Department of Homeland Security
Office of Inspector General

Technical Security Evaluation of DHS Activities at Los Angeles International Airport (Redacted)

Notice: The Department of Homeland Security, Office of the Inspector General, has redacted this report for public release.

OIG-09-01

October 2008

Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 1, 2008

Preface

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

This report addresses the strengths and weaknesses of the implementation of technical and information security policies and procedures at DHS components located at Los Angeles International Airport, California. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and reviews 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. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Table of Contents/Abbreviations

Abbreviations

CBP	Customs and Border Protection
CIO	Chief Information Officer
DAA	Designated Accrediting Authority
DHS	Department of Homeland Security
DHS Directive 4300A	DHS Sensitive Systems Policy Directive 4300A
DHS 4300A Handbook	DHS 4300A Sensitive Systems Handbook
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
FWFL	Far West Field LAN
HVAC	Heating, Ventilation, and Air Conditioning
ICE	Immigration and Customs Enforcement
ISA	Interconnection Security Agreement
ISSM	Information Systems Security Manger
IT	Information Technology
LAN	Local Area Network
LAX	Los Angeles International Airport
NOC	Network Operation Center
OIG	Office of Inspector General
SAC	Special Agent in Charge
SOC	Security Operation Center
SSP	System Security Plan
TA-FISMA	Trusted Agent FISMA
TECS	Treasury Enforcement Communications System
TSA	Transportation Security Administration
UPS	Uninterruptible Power Supply
USCG	United States Coast Guard
WLAN	Wireless Local Area Network

OIG

Department of Homeland Security
Office of Inspector General

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 Los Angeles International Airport. Customs and Border Protection, Immigration and Customs Enforcement, Transportation Security Administration, and the United States Coast Guard operate information technology systems or have a presence at this airport in support of Homeland Security operations.

Our evaluation focused on how these components had implemented computer security operational, technical, and management controls for their information technology assets at this site. We performed onsite inspections of the areas where these assets were located, interviewed Department of Homeland Security 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 this site have deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of their information technology systems. Specifically, these components need to improve their physical security operational controls for telecommunications equipment and servers. These components also could improve their technical controls by [redacted]

Additionally, these components need to improve their management controls by upgrading documentation to include information technology assets at Los Angeles International Airport.

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 non-repudiation within the DHS IT infrastructure and operations. A companion document—the *DHS 4300A Sensitive Systems Handbook* (DHS 4300A Handbook)—provides detailed guidance on the implementation of these policies.

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. 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.

Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and the United States Coast Guard (USCG) each have activities at Los Angeles International Airport (LAX). They rely on a range of IT assets to support their respective missions. As a Category X airport, LAX is classified among those airports with the largest number of enplanements.[1]

CBP's activities at LAX include processing passengers and baggage on arriving international flights. CBP staff at LAX use their systems to access various applications, including the Treasury Enforcement Communications System (TECS).[2]

ICE's Office of Investigations at the El Segundo Field Office supports operations at LAX that focus on a broad array of national security, financial, and smuggling violations, for example,

- Illegal arms exports,
- Financial crimes,
- Commercial fraud,
- Human trafficking,
- Narcotics smuggling,
- Child pornography/exploitation, and
- Immigration fraud.

Using their unique legal authorities, ICE special agents also conduct investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack, or exploitation.

TSA's activities include screening passengers and baggage on all departing flights at LAX. In support of these activities, TSA has operations in several buildings at LAX, and TSA staff use Digital Subscriber Lines circuits to access computer systems.

[1] 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.

[2] TECS is a CBP mission-critical law enforcement application designed to identify people and businesses suspected of or involved in violation of federal law. TECS is also a communications system permitting message transmittal among DHS law enforcement offices and other national, state, and local law enforcement agencies.

USCG personnel at LAX, designated Air Station Los Angeles, maintain search and rescue helicopters 24 hours a day, 365 days a year. They are responsible for protecting the coastal area of Southern California from Dana Point to Morro Bay. Additionally, USCG helicopters conduct homeland security patrols for the Ports of Los Angeles, Long Beach, and Hueneme. Its responsibilities include the over-water approach and departure corridors for LAX and the Channel Islands National Parks.

Results of Review

CBP Did Not Comply Fully With DHS Sensitive System Policies

CBP could strengthen operational, technical, and management controls for its servers, routers, and switches operating at LAX. For example, CBP could improve business continuity and physical security, and ensure that [redacted]

Additionally, CBP should take actions to ensure that its IT assets are scanned on a regular basis. Further, required system documentation should be updated to include CBP's IT assets at LAX. Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at LAX.

<u>Operational Controls</u>

Onsite implementation of operational controls that did not conform fully to DHS policies included [redacted]

Additionally, CBP needs to improve its [redacted]

Communications Redundancy

CBP experienced a network outage that disrupted its operations for more than 10 hours and affected more than 17,000 passengers on August 11, 2007.[3] This outage resulted in significant delays in processing arriving international passengers, causing the terminals to fill with passengers waiting to be processed. Because of this situation, the LAX fire marshal restricted the number of passengers that CBP could stage in the waiting areas and jet ways. Consequently, CBP staff at LAX were forced to keep many passengers on board aircraft for hours following international flights. Additionally, CBP staff were forced to reroute some flights to a nearby airport. This outage was exacerbated by an old IT infrastructure, which did not have network or power redundancy at LAX.

Subsequently, CBP has taken steps to ensure communications redundancy at LAX. Specifically, CBP added circuits and hardware to remove a single point-of-failure deficiency that previously existed. CBP also established a new

[3] Our draft report, *Customs and Border Protection Did Not Manage Effectively a Network Outage at Los Angeles International Airport*, will provide further information on the outage.

telecommunications closet in a second building at LAX. These actions ensure that CBP users at LAX will not be limited to one communications pathway when accessing CBP systems.

Business Continuity

CBP's business continuity capability needs to be strengthened at LAX. For example, [redacted]

CBP has implemented uninterruptible power supplies (UPS) [redacted]

Further, installing UPS devices for telecommunications equipment is not enough to ensure that CBP workstations will be in operation following a power failure. [redacted]

However, CBP has taken steps to ensure that they will be able to process passengers during a communications or power outage that lasts for a long duration. [redacted]

According to the DHS 4300A Handbook:

> "DHS must have the capability to ensure continuity of essential functions under all circumstances."

Physical Security Controls

CBP has taken steps to place its communications assets in locked cabinets within areas controlled by CBP. These actions will help secure CBP's IT assets at LAX from damage.

[redacted]

Figure 1: CBP replaced the old rack (left) with a new locking cabinet (right)

However, CBP has not completed this conversion at all locations at LAX. [redacted]

According to the DHS 4300A Handbook:

> "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."

Environmental Controls

During our September 2007 walk-through of DHS facilities, we noted that many of the CBP telecommunications rooms had temperatures exceeding 70 degrees Fahrenheit. While CBP is placing this equipment in cabinets that contain fans, there are no temperature sensors in the cabinets to automatically turn on the fans or to alert CBP staff if temperature exceeds 70 degrees Fahrenheit.

According to the DHS 4300A Handbook:

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

[redacted]

Additionally, at LAX, CBP is relying on the facility's fire suppression system. However, there were also fire extinguishers in two telecommunications rooms that either were not charged or had not been inspected within 12 years. Fire extinguishers that will not perform could cause CBP staff to waste valuable time during an emergency.

Further, in several of the server and telecommunications rooms there was poor electrical wiring, misplaced ceiling tiles, dust, and storage of non-IT assets. While we are aware that construction is ongoing, CBP should take steps to ensure that its IT assets will not be accidentally damaged during this transition period.

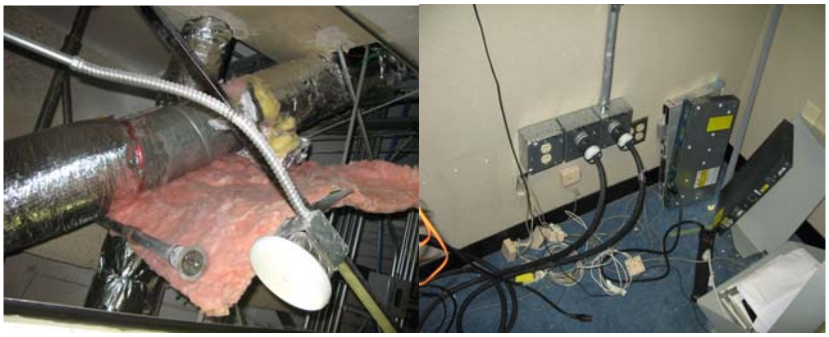


Figure 2: Missing ceiling tiles and inadequate storage at LAX.

<u>Technical Controls</u>

CBP's implementation of technical controls at LAX that did not conform fully to DHS [redacted]

Inadequate Network Monitoring

[redacted]

[redacted]

[redacted]

[redacted] Specifically, CBP has centralized its network monitoring activities [redacted]

Unsupported Operating System

CBP is operating six refugee fingerprint processing machines at LAX. At least one of these machines has an unsupported operating system. CBP is now working with the vendor to upgrade the operating systems on the refugee fingerprint devices at LAX and four other airports.

Operating systems that are not supported by their vendors may not receive updates or patches when a vulnerability or exploitation has been identified.

Inadequate Vulnerability Assessment

[redacted]

According to DHS Directive 4300A:

> "Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on IT systems containing sensitive information annually or whenever significant changes are made to the IT systems. This should include scanning for unauthorized wireless devices. Evidence that annual assessments have been conducted should be included with Security Assessment Reports (SAR)."

Inadequate Access Control

CBP could strengthen the access controls on its servers at LAX. [redacted]

According to the DHS 4300A Handbook,

> "Passwords shall be at least 8 characters in length … shall be changed or expire in 180 days or less."

[redacted]

Automated systems are vulnerable to fraudulent or malicious activity by anyone with the authority or capability to access information not required to perform their job-related duties.

According to the DHS 4300A Handbook,

> "To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks—i.e., users should be able to access only the system resources needed to fulfill their job responsibilities."

Vulnerable Services

CBP servers, routers, and switches at LAX have numerous [redacted]

[redacted]

[redacted]

[redacted] increase the risk that CBP systems may be compromised by malicious users or external attacks.

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."

Further, CBP's switches at LAX were not properly configured to prevent an "insider" from gaining unauthorized privileges and information.[4] [redacted] This may allow an attacker to capture login credentials and remotely take control of the router and change or delete configuration files.

[4] According to the National Institute of Standards and Technology's *Threat Assessment of Malicious Code and Human Threats* (NISTIR 4939), "Insiders are legitimate users of a system. When they use that access to circumvent security, that is known as an insider attack."

According to DHS Directive 4300A:

> [redacted]
> A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved by the Component shall be used instead."

Management Controls

CBP's implementation of management controls at LAX did not conform fully to DHS policies. [redacted] These management controls deficiencies increase the risk to CBP's IT investments, systems, and data from new threats and vulnerabilities for which safeguards have not been implemented.

Far West Field LAN

CBP's LAN at LAX is part of the FWFL.[5] Starting in September 2007, CBP upgraded old routers, switches, and circuits at LAX. However, CBP has not conducted a new risk assessment to determine if there is any potential security risk associated with the new infrastructure at LAX.

Additionally, CBP has not updated Trusted Agent – Federal Information Security Management Act (TA-FISMA) to include the new infrastructure at LAX. Specifically, LAX LAN is part of the FWFL, which is a "type accreditation" system.[6] However, CBP has not prepared the necessary attachments to its documentation annotating LAX site-specific physical and logical variations related to the new infrastructure that CBP had implemented at LAX.

[5] The Far West Field LAN system consists of 83 Field LAN systems, including the LAX LAN, connected to the CBP Private IP WAN. The Far West Field LANs consists of servers, desktop computers, printers, interconnecting wiring, and associated software. Its mission is to support the Field Offices/Agents with applications and technologies in the securing and protection of our Nation's borders.

[6] Type accreditation allows for common security control across sites to be consolidated and for a single master certification and authorization to be conducted.

According to DHS Directive 4300A:

> "Components shall conduct and document risk assessments every three years, when high impact weaknesses are identified, or whenever significant changes to the system configuration or to the operational/threat environment have been made, whichever occurs first."

According to DHS 4300A Sensitive Security Handbook, Attachment D –Type Accreditation:

> "To account for unique physical and logical variations at the site level, a description of any differences and the associated risks at each site are documented, and the site-specific documents are incorporated as attachments or appendices to the master C&A package."

Wireless Local Area Network

In November 2006, CBP installed a WLAN at LAX to provide high-speed mobile data connectivity and wireless coverage to CBP agents operating in and around LAX. However, CBP staff at LAX did not test the WLAN once it was connected to the CBP network. During the time of our visit at LAX, December 2007, CBP staff were unable to operate this system because of technical problems.

