of Policy and Planning

SUBJECT: U.S. Customs and Border Protection's Comments on the Office of Inspector General Draft Report, "DHS' Progress in Addressing Technical Security Challenges at Washington Dulles International Airport"

Thank you for providing us with a copy of the draft report entitled "DHS' Progress in Addressing Technical Security Challenges at Washington Dulles International Airport." This report assess whether corrective actions for the reported weaknesses (OIG-07-25) had been implemented, and whether those actions comply with the department's and components' technical and information security policies and procedures.

The Office of Inspector General (OIG) concluded that the department has made significant progress in improving technical security for information technology assets. However, further work is needed to comply with government policies and procedures. The OIG is recommending that the Customs and Border Protection (CBP) Chief Information Officer (CIO) take the actions below for CBP activities at Washington Dulles International. CBP concurs with the three recommendations and is providing corrective actions for each.

Recommendation 1: Implement physical security and environmental controls to compensate for reported deficiencies.

Response: CBP concurs with this recommendation.

Due Date: FY 2011

Recommendation 2: Implement business continuity capabilities to compensate for reported deficiencies.

Response: CBP concurs with this recommendation.

Due Date: January 31, 2009

Recommendation 3: Implement and document technical controls and processes to

compensate for reported deficiencies.

Response: CBP concurs with this recommendation.

Due Date: June 30, 2009

CBP worked with the Transportation Security Administration SSI and Audit Liaison Offices on sensitivity determination. Because of sensitivities identified, CBP will provide responses and corrective actions for the recommendations under a separate cover.

If you have any questions, please contact Robin White, Audit Liaison, Office of Policy and Planning, at (202) 344-1061.

SENSITIVE SECURITY INFORMATION

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

JAN 1 5 2009

Transportation Security Administration

INFORMATION

MEMORANDUM FOR: Richard L. Skinner
Inspector General
Department of Homeland Security (DHS)

FROM: Kip Hawley
Assistant Secretary

SUBJECT: Transportation Security Administration's (TSA) Response to DHS's Office of Inspector General (OIG) Draft Report, *DHS' Progress in Addressing Technical Security Challenges at Washington Dulles International Airport*, December 2008

Purpose

This memorandum constitutes TSA's response to OIG's Draft Report, *DHS' Progress in Addressing Technical Security Challenges at Washington Dulles International Airport.* TSA appreciates OIG's effort on this evaluation and will use the findings and recommendations to continue to improve technical security at our Washington Dulles International (IAD) Airport operation.

Background

In January 2007, OIG reported that Customs and Border Protection (CBP) and TSA information technology (IT) security controls at IAD had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of CBP's and TSA's automated systems. Between June and October 2008, OIG conducted a follow-up evaluation of DHS activities at IAD to determine whether corrective actions for the reported weaknesses had been taken, and whether those actions comply with the Department's and components' technical and information security policies and procedures. OIG conducted onsite verification of the corrective actions, interviewed department staff, and conducted technical tests of internal controls.

OIG found that the department has made significant progress improving technical security for information technology assets. However, further work is needed to comply with government policies and procedures.

Discussion

The TSA Chief Information Office, through its Chief Information Security Officer in the IT Security Branch, works closely with other TSA programs such as, the Chief Administrative Office's Office of Real Estate, the Office of Security Physical Security Division, and Federal Security Director staff to ensure that local TSA offices and administrative space meet physical and environmental IT security requirements. The IT Security Branch and the Office of Security's Physical Security Division also use internal assessments to systematically verify that these requirements are being met and IT assets are protected.

TSA appreciates OIG's recognition of TSA's significant progress in improving technical security at IAD. Some examples of recent progress made by TSA include: installing an access control system on the door leading to the building telecommunications room restricting access to authorized individuals; and installing locks and cables to secure other IT equipment.

TSA continues to improve technical security controls at IAD, and these improvements are reflected in our attached response to OIG's recommendations.

SENSITIVE SECURITY INFORMATION

Transportation Security Administration (TSA) Response
Department of Homeland Security (DHS) Office of Inspector General (OIG)
Draft Report:
***DHS' Progress in Addressing Technical Security Challenges at Washington Dulles International Airport,* December 2008**

DHS OIG recommends that the TSA Chief Information Office (CIO) take the following actions for TSA activities at Washington Dulles International (IAD) Airport:

Recommendation 4: Implement physical security and environmental controls to compensate for reported deficiencies in TSA's LAN rooms, telecommunications closets, and airport passenger screening workstation desks.