According to CBP staff, CBP did not test the WLAN after it was connected to the CBP network and does not know if CBP staff have ever used this system. Additionally, CBP did not document the WLAN in the FWFL SSP. Further, the WLAN was not included in CBP's systems inventory, DHS' Trusted Agent FISMA (TA-FISMA) reporting tool.[7]

According to the DHS 4300A:

> "Component [Information Systems Security Managers] ISSMs shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive IT systems, networks, or to their physical environments, interfaces, or user community. SSPs shall be updated and re-certification conducted if warranted."

[7] DHS uses an enterprise management tool, *Trusted Agent FISMA*, to collect and track data related to all Plans of Action and Milestones, including self-assessments, and certification and accreditation data.

CBP management cannot be assured that IT systems and data are adequately secured unless the various activities leading to accreditation are performed and the Designated Accrediting Authority (DAA) has accepted in writing the risks associated with operating the systems.

Miscellaneous Issue

CBP operates 1,900 IT devices at various facilities throughout the country that are not regularly scanned for vulnerabilities. [redacted] Further, the CBP SOC maintains a list of an additional 1,048 devices that it has excluded from being scanned for vulnerabilities. During the course of this evaluation, CBP started requiring vulnerability assessments [redacted] Finally, according to CBP staff, they have developed a new approach to vulnerability assessments [redacted] starting in February 2008.

These deficiencies increase the risk that CBP IT systems used at LAX and other locations are vulnerable [redacted]. CBP is at increased risk that a device may be open to attack if it does not perform vulnerability assessments regularly.

Recommendations

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

Recommendation #1: Implement business continuity of operations capability for CBP facilities at LAX, including the installation of a backup power supply.

Recommendation #2: Implement stronger physical security and environmental controls to protect CBP's IT assets from possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

Recommendation #3: Use a connection protocol that employs secure authentication.

<u>Recommendation #4:</u> Apply the necessary operating system upgrades.

<u>Recommendation #5:</u> Close all unnecessary ports from the servers, routers, and switches.

<u>Recommendation #6:</u> Update the FWFL SSP and perform risk assessments whenever there are significant changes to the system.

<u>Recommendation #7:</u> Regularly perform vulnerability assessments on IT systems containing sensitive information, as required by DHS Directive 4300A.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS Chief Information Officer. We have included a copy of the comments in their entirety at Appendix B.

In the comments, CBP concurred with recommendations one, two, and four through seven. These recommendations will be considered resolved but open pending verification of all planned actions.

CBP did not concur with recommendation three. [redacted]

> [redacted]

We maintain that CBP should comply with DHS 4300A and use a secure communications protocol.

ICE Did Not Comply Fully With DHS Sensitive System Policies

ICE could strengthen operational, technical, and management policies for the server, router, and switches at the El Segundo Field Office.[8] For example, ICE could enhance physical security of its server room, [redacted] Additionally, required system documentation should be updated to include ICE's IT assets at the El Segundo Field Office. Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at El Segundo.

Operational Controls

Onsite implementation of operational controls that did not conform fully to DHS policies included physical security and environmental controls. Specifically, ICE could better protect its IT assets by restricting access to ICE's server room or by placing the IT assets in a locked cabinet. Additionally, ICE IT assets are at risk of damage or malfunctioning because of the absence of an adequate HVAC system in its server room. These environmental and physical security controls deficiencies place the IT assets at the El Segundo Field Office at increased risk from unauthorized access and damage.

Physical Security and Environmental Controls

The ICE suite at El Segundo was not properly secure to prevent unauthorized access. [redacted]

[8] The El Segundo Field Office of Investigations supports ICE operations at LAX.

[redacted]

[redacted]

ICE also needs better physical security controls to limit access to its server room, which is located next to the main entrance to ICE office space. However, the server room door is always left open because the room does not have an adequate HVAC system. For example, the server room temperature was 76.6 degrees Fahrenheit at the time of our visit. Additionally, anyone entering the server room would have access to ICE back-up tapes, server, router, and switches because they are not stored in a locked cabinet. Figure 4 illustrates how the server room is not restricted, and the door is left open because of the absence of an HVAC system. Figure 5 shows the ICE IT assets that are not in a locked cabinet.

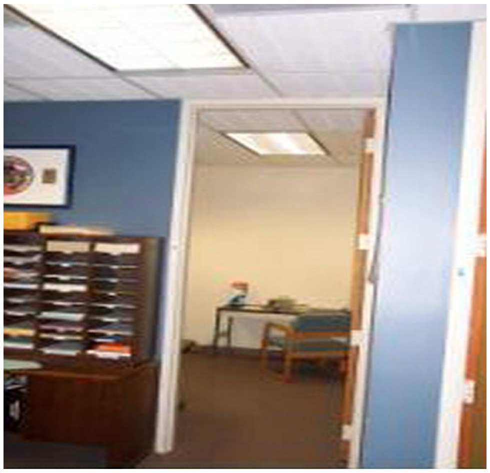


Figure 4: ICE server room with open door

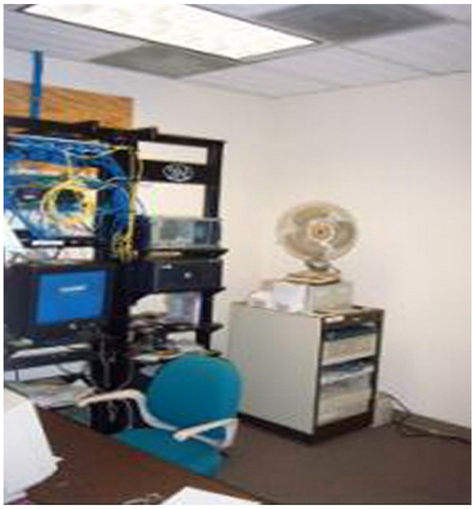


Figure 5: ICE server not secured in a locked cabinet

According to the DHS 4300A Handbook:

> "To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks—i.e., users should be able to access only the system resources needed to fulfill their job responsibilities."
>
> *********
>
> "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."
>
> *********
>
> "Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit."

<u>Technical Controls</u>

ICE's implementation of technical controls that did not conform fully to DHS policies includes operating a server that was running an unsupported operating system. Additionally, ICE's server, router, and switches were not properly configured to prevent an insider from gaining unauthorized privilege and information. These deficiencies increase the risk that ICE IT systems used at El Segundo Field Office are vulnerable to internal attacks.

Unsupported Operating System

An unsupported operating system was running on ICE's server at the El Segundo Field Office. [redacted] Operating systems that are not supported by their vendors may not receive updates or patches when a vulnerability or exploitation has been identified.

Access Controls

ICE could strengthen its access controls at the El Segundo Field Office. Specifically, users had administrative access to multiple files and directories. Additionally, shared administrative login accounts were in place, allowing multiple people to use the same account for system access.

This configuration increases the risk of loss or theft of ICE mission-sensitive data. For example, unauthorized personnel may have the ability to write, alter, or delete data that reside on shared resources.

According to the DHS 4300A Handbook:

> “To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks—i.e., users should be able to access only the system resources needed to fulfill their job responsibilities.”

Vulnerable Services

[redacted] An attacker could

potentially exploit this vulnerability to gain a list of usernames and other sensitive information.

Further, ICE's switches at El Segundo were not properly configured to prevent an insider from gaining unauthorized privileges and information. [redacted] This may allow an attacker to capture login credentials, remotely take control of the devices, and change or delete configuration files.

According to DHS Directive 4300A:

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

Management Controls

ICE's implementation of management controls at El Segundo did not conform fully to DHS policies. For example, ICE did not provide a system security plan that included the IT assets located at the El Segundo Field Office. Additionally, ICE's server and telecommunications equipment uses the CBP backbone for connectivity. However, ICE did not have an interconnection security agreement (ISA) between ICE and CBP for use of this system connectivity. These management controls deficiencies increase the risk to ICE's IT investments, systems, and data from new threats and vulnerabilities for which safeguards have not been implemented.

According to the DHS 4300A:

> "Component [Information Systems Security Managers] ISSMs shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive IT systems, networks, or to their physical environments, interfaces, or user community. SSPs shall be updated and re-certification conducted if warranted."

According to the DHS 4300A Handbook:

> "Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA)."
>
> **********
>
> "Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority."

Recommendations

We recommend that the ICE CIO take the following actions for ICE activities at LAX:

Recommendation #8: Implement stronger physical security to protect ICE's IT assets from possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

Recommendation #9: Provide an adequate HVAC system for the server room or obtain a waiver from the DAA.

Recommendation #10: Use a connection protocol that employs secure authentication.

Recommendation #11: Apply the necessary operating system upgrades to the server.

Recommendation #12: Eliminate or disable unnecessary ports from the server and router.

Recommendation #13: Establish and maintain the required interconnection security agreements.

Recommendation #14: Include the IT assets at the El Segundo Field Office in the system security plan for the Special Agent in Charge, West Region.

Management Comments and OIG Analysis

In the comments, ICE concurred with recommendations 8 through 12. These recommendations will be considered resolved but open pending verification of all planned actions. ICE did not concur with recommendations 13 and 14.

According to ICE, the deficiency associated with recommendation 13 is not applicable as both systems would have an aggregate security categorization of ‘high.’ [redacted]

Additionally, according to ICE, the deficiency associated with recommendation [redacted] However, according to DHS 4300A, Attachment D, *Type Accreditation*:

> “The documentation contains two critical types of information:
> - Site-specific details (e.g., deviations to functionality, configurations, and physical controls)
> - Site-specific risk analysis (e.g., additional risks that are perpetrated by the deviations at the site)”

[redacted] We maintain that ICE should comply with DHS 4300A and include the El Segundo Field Office in the appropriate system security plan.

TSA Did Not Comply Fully With DHS Sensitive System Policies

TSA could strengthen operational, technical, and management controls for its servers, router, and switches operating at LAX. For example, TSA could remove excess storage from its server room, implement fire suppression, and ensure that the most recent software security patches are installed on its server, router, and switches. Additionally, not all TSA IT resources at LAX are included in the TSA system inventory. Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by TSA at LAX.

Operational Controls

Onsite implementation of operational controls that did not conform fully to DHS policies included excess storage near computer equipment and inadequate environmental controls. Specifically, TSA could better protect its IT assets by ensuring that the immediate areas around the server and communication equipment are not used for general storage.

Physical Security

TSA administrative functions for LAX operations are performed in an offsite facility where TSA has several rooms with IT equipment. Although, these rooms are behind several locked doors, TSA needs to improve its physical security. For example, the server room at this location was being used to store new equipment as well as old equipment prior to disposal. There were also two unbraced shelves that could hinder access to the TSA servers, router, and switches following an earthquake. Figure 6 illustrates the condition of the TSA server room.

Additionally, the TSA telecommunications room in the logistics department contains a switch and a server that were not in a locked cabinet. This room was also used to store some non-IT related items. Further, TSA has a switch in another room that also was not in a locked cabinet.

The examples mentioned above increase the risk of accidental loss of power or damage to IT resources supporting TSA operations at LAX.

According to the DHS 4300A Handbook,

> "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."

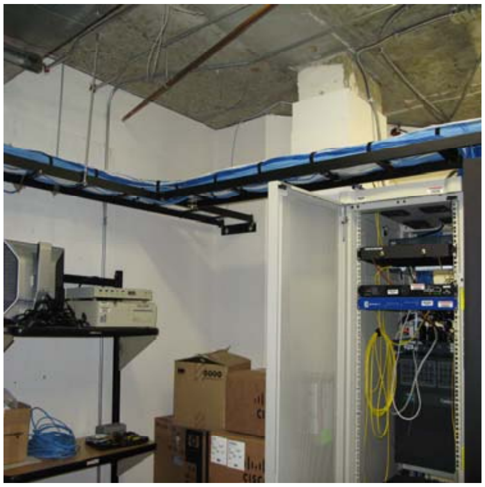


Figure 6: TSA server room used for storage

Environmental Controls

TSA also could improve environmental controls for its IT assets. For example, the temperature was 76.7 degrees Fahrenheit in the telecommunications room in the logistics department. Further, TSA was using a portable fan to cool down the switch mounted on the wall and the stand-alone server underneath the table. Figure 7 illustrates the condition of the TSA telecommunications room at LAX.

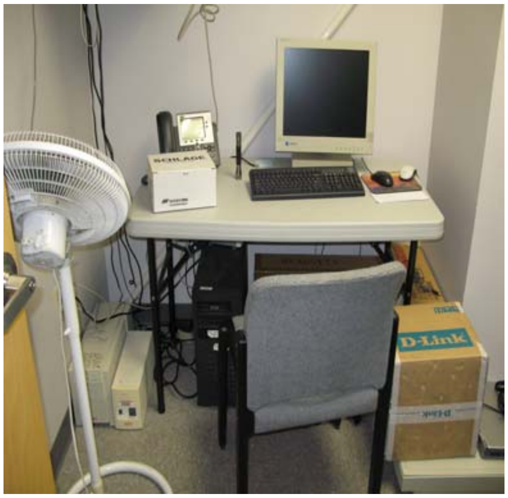


Figure 7: Portable fan used to cool switch and server area

TSA's communications equipment was also at risk of failure because of the absence of temperature or humidity sensors in the communications rooms. The absence of environmental sensors and proper HVAC for IT equipment increases the risk that TSA's IT assets may malfunction.

According to the DHS 4300A Handbook,

> "The condition of the air is important to prevent damage to IT equipment."

Additionally, TSA did not have a fire suppression system in place at LAX. Specifically, no water sprinklers or fire extinguishers were at the server room or telecommunication closets. The absence of an adequate fire suppression system places TSA's IT assets at risk of possible loss, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters. As a compensating control, TSA has already deployed fire extinguishers to resolve this deficiency.

According to the DHS 4300A Handbook:

> "When a centralized fire suppression system is not available, fire extinguishers should be readily available."

Technical Controls

TSA's implementation of technical controls at LAX that did not conform fully to DHS policies include inadequate access controls, insecure communications protocols, and open ports with known vulnerabilities. These deficiencies increase the risk that TSA IT systems used at LAX are vulnerable to internal attacks.

Access Controls

Configuration management for the TSA server needs to be strengthened. Specifically, the Lightweight Directory Access Protocol is configured to allow anonymous access to the TSA server. As a result, an unauthorized user or a hacker could log in to the system without proper credentials.
Additionally, the Windows built-in user group "EVERYONE" was configured to allow full control and access to shared data. This may allow an unauthenticated user to upload malicious code onto a shared resource.

The purpose of access controls is to protect against the unauthorized disclosure, modification, or destruction of data residing in these systems, as well as the applications themselves. Automated systems are vulnerable to fraudulent or malicious activity by anyone with the authority or capability to access information not required to perform their duties.

According to the DHS 4300A Handbook:

> "To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks—i.e., users should be able to access only the system resources needed to fulfill their job responsibilities."

Insecure Communications Protocols

TSA's switches at LAX were not properly configured to prevent an insider from gaining unauthorized privileges and information. For example, telnet was being used on a TSA switch at LAX. However, telnet does not encrypt login and password credentials. This may allow an attacker to capture login credentials and remotely take control of the router and change or delete configuration files.

Additionally, the File Transfer Protocol (FTP) port 21 was active, leaving the device vulnerable to unauthorized access. FTP is not permitted on DHS systems due to the potential risk when used for non-administrative purposes. For instance, just like telnet, FTP transmits login and password credentials in clear text.

According to DHS Directive 4300A:

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

Vulnerable Services

TSA's servers, router, and switches at LAX have numerous open ports and services on its system that may not be necessary. For example, the following services with known vulnerabilities were running:

- The server was configured to allow **Domain Name System** zone transfers to be performed. This potentially poses a security risk of denial of service attacks.
- **Web Server** was running on a nonstandard port.
- The version of **Internet Information Services** running on the system is vulnerable to denial of service attacks.

Additionally, the Null session was configured to allow a user to connect to the system without authentication. An attacker could potentially exploit the null session to gain a list of usernames and other potentially sensitive information. Unnecessary open ports and services increase the risk that TSA systems may be compromised by malicious users or external attacks.

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

TSA's implementation of management controls at LAX did not conform fully to DHS policies. Specifically, not all TSA IT resources at LAX are accounted for in its system inventory. For example, the logistics server and database are not included in the TSA system inventory or the TSA certification and accreditation process. TSA management cannot be assured that IT systems and data are adequately secured unless the various activities leading to accreditation are performed and the DAA has accepted in writing the risks associated with operating the systems.

These management controls deficiencies increase the risk to TSA's IT investments, systems, and data from new threats and vulnerabilities for which safeguards have not been implemented.

According to DHS 4300A Handbook:

> "The initial Risk Assessment is updated and revised and becomes the final Risk Assessment as part of the overall accreditation process after the controls are implemented and tested and the results/corrective actions are implemented. Through the development of the final Risk Assessment, the definition of the program residual risk can be determined for the DAA's acceptance during accreditation."

Recommendations

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

Recommendation #15: Improve its physical and environmental controls to protect TSA's IT assets from possible accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

Recommendation #16: Use a connection protocol that employs secure authentication.

Recommendation #17: Eliminate or disable unnecessary ports from the servers, router, and switches.

Recommendation #18: Ensure that all IT systems are included in TSA's inventory.

Management Comments and OIG Analysis

In the comments, TSA concurred with recommendations 15 through 18. These recommendations will be considered resolved but open pending verification of all planned actions.

USCG Did Not Comply Fully With DHS Sensitive System Policies

USCG could strengthen operational and technical controls for its server, router, and switches operating at LAX. For example, USCG back-up tapes should be stored in an off-site facility. Additionally, USCG could strengthen access controls and ensure that only necessary ports are open on its server, router, and switches. [redacted] Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by USCG at LAX.

Operational Controls

Onsite implementation of operational controls that did not conform fully to DHS policies included USCG IT assets that were not in a locked cabinet. Further, USCG needs to better safeguard its sensitive data stored on back-up tapes. Unauthorized personnel may have access to USCG IT assets and sensitive data stored in the back-up tapes. Figure 8 below illustrates USCG's open-rack pack with its back-up tapes stored in the USCG server room. [redacted] To ensure the availability and integrity of USCG data, back-up tapes should be stored in an off-site facility accessible by authorized personnel only.

[redacted]

[redacted]

According to the DHS 4300A Handbook:

> "Components shall ensure backup media are stored off site in accordance with their business continuity and IT Contingency plans."

<u>Technical Controls</u>

USCG's implementation of technical controls at LAX that did not conform fully to DHS policies include access control and password management requirements. [redacted] These deficiencies increase the risk that USCG IT systems used at LAX are vulnerable to internal attacks.

Access Controls

[redacted] Excess privilege given to users can put USCG data at risk by allowing insiders and others the opportunity to penetrate a system. This could result in the loss, theft, or destruction of USCG data.

Additionally, USCG could strengthen password policies on its LAX systems. [redacted]

According to the DHS 4300A Handbook:

> "To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks—i.e., users should be able to access only the system resources needed to fulfill their job responsibilities."

System Patches

According to our technical scans, [redacted] USCG data may be compromised if patches are not installed in a timely fashion.

Vulnerable Services

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

Unnecessary open ports and services increase the risk that USCG's systems at LAX may be compromised by malicious users or external attacks.

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."

Insecure Communications Protocols

[redacted]

According to DHS Directive 4300A:

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

Management Controls

We did not find any reportable management control deficiencies for the USCG site at LAX.

Recommendations

We recommend that the USCG CIO take the following actions for USCG activities at LAX:

Recommendation #19: Store back-up tapes in an off-site facility.

Recommendation #20: Implement the password policy established by DHS Directive 4300A.

Recommendation #21: Develop a process for implementing identified patches in a timely fashion.

Recommendation #22: Eliminate or disable unnecessary ports from the server and router.

Recommendation #23: Use a connection protocol that employs secure authentication.

Management Comments and OIG Analysis

In the comments, USCG concurred with recommendations 19 through 23. These recommendations will be considered resolved but open pending verification of all planned actions.

Purpose, Scope, and Methodology

This review is part of a program to evaluate, on an ongoing basis, the implementation of DHS technical and information security policies and procedures at DHS sites. The objective of this program is to determine the extent to which critical DHS sites comply with the department's technical and information security policies and procedures, according to DHS Directive 4300A and its companion document, the DHS 4300A Handbook.

We coordinated the implementation of this technical security evaluation program with the DHS Chief Information Security Officer (CISO). We mutually agreed to the wording for the Rules of Behavior for the technical testing.[9] Our entrance and exit conferences were held with DHS components officials.

Technical evaluations were performed only after the DHS CISO and DHS components official agreed to our negotiated Rules of Behavior. These technical evaluations included:

- Security scans of the servers, routers, and switches using various software packages, and
- Scans to determine whether wireless devices were being used by DHS components.

We reviewed applicable DHS and components' policies and procedures, and components' responses to our site surveys and technical questionnaires. For example, we used components' responses to identify occupied space, server rooms, and telecommunications closets. Our onsite review included a physical review of components' space and interviews with components staff.

Our technical review included technical scans of security controls as well as scans for DHS wireless devices operating at LAX. Additionally, we reviewed guidance provided by DHS to the components in the areas of patch management, operation systems, and wireless security.

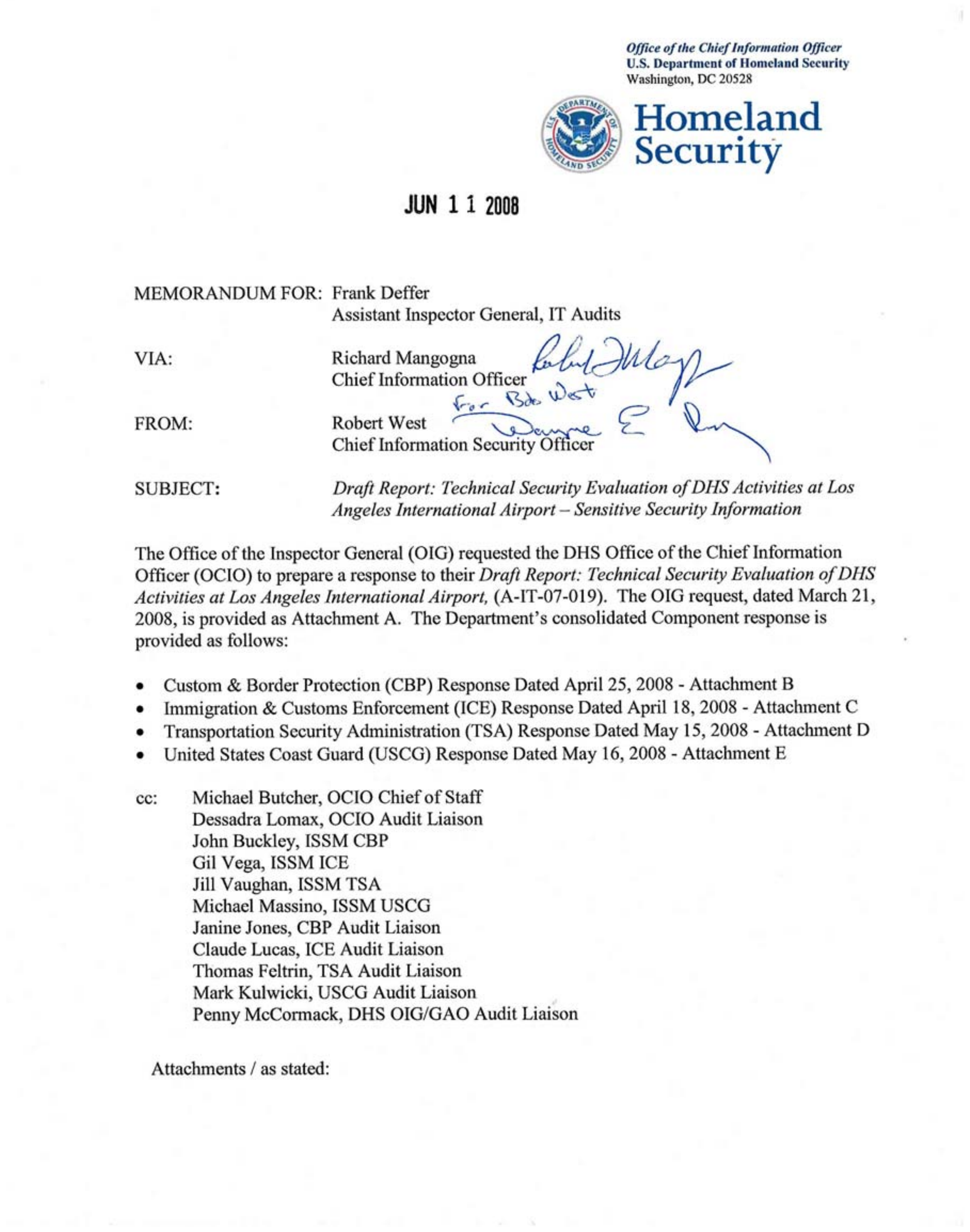
We provided components with briefings concerning the results of fieldwork and the information summarized in this report. We conducted this review between September 2007 and March 2008.

[9] The Rules of Behavior established the boundaries and schedules for the technical evaluations.

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 by DHS management and staff to provide the information and access necessary to accomplish this review. Our points of contact for this report are Frank Deffer, Assistant Inspector General for Information Technology, (202) 254-4100, and Roger Dressler, Director for Information Systems and Architectures, (202) 254-5441. Major OIG contributors to the review are identified in Appendix C.