TSA Concurs. TSA concurs with OIG's recommendation and continues to make progress improving physical and environmental controls for information technology (IT) assets at IAD. For example, OIG noted at the time of its evaluation that TSA telecommunications equipment was not properly secured. TSA has since coordinated with the building management company to add a lock to the telecommunications room door. Access to this room is now restricted to authorized personnel and is tracked by building management. Also, OIG noted that a workstation was not secured. Since the assessment, TSA has installed cable locks on all PC equipment located at the terminal. Finally, as the draft report noted, TSA has detailed plans and diagrams of a cage structure which will better protect IT equipment in the LAN room. TSA's Office of Security, Physical Security Division, has recently obtained permission to purchase the structure, and installation is expected to occur by Spring 2009.

Recommendation 5: Implement and document technical controls and processes to compensate for reported deficiencies.

TSA Concurs. TSA CIO implements and documents technical controls and processes to compensate for deficiencies and will continue to improve in this area. TSANet makes use of the Plan of Actions and Milestones (POA&Ms) process to ensure that deficiencies are documented, tracked, and addressed. For example, there are existing POA&Ms concerning the OIG identified deficiencies "null session" and "Remote Desktop Protocol." Additionally, the TSANet System Security Plan (SSP) will be amended to reflect that certain open ports, which were identified by OIG as unnecessary and having known vulnerabilities, are actually in use and needed for operations. TSA disagrees that these ports are unnecessary as they are actively used for file and print capabilities.

However, TSA recognizes the need to document the use of these ports; therefore, the TSANet SSP will be amended appropriately. Finally, TSA has disabled Domain Guest accounts at IAD. As a result, anyone trying to login with a Guest username will be denied access.

Recommendation 6: Apply the necessary operating system updates to systems operating at IAD.

TSA Concurs. TSA concurs and has already implemented this recommendation. Through Unisys, TSA employs an update (patch) management process which uses Altiris software to ensure that updates to all workstations and servers are installed in a timely way. All necessary operating system updates have been applied to all systems operating at IAD.

Appendix D
CBP Single Points of Failure at IAD

Sharon Huiswoud, Director, Department of Homeland Security, Information Technology Audits

Kevin Burke, Audit Manager, Department of Homeland Security, Information Technology Audits

Beverly Dale, Senior Auditor, Department of Homeland Security, Information Technology Audits

Frederick Shappee, Program Analyst, Department of Homeland Security, Information Technology Audits

Ravi Jindal, Management and Program Assistant, Department of Homeland Security, Information Technology Audits

Kia Smith, Referencer

Department of Homeland Security

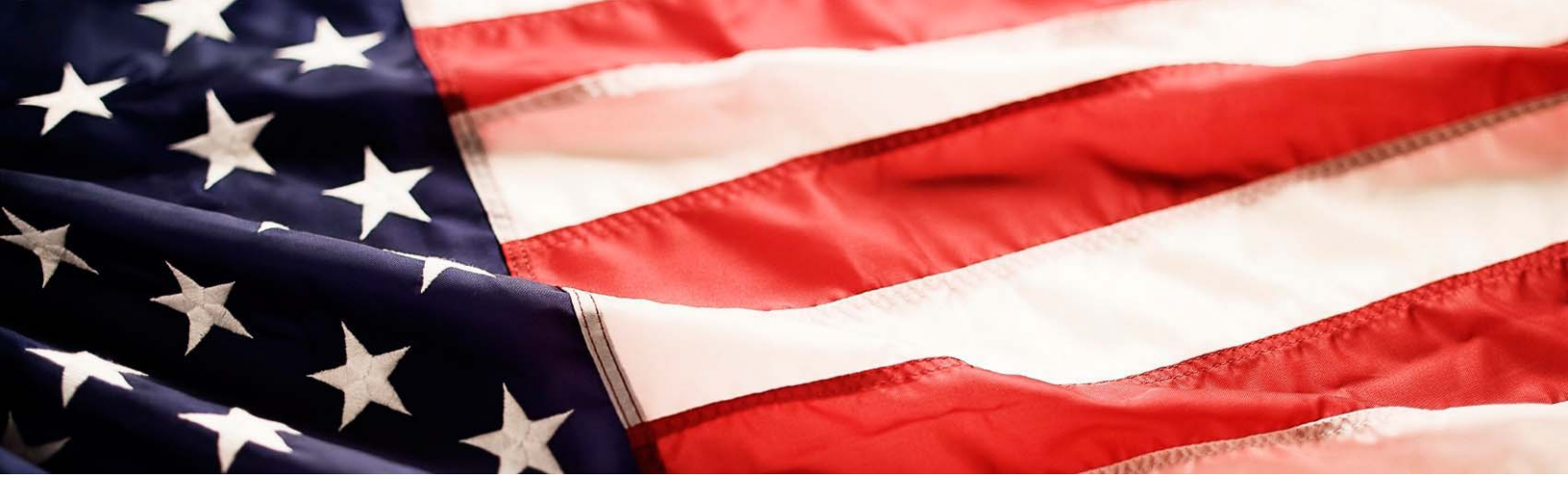
Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Component Liaison
DHS Chief Information Officer
CBP Chief Information Officer
TSA Chief Information 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 report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

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