Appendix B
Management's Response to the Draft Report



Office of the Chief Information Officer
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

JUN 1 1 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General, IT Audits

VIA: Richard Mangogna
Chief Information Officer

For Bob West

FROM: Robert West
Chief Information Security Officer

SUBJECT: *Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport – Sensitive Security Information*

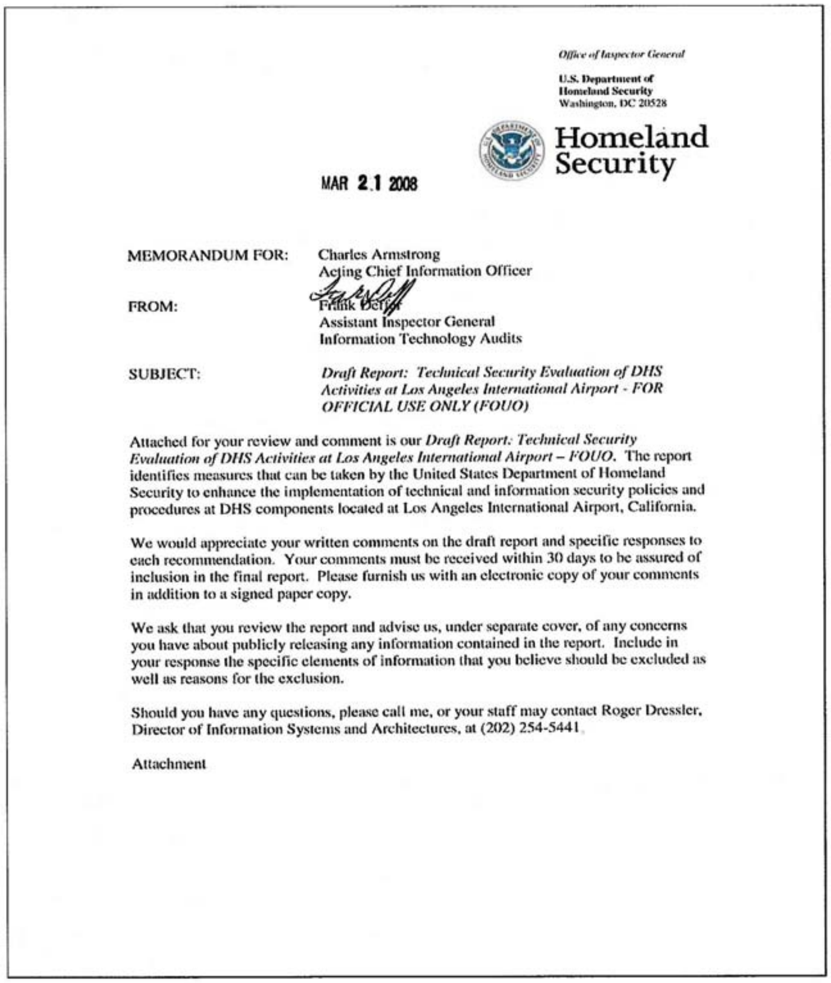
The Office of the Inspector General (OIG) requested the DHS Office of the Chief Information Officer (OCIO) to prepare a response to their *Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport,* (A-IT-07-019). The OIG request, dated March 21, 2008, is provided as Attachment A. The Department's consolidated Component response is provided as follows:

- Custom & Border Protection (CBP) Response Dated April 25, 2008 - Attachment B
- Immigration & Customs Enforcement (ICE) Response Dated April 18, 2008 - Attachment C
- Transportation Security Administration (TSA) Response Dated May 15, 2008 - Attachment D
- United States Coast Guard (USCG) Response Dated May 16, 2008 - Attachment E

cc: Michael Butcher, OCIO Chief of Staff
Dessadra Lomax, OCIO Audit Liaison
John Buckley, ISSM CBP
Gil Vega, ISSM ICE
Jill Vaughan, ISSM TSA
Michael Massino, ISSM USCG
Janine Jones, CBP Audit Liaison
Claude Lucas, ICE Audit Liaison
Thomas Feltrin, TSA Audit Liaison
Mark Kulwicki, USCG Audit Liaison
Penny McCormack, DHS OIG/GAO Audit Liaison

Attachments / as stated:

ATTACHMENT A:
OIG Transmittal Letter Requesting Comments on Draft Report Dated March 21, 2008
Technical Security Evaluation of DHS Activities at Los Angeles International Airport



Office of Inspector General

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

Homeland
Security

MAR 2 1 2008

MEMORANDUM FOR: Charles Armstrong
Acting Chief Information Officer

FROM: Frank Deffer
Assistant Inspector General
Information Technology Audits

SUBJECT: *Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport - FOR OFFICIAL USE ONLY (FOUO)*

Attached for your review and comment is our *Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport – FOUO.* The report identifies measures that can be taken by the United States Department of Homeland Security to enhance the implementation of technical and information security policies and procedures at DHS components located at Los Angeles International Airport, California.

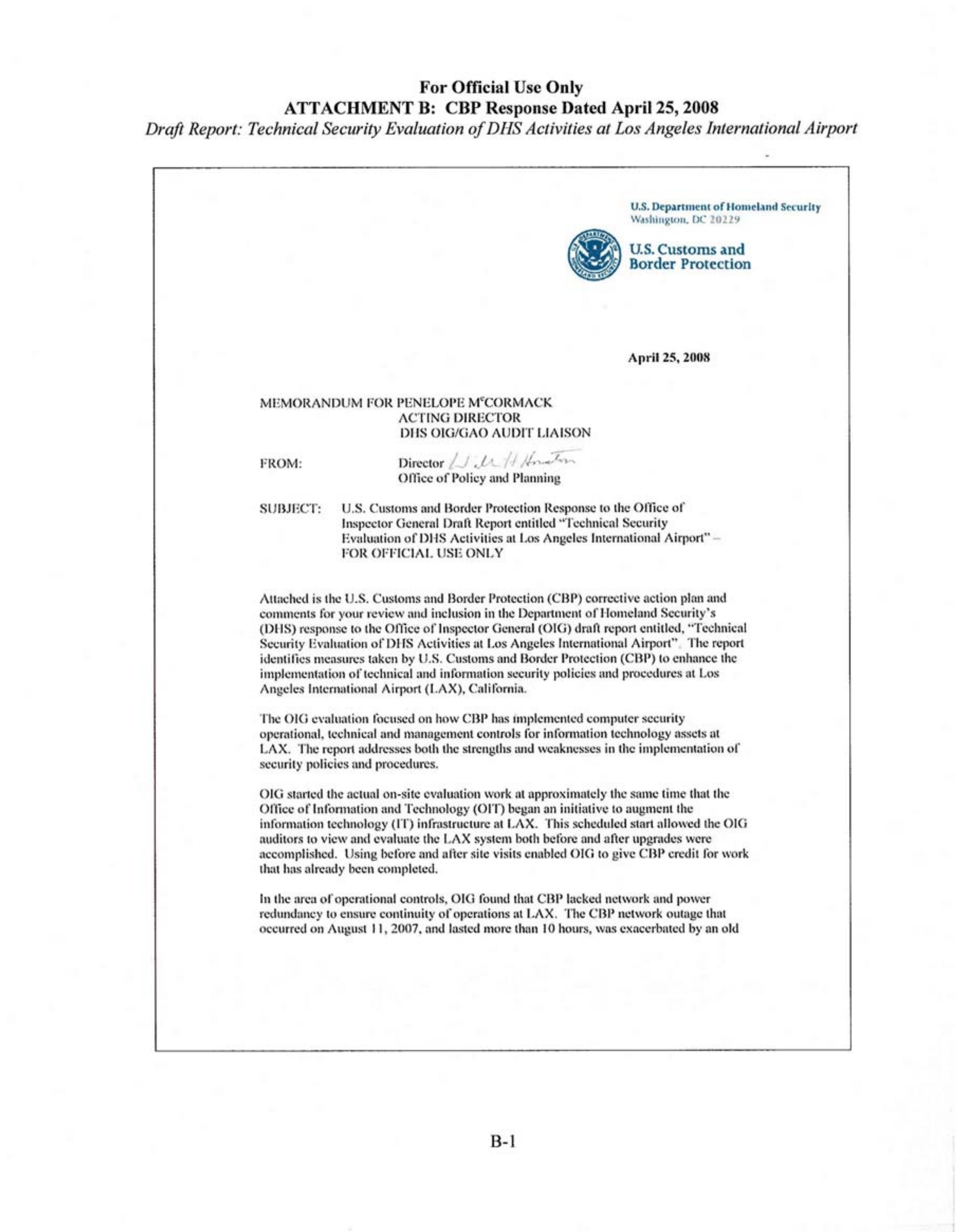
We would appreciate your written comments on the draft report and specific responses to each recommendation. Your comments must be received within 30 days to be assured of inclusion in the final report. Please furnish us with an electronic copy of your comments in addition to a signed paper copy.

We ask that you review the report and advise us, under separate cover, of any concerns you have about publicly releasing any information contained in the report. Include in your response the specific elements of information that you believe should be excluded as well as reasons for the exclusion.

Should you have any questions, please call me, or your staff may contact Roger Dressler, Director of Information Systems and Architectures, at (202) 254-5441.

Attachment

Appendix B
Management's Response to the Draft Report



For Official Use Only
ATTACHMENT B: CBP Response Dated April 25, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

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

U.S. Customs and Border Protection

April 25, 2008

MEMORANDUM FOR PENELOPE M^cCORMACK
ACTING DIRECTOR
DHS OIG/GAO AUDIT LIAISON

FROM: Director
Office of Policy and Planning

SUBJECT: U.S. Customs and Border Protection Response to the Office of Inspector General Draft Report entitled "Technical Security Evaluation of DHS Activities at Los Angeles International Airport" – FOR OFFICIAL USE ONLY

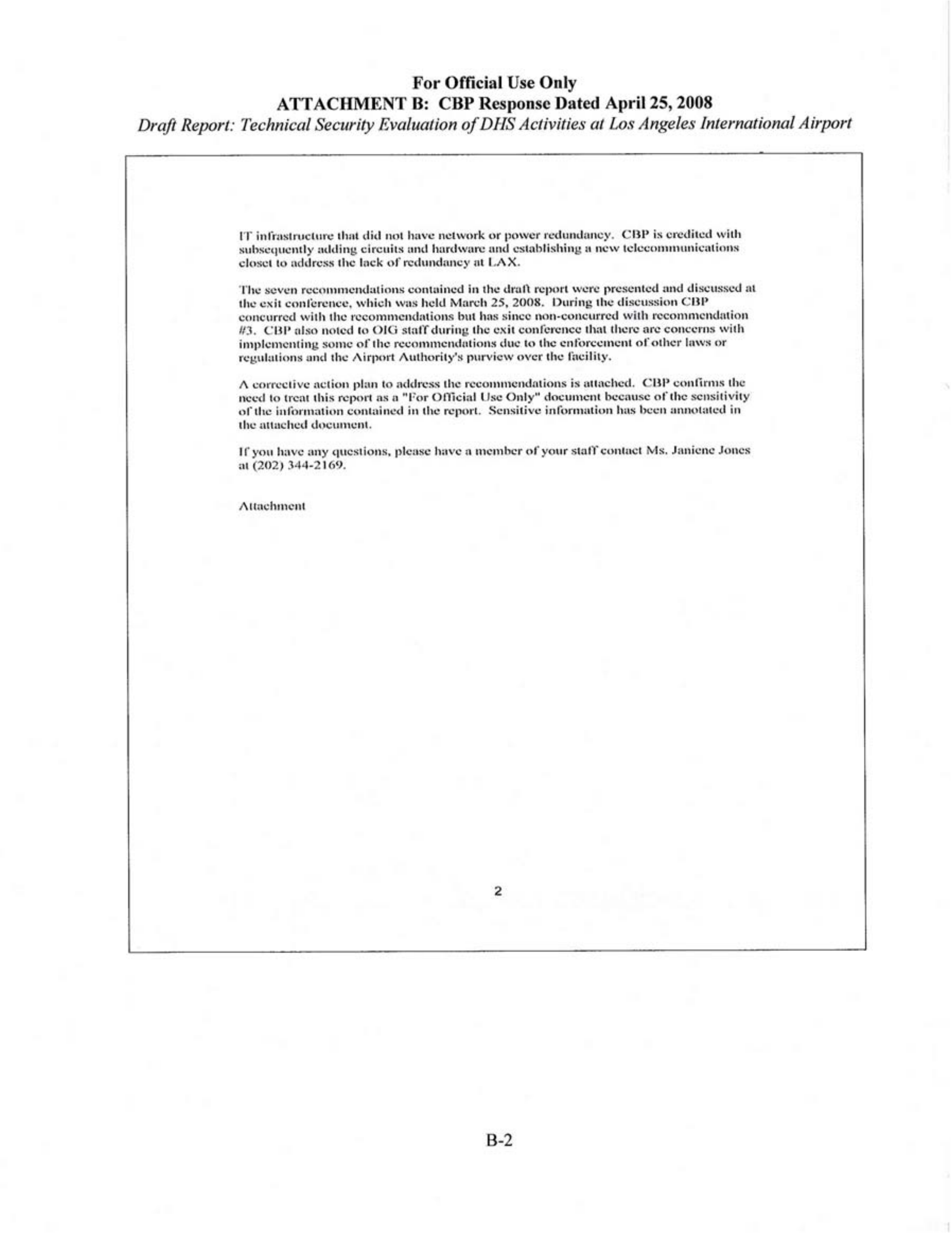
Attached is the U.S. Customs and Border Protection (CBP) corrective action plan and comments for your review and inclusion in the Department of Homeland Security's (DHS) response to the Office of Inspector General (OIG) draft report entitled, "Technical Security Evaluation of DHS Activities at Los Angeles International Airport". The report identifies measures taken by U.S. Customs and Border Protection (CBP) to enhance the implementation of technical and information security policies and procedures at Los Angeles International Airport (LAX), California.

The OIG evaluation focused on how CBP has implemented computer security operational, technical and management controls for information technology assets at LAX. The report addresses both the strengths and weaknesses in the implementation of security policies and procedures.

OIG started the actual on-site evaluation work at approximately the same time that the Office of Information and Technology (OIT) began an initiative to augment the information technology (IT) infrastructure at LAX. This scheduled start allowed the OIG auditors to view and evaluate the LAX system both before and after upgrades were accomplished. Using before and after site visits enabled OIG to give CBP credit for work that has already been completed.

In the area of operational controls, OIG found that CBP lacked network and power redundancy to ensure continuity of operations at LAX. The CBP network outage that occurred on August 11, 2007, and lasted more than 10 hours, was exacerbated by an old

B-1



For Official Use Only
ATTACHMENT B: CBP Response Dated April 25, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

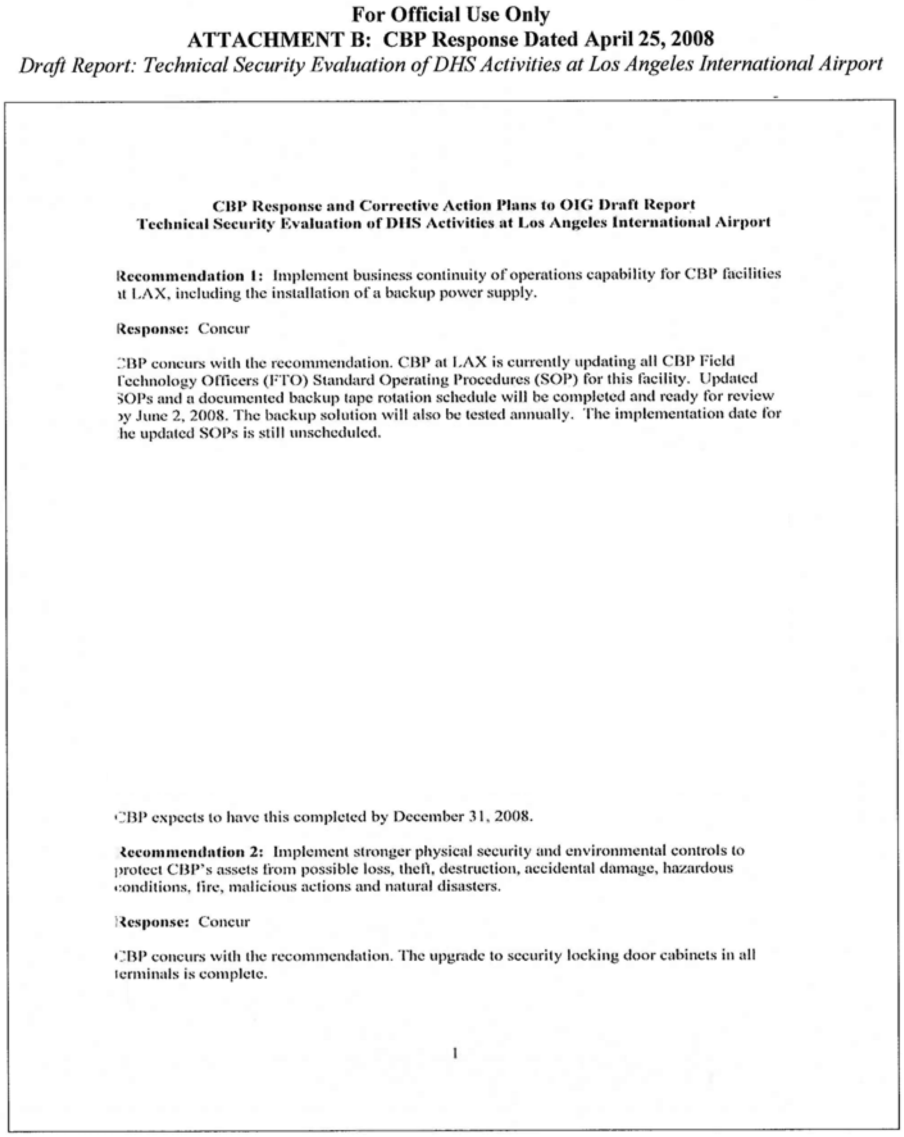
IT infrastructure that did not have network or power redundancy. CBP is credited with subsequently adding circuits and hardware and establishing a new telecommunications closet to address the lack of redundancy at LAX.

The seven recommendations contained in the draft report were presented and discussed at the exit conference, which was held March 25, 2008. During the discussion CBP concurred with the recommendations but has since non-concurred with recommendation #3. CBP also noted to OIG staff during the exit conference that there are concerns with implementing some of the recommendations due to the enforcement of other laws or regulations and the Airport Authority's purview over the facility.

A corrective action plan to address the recommendations is attached. CBP confirms the need to treat this report as a "For Official Use Only" document because of the sensitivity of the information contained in the report. Sensitive information has been annotated in the attached document.

If you have any questions, please have a member of your staff contact Ms. Janiene Jones at (202) 344-2169.

Attachment



For Official Use Only
ATTACHMENT B: CBP Response Dated April 25, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

CBP Response and Corrective Action Plans to OIG Draft Report
Technical Security Evaluation of DHS Activities at Los Angeles International Airport

Recommendation 1: Implement business continuity of operations capability for CBP facilities at LAX, including the installation of a backup power supply.

Response: Concur

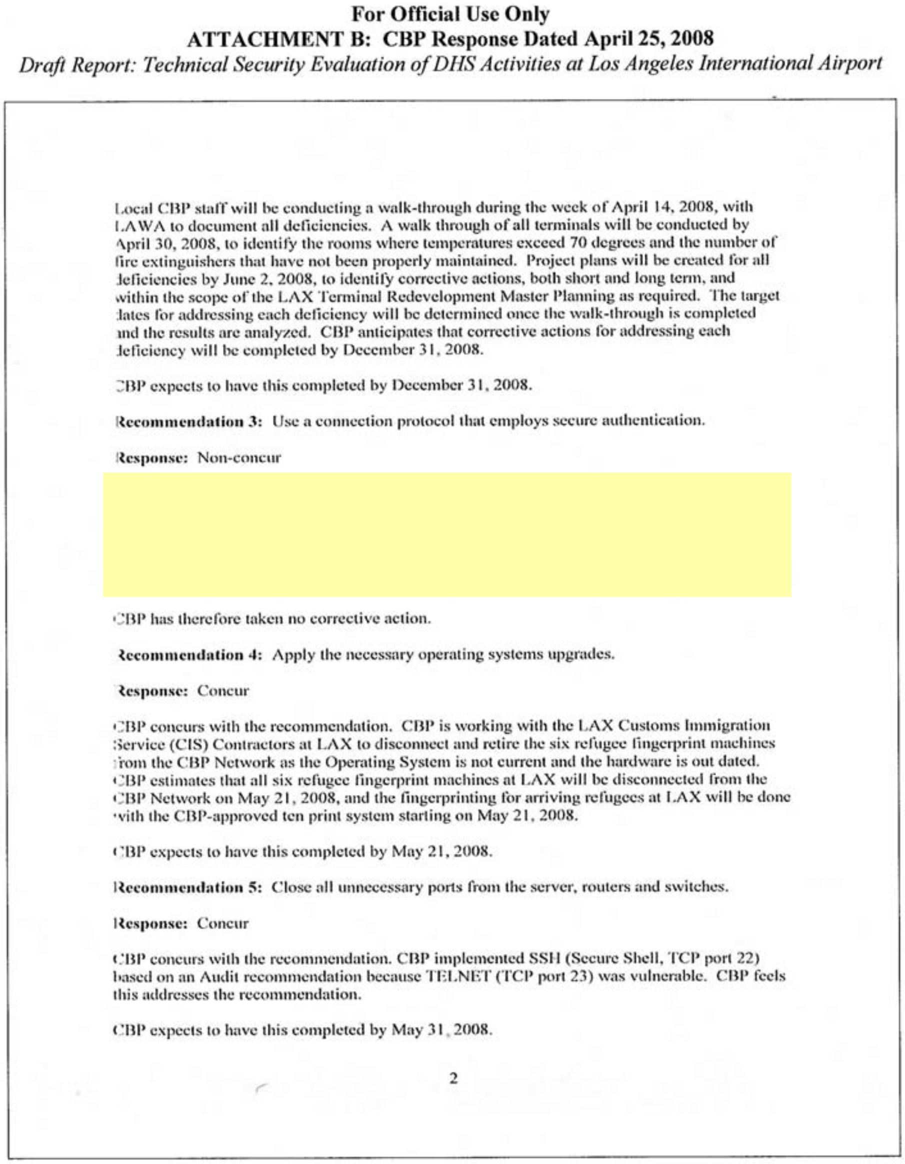
CBP concurs with the recommendation. CBP at LAX is currently updating all CBP Field Technology Officers (FTO) Standard Operating Procedures (SOP) for this facility. Updated SOPs and a documented backup tape rotation schedule will be completed and ready for review by June 2, 2008. The backup solution will also be tested annually. The implementation date for he updated SOPs is still unscheduled.

CBP expects to have this completed by December 31, 2008.

Recommendation 2: Implement stronger physical security and environmental controls to protect CBP's assets from possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions and natural disasters.

Response: Concur

CBP concurs with the recommendation. The upgrade to security locking door cabinets in all terminals is complete.



For Official Use Only

ATTACHMENT B: CBP Response Dated April 25, 2008

Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

Local CBP staff will be conducting a walk-through during the week of April 14, 2008, with LAWA to document all deficiencies. A walk through of all terminals will be conducted by April 30, 2008, to identify the rooms where temperatures exceed 70 degrees and the number of fire extinguishers that have not been properly maintained. Project plans will be created for all deficiencies by June 2, 2008, to identify corrective actions, both short and long term, and within the scope of the LAX Terminal Redevelopment Master Planning as required. The target dates for addressing each deficiency will be determined once the walk-through is completed and the results are analyzed. CBP anticipates that corrective actions for addressing each deficiency will be completed by December 31, 2008.

CBP expects to have this completed by December 31, 2008.

Recommendation 3: Use a connection protocol that employs secure authentication.

Response: Non-concur

[redacted]

CBP has therefore taken no corrective action.

Recommendation 4: Apply the necessary operating systems upgrades.

Response: Concur

CBP concurs with the recommendation. CBP is working with the LAX Customs Immigration Service (CIS) Contractors at LAX to disconnect and retire the six refugee fingerprint machines from the CBP Network as the Operating System is not current and the hardware is out dated. CBP estimates that all six refugee fingerprint machines at LAX will be disconnected from the CBP Network on May 21, 2008, and the fingerprinting for arriving refugees at LAX will be done with the CBP-approved ten print system starting on May 21, 2008.

CBP expects to have this completed by May 21, 2008.

Recommendation 5: Close all unnecessary ports from the server, routers and switches.

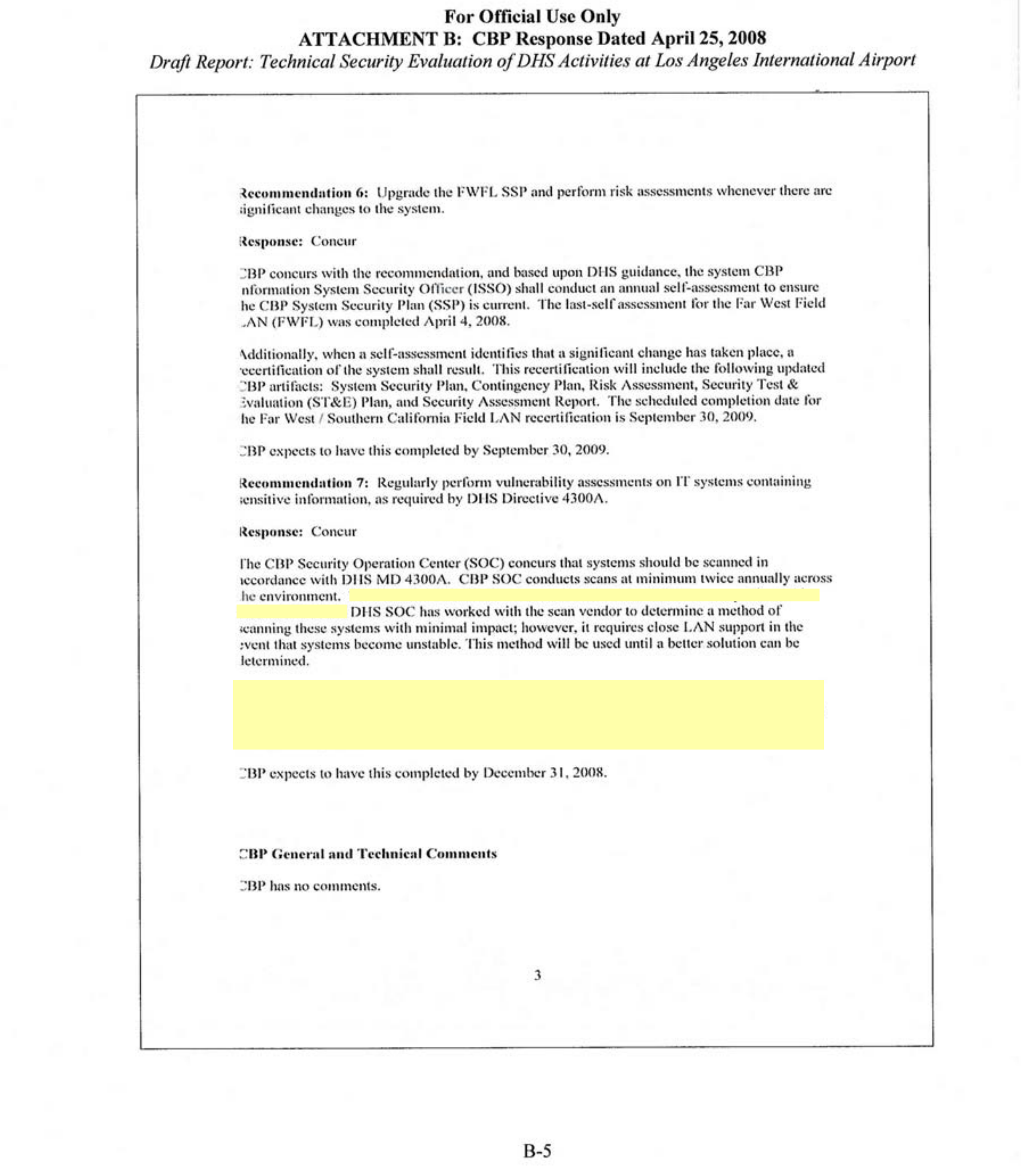
Response: Concur

CBP concurs with the recommendation. CBP implemented SSH (Secure Shell, TCP port 22) based on an Audit recommendation because TELNET (TCP port 23) was vulnerable. CBP feels this addresses the recommendation.

CBP expects to have this completed by May 31, 2008.

2

B-4



For Official Use Only
ATTACHMENT B: CBP Response Dated April 25, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

Recommendation 6: Upgrade the FWFL SSP and perform risk assessments whenever there are significant changes to the system.

Response: Concur

CBP concurs with the recommendation, and based upon DHS guidance, the system CBP nformation System Security Officer (ISSO) shall conduct an annual self-assessment to ensure he CBP System Security Plan (SSP) is current. The last-self assessment for the Far West Field LAN (FWFL) was completed April 4, 2008.

Additionally, when a self-assessment identifies that a significant change has taken place, a recertification of the system shall result. This recertification will include the following updated CBP artifacts: System Security Plan, Contingency Plan, Risk Assessment, Security Test & Evaluation (ST&E) Plan, and Security Assessment Report. The scheduled completion date for he Far West / Southern California Field LAN recertification is September 30, 2009.

CBP expects to have this completed by September 30, 2009.

Recommendation 7: Regularly perform vulnerability assessments on IT systems containing sensitive information, as required by DHS Directive 4300A.

Response: Concur

The CBP Security Operation Center (SOC) concurs that systems should be scanned in accordance with DHS MD 4300A. CBP SOC conducts scans at minimum twice annually across he environment. [redacted] DHS SOC has worked with the scan vendor to determine a method of scanning these systems with minimal impact; however, it requires close LAN support in the event that systems become unstable. This method will be used until a better solution can be determined.

[redacted]

CBP expects to have this completed by December 31, 2008.

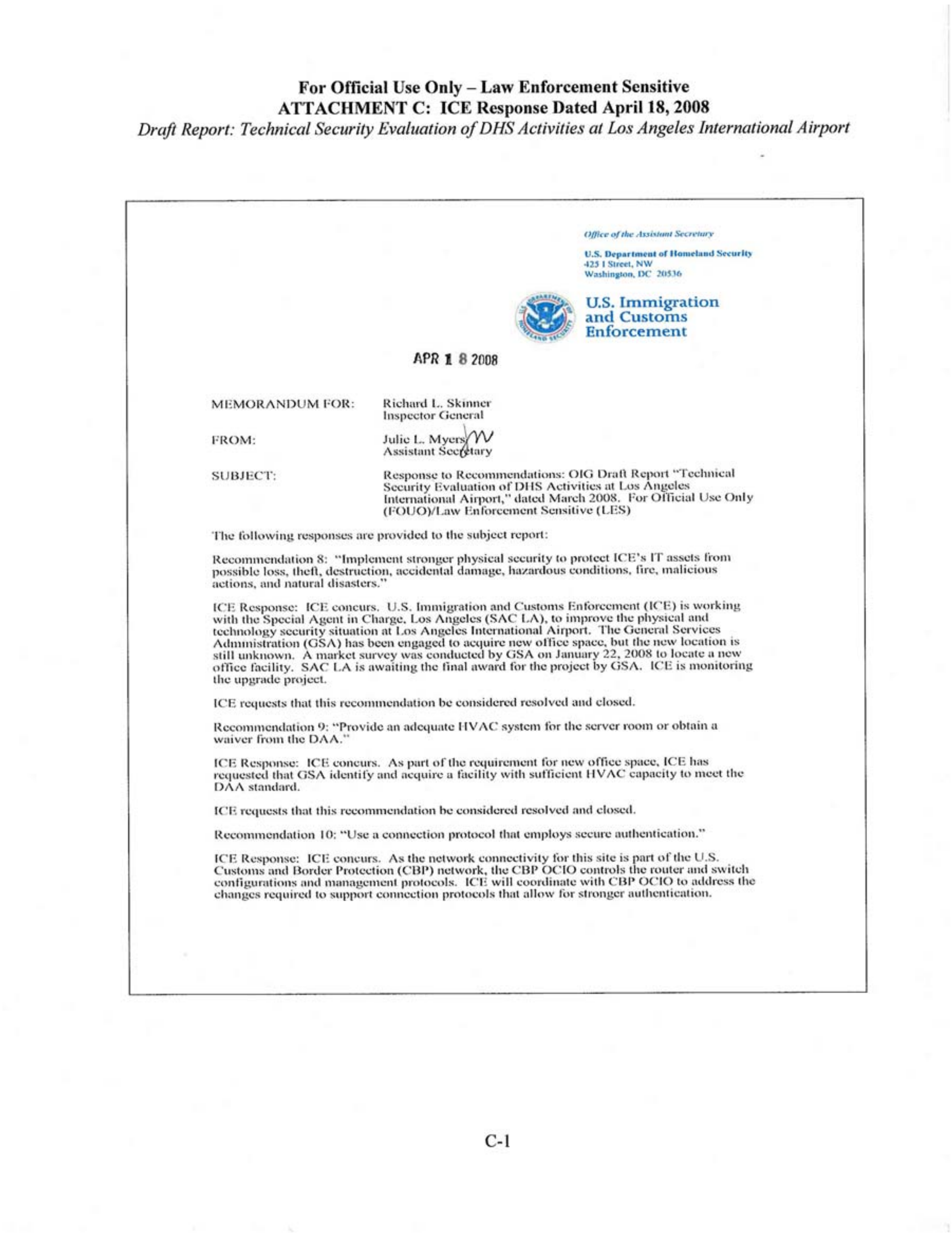
CBP General and Technical Comments

CBP has no comments.

3

B-5

Appendix B
Management's Response to the Draft Report



For Official Use Only – Law Enforcement Sensitive
ATTACHMENT C: ICE Response Dated April 18, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

Office of the Assistant Secretary

U.S. Department of Homeland Security
425 I Street, NW
Washington, DC 20536

U.S. Immigration
and Customs
Enforcement

APR 1 8 2008

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Julie L. Myers
Assistant Secretary

SUBJECT: Response to Recommendations: OIG Draft Report "Technical Security Evaluation of DHS Activities at Los Angeles International Airport," dated March 2008. For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)

The following responses are provided to the subject report:

Recommendation 8: "Implement stronger physical security to protect ICE's IT assets from possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters."

ICE Response: ICE concurs. U.S. Immigration and Customs Enforcement (ICE) is working with the Special Agent in Charge, Los Angeles (SAC LA), to improve the physical and technology security situation at Los Angeles International Airport. The General Services Administration (GSA) has been engaged to acquire new office space, but the new location is still unknown. A market survey was conducted by GSA on January 22, 2008 to locate a new office facility. SAC LA is awaiting the final award for the project by GSA. ICE is monitoring the upgrade project.

ICE requests that this recommendation be considered resolved and closed.

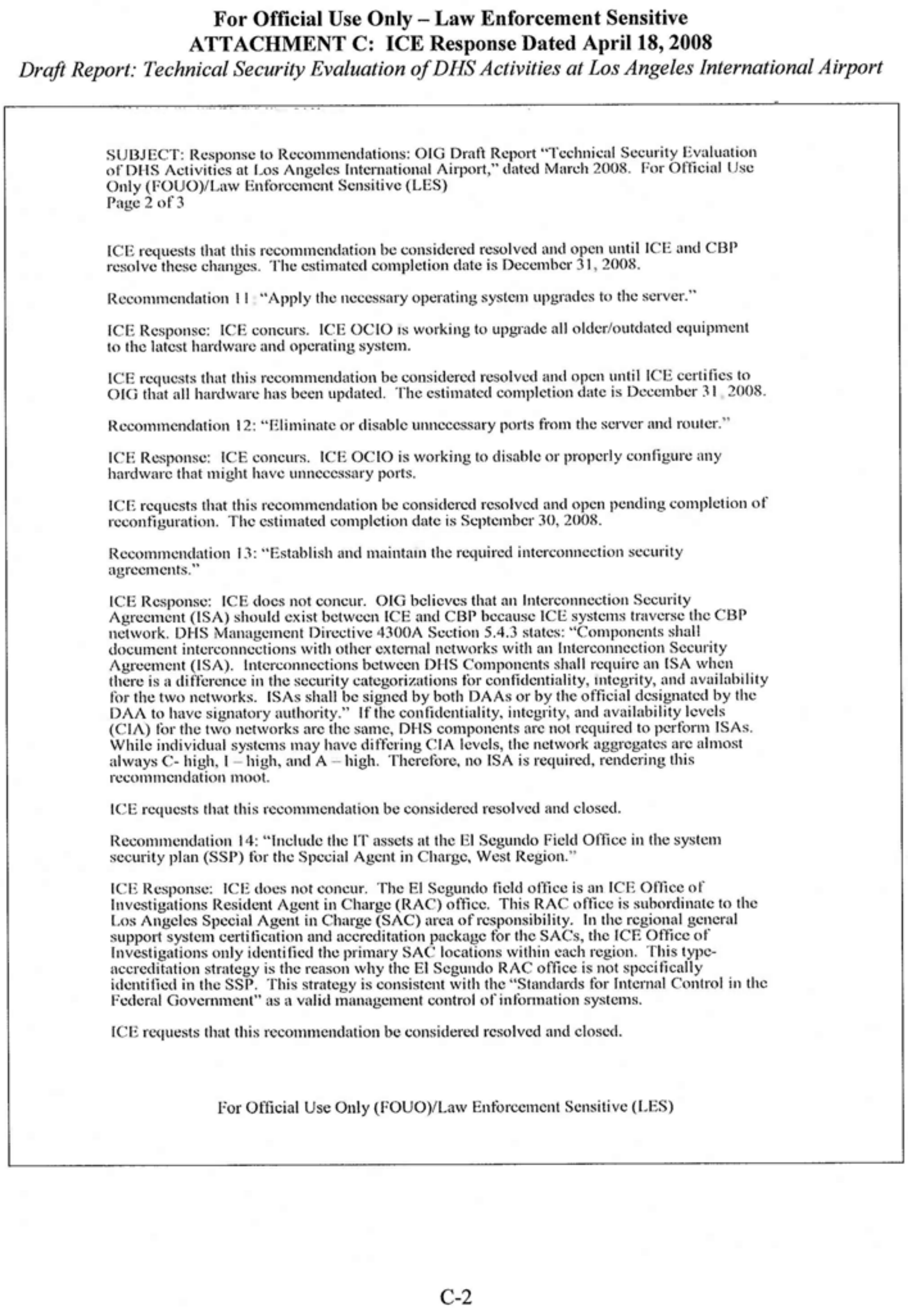
Recommendation 9: "Provide an adequate HVAC system for the server room or obtain a waiver from the DAA."

ICE Response: ICE concurs. As part of the requirement for new office space, ICE has requested that GSA identify and acquire a facility with sufficient HVAC capacity to meet the DAA standard.

ICE requests that this recommendation be considered resolved and closed.

Recommendation 10: "Use a connection protocol that employs secure authentication."

ICE Response: ICE concurs. As the network connectivity for this site is part of the U.S. Customs and Border Protection (CBP) network, the CBP OCIO controls the router and switch configurations and management protocols. ICE will coordinate with CBP OCIO to address the changes required to support connection protocols that allow for stronger authentication.



For Official Use Only – Law Enforcement Sensitive

ATTACHMENT C: ICE Response Dated April 18, 2008

Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

SUBJECT: Response to Recommendations: OIG Draft Report "Technical Security Evaluation of DHS Activities at Los Angeles International Airport," dated March 2008. For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)
Page 2 of 3

ICE requests that this recommendation be considered resolved and open until ICE and CBP resolve these changes. The estimated completion date is December 31, 2008.

Recommendation 11: "Apply the necessary operating system upgrades to the server."

ICE Response: ICE concurs. ICE OCIO is working to upgrade all older/outdated equipment to the latest hardware and operating system.

ICE requests that this recommendation be considered resolved and open until ICE certifies to OIG that all hardware has been updated. The estimated completion date is December 31, 2008.

Recommendation 12: "Eliminate or disable unnecessary ports from the server and router."

ICE Response: ICE concurs. ICE OCIO is working to disable or properly configure any hardware that might have unnecessary ports.

ICE requests that this recommendation be considered resolved and open pending completion of reconfiguration. The estimated completion date is September 30, 2008.

Recommendation 13: "Establish and maintain the required interconnection security agreements."

ICE Response: ICE does not concur. OIG believes that an Interconnection Security Agreement (ISA) should exist between ICE and CBP because ICE systems traverse the CBP network. DHS Management Directive 4300A Section 5.4.3 states: "Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority." If the confidentiality, integrity, and availability levels (CIA) for the two networks are the same, DHS components are not required to perform ISAs. While individual systems may have differing CIA levels, the network aggregates are almost always C- high, I – high, and A – high. Therefore, no ISA is required, rendering this recommendation moot.

ICE requests that this recommendation be considered resolved and closed.

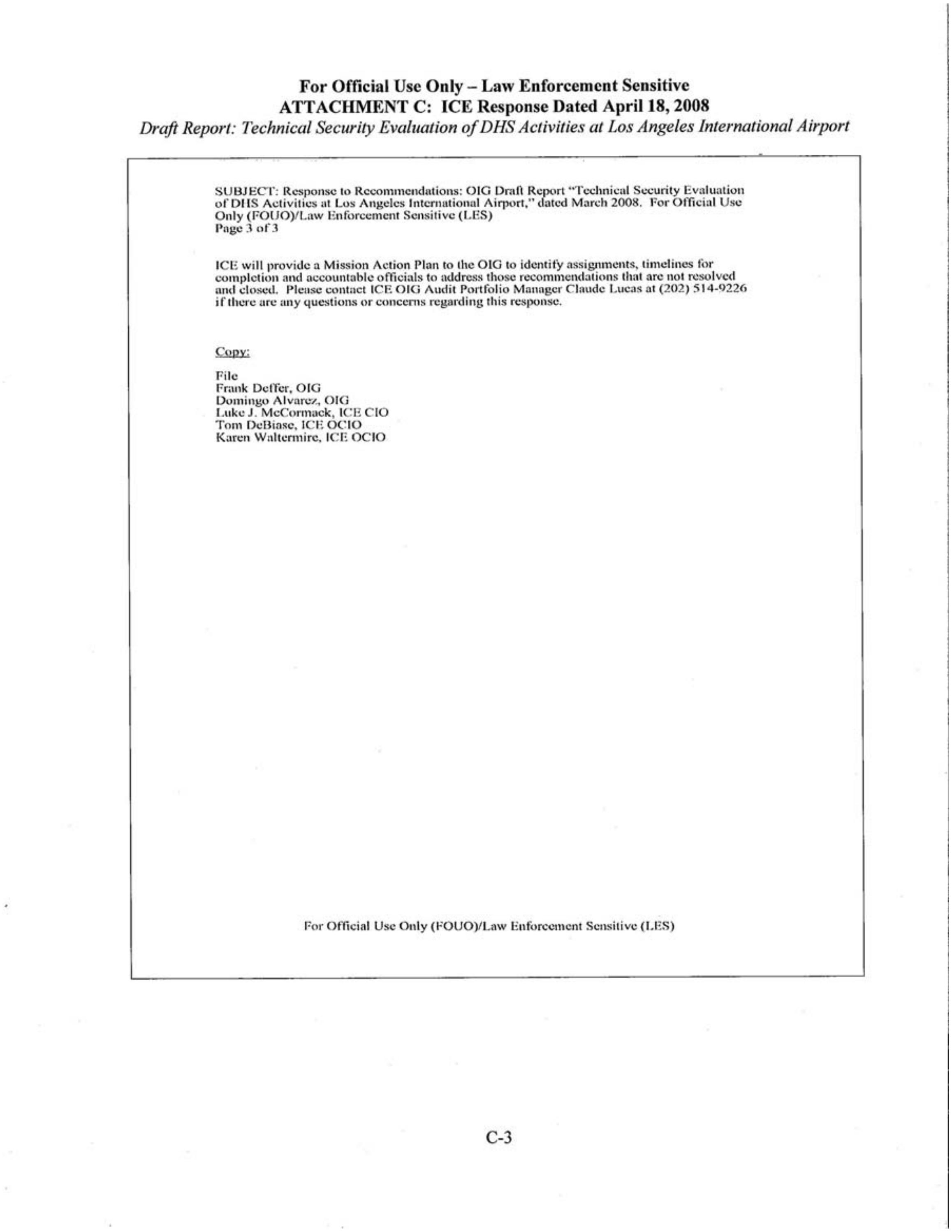
Recommendation 14: "Include the IT assets at the El Segundo Field Office in the system security plan (SSP) for the Special Agent in Charge, West Region."

ICE Response: ICE does not concur. The El Segundo field office is an ICE Office of Investigations Resident Agent in Charge (RAC) office. This RAC office is subordinate to the Los Angeles Special Agent in Charge (SAC) area of responsibility. In the regional general support system certification and accreditation package for the SACs, the ICE Office of Investigations only identified the primary SAC locations within each region. This type-accreditation strategy is the reason why the El Segundo RAC office is not specifically identified in the SSP. This strategy is consistent with the "Standards for Internal Control in the Federal Government" as a valid management control of information systems.

ICE requests that this recommendation be considered resolved and closed.

For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)

C-2



For Official Use Only – Law Enforcement Sensitive
ATTACHMENT C: ICE Response Dated April 18, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

SUBJECT: Response to Recommendations: OIG Draft Report "Technical Security Evaluation of DHS Activities at Los Angeles International Airport," dated March 2008. For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)
Page 3 of 3

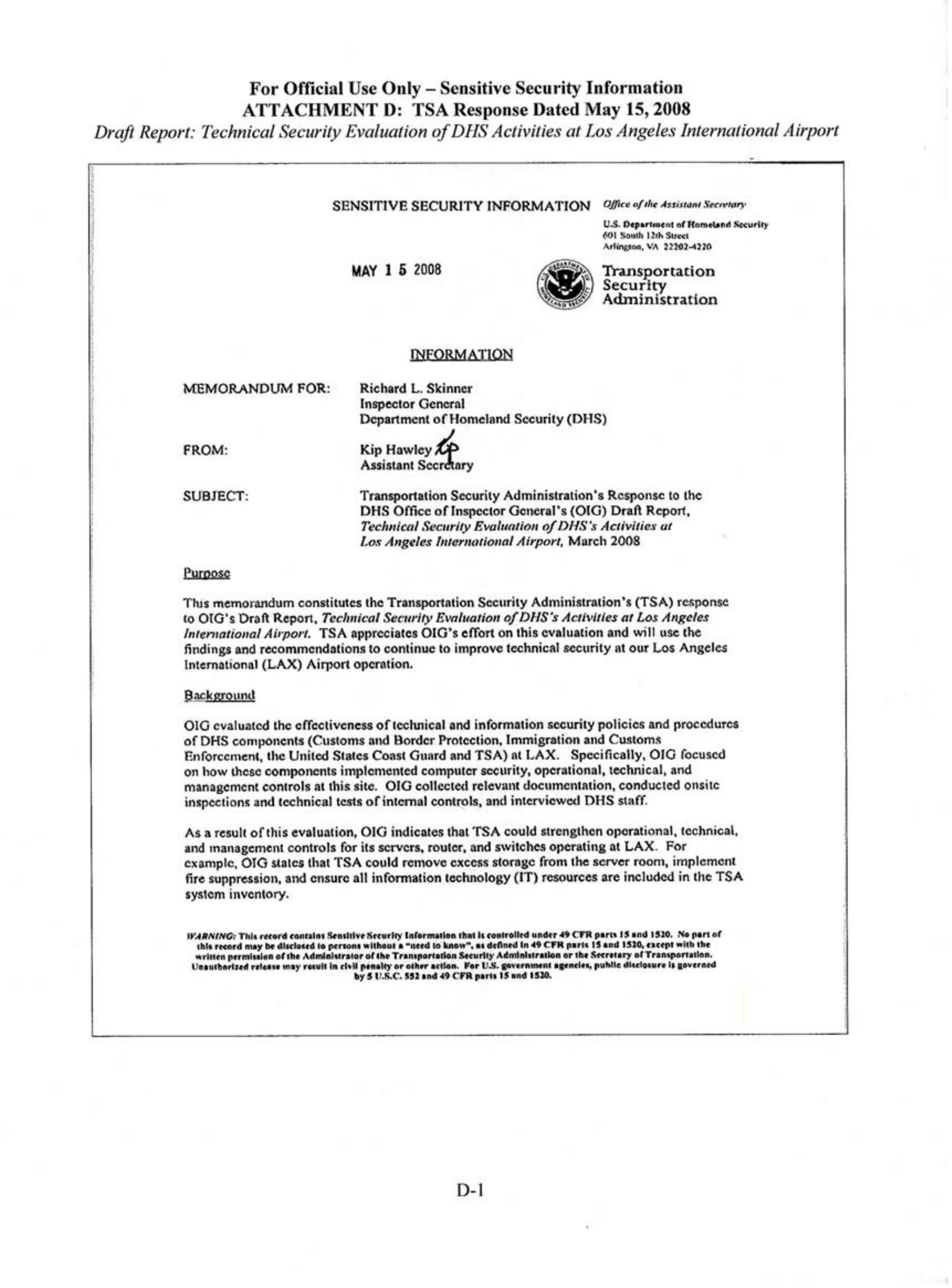
ICE will provide a Mission Action Plan to the OIG to identify assignments, timelines for completion and accountable officials to address those recommendations that are not resolved and closed. Please contact ICE OIG Audit Portfolio Manager Claude Lucas at (202) 514-9226 if there are any questions or concerns regarding this response.

Copy:

File
Frank Deffer, OIG
Domingo Alvarez, OIG
Luke J. McCormack, ICE CIO
Tom DeBiase, ICE OCIO
Karen Waltermire, ICE OCIO

For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)

C-3



For Official Use Only – Sensitive Security Information
ATTACHMENT D: TSA Response Dated May 15, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

SENSITIVE SECURITY INFORMATION

Office of the Assistant Secretary

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

MAY 1 5 2008

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 Response to the DHS Office of Inspector General's (OIG) Draft Report, *Technical Security Evaluation of DHS's Activities at Los Angeles International Airport*, March 2008

Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) response to OIG's Draft Report, *Technical Security Evaluation of DHS's Activities at Los Angeles 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 Los Angeles International (LAX) Airport operation.

Background

OIG evaluated the effectiveness of technical and information security policies and procedures of DHS components (Customs and Border Protection, Immigration and Customs Enforcement, the United States Coast Guard and TSA) at LAX. Specifically, OIG focused on how these components implemented computer security, operational, technical, and management controls at this site. OIG collected relevant documentation, conducted onsite inspections and technical tests of internal controls, and interviewed DHS staff.

As a result of this evaluation, OIG indicates that TSA could strengthen operational, technical, and management controls for its servers, router, and switches operating at LAX. For example, OIG states that TSA could remove excess storage from the server room, implement fire suppression, and ensure all information technology (IT) resources are included in the TSA system inventory.

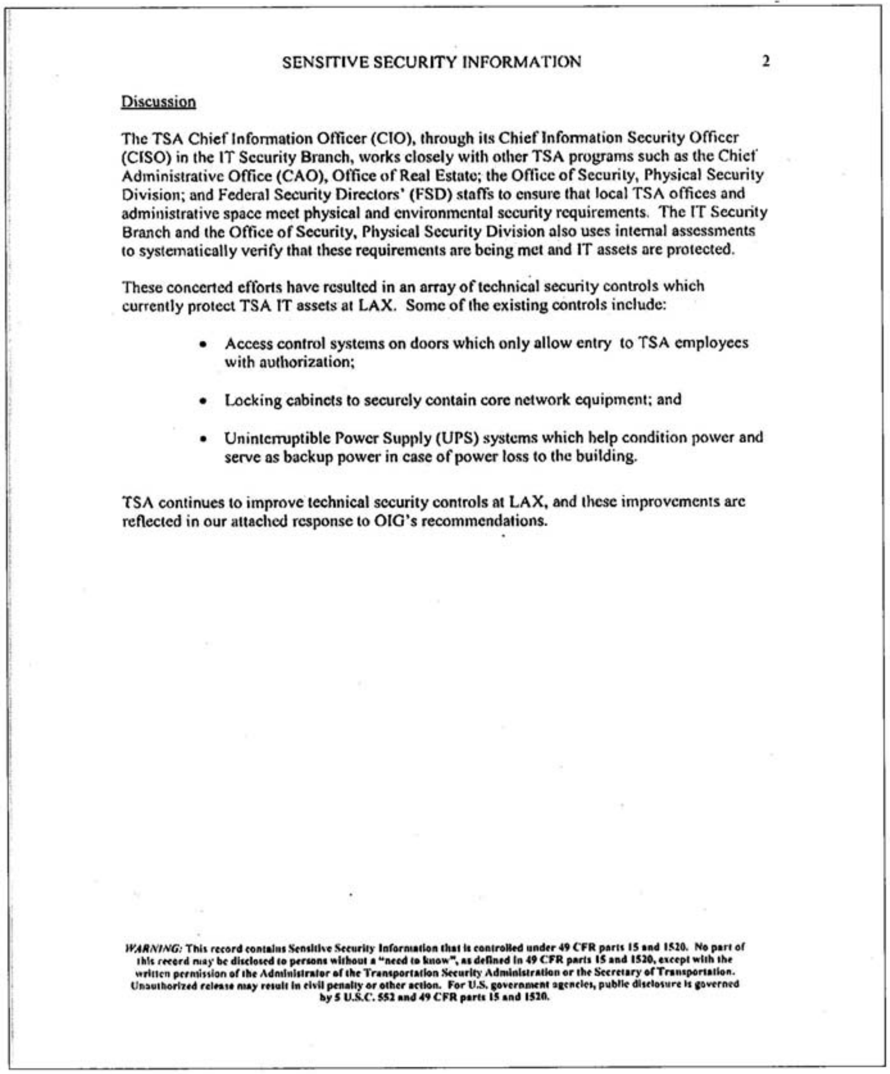
WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

D-1

For Official Use Only – Sensitive Security Information

ATTACHMENT D: TSA Response Dated May 15, 2008

Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport



Discussion

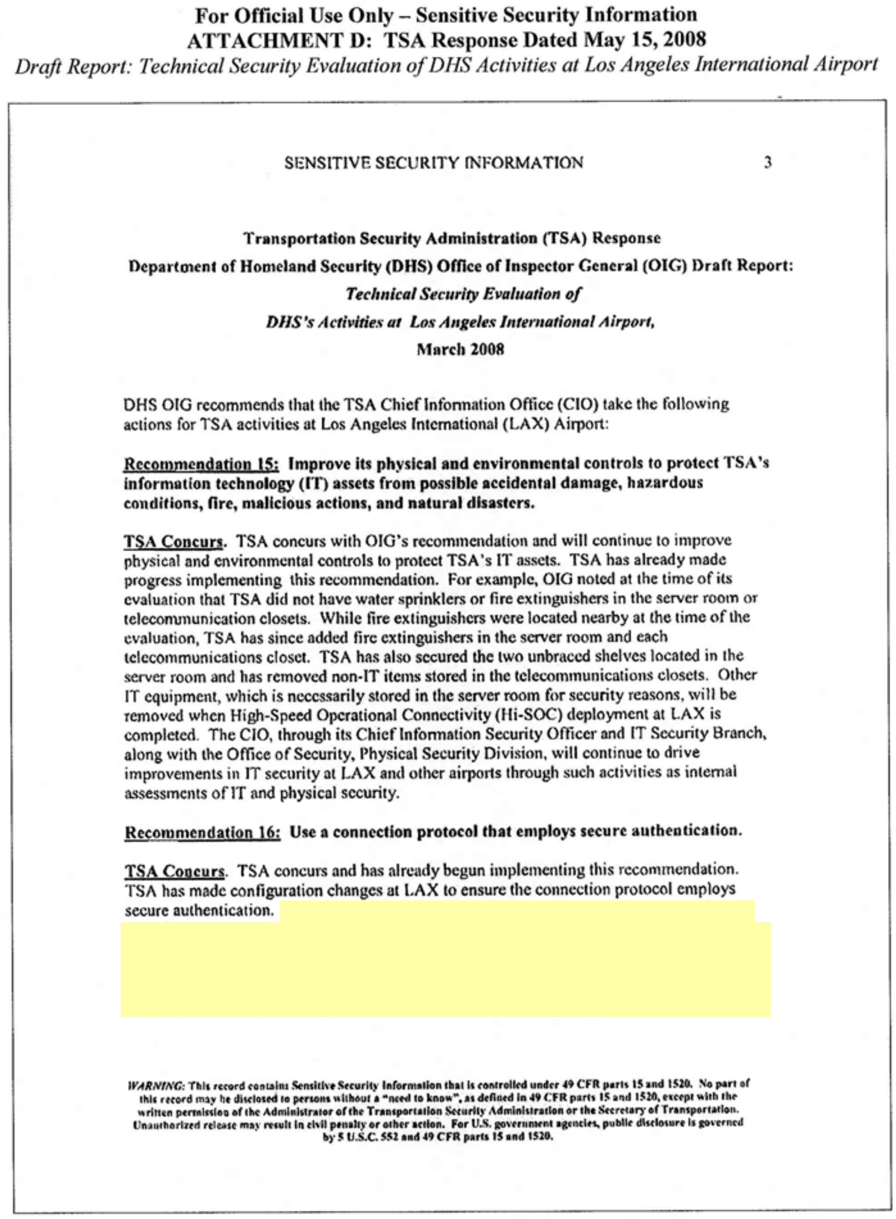
The TSA Chief Information Officer (CIO), through its Chief Information Security Officer (CISO) in the IT Security Branch, works closely with other TSA programs such as the Chief Administrative Office (CAO), Office of Real Estate; the Office of Security, Physical Security Division; and Federal Security Directors' (FSD) staffs to ensure that local TSA offices and administrative space meet physical and environmental security requirements. The IT Security Branch and the Office of Security, Physical Security Division also uses internal assessments to systematically verify that these requirements are being met and IT assets are protected.

These concerted efforts have resulted in an array of technical security controls which currently protect TSA IT assets at LAX. Some of the existing controls include:

- Access control systems on doors which only allow entry to TSA employees with authorization;
- Locking cabinets to securely contain core network equipment; and
- Uninterruptible Power Supply (UPS) systems which help condition power and serve as backup power in case of power loss to the building.

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

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



Transportation Security Administration (TSA) Response
Department of Homeland Security (DHS) Office of Inspector General (OIG) Draft Report:
Technical Security Evaluation of
DHS's Activities at Los Angeles International Airport,
March 2008

DHS OIG recommends that the TSA Chief Information Office (CIO) take the following actions for TSA activities at Los Angeles International (LAX) Airport:

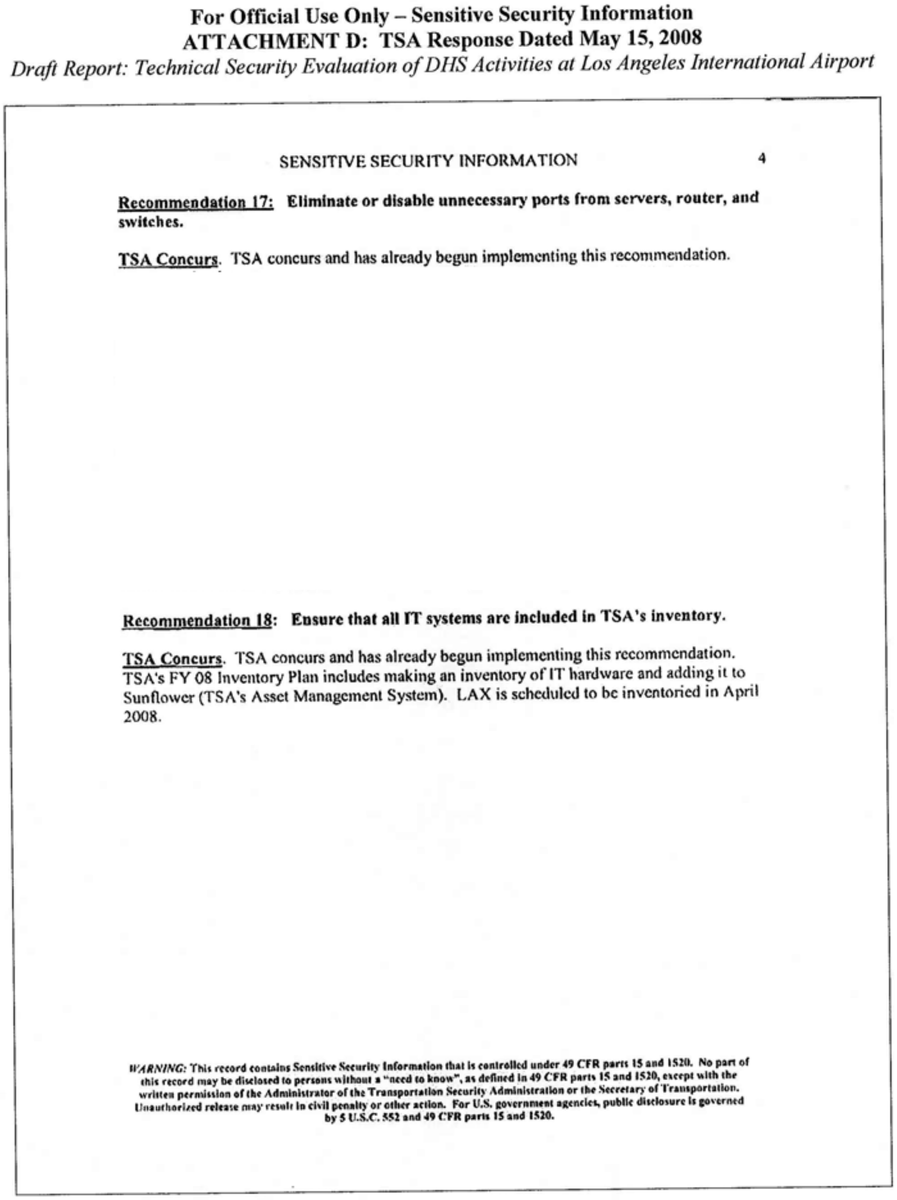
Recommendation 15: Improve its physical and environmental controls to protect TSA's information technology (IT) assets from possible accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

TSA Concurs. TSA concurs with OIG's recommendation and will continue to improve physical and environmental controls to protect TSA's IT assets. TSA has already made progress implementing this recommendation. For example, OIG noted at the time of its evaluation that TSA did not have water sprinklers or fire extinguishers in the server room or telecommunication closets. While fire extinguishers were located nearby at the time of the evaluation, TSA has since added fire extinguishers in the server room and each telecommunications closet. TSA has also secured the two unbraced shelves located in the server room and has removed non-IT items stored in the telecommunications closets. Other IT equipment, which is necessarily stored in the server room for security reasons, will be removed when High-Speed Operational Connectivity (Hi-SOC) deployment at LAX is completed. The CIO, through its Chief Information Security Officer and IT Security Branch, along with the Office of Security, Physical Security Division, will continue to drive improvements in IT security at LAX and other airports through such activities as internal assessments of IT and physical security.

Recommendation 16: Use a connection protocol that employs secure authentication.

TSA Concurs. TSA concurs and has already begun implementing this recommendation. TSA has made configuration changes at LAX to ensure the connection protocol employs secure authentication. [redacted]

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**



For Official Use Only – Sensitive Security Information
ATTACHMENT D: TSA Response Dated May 15, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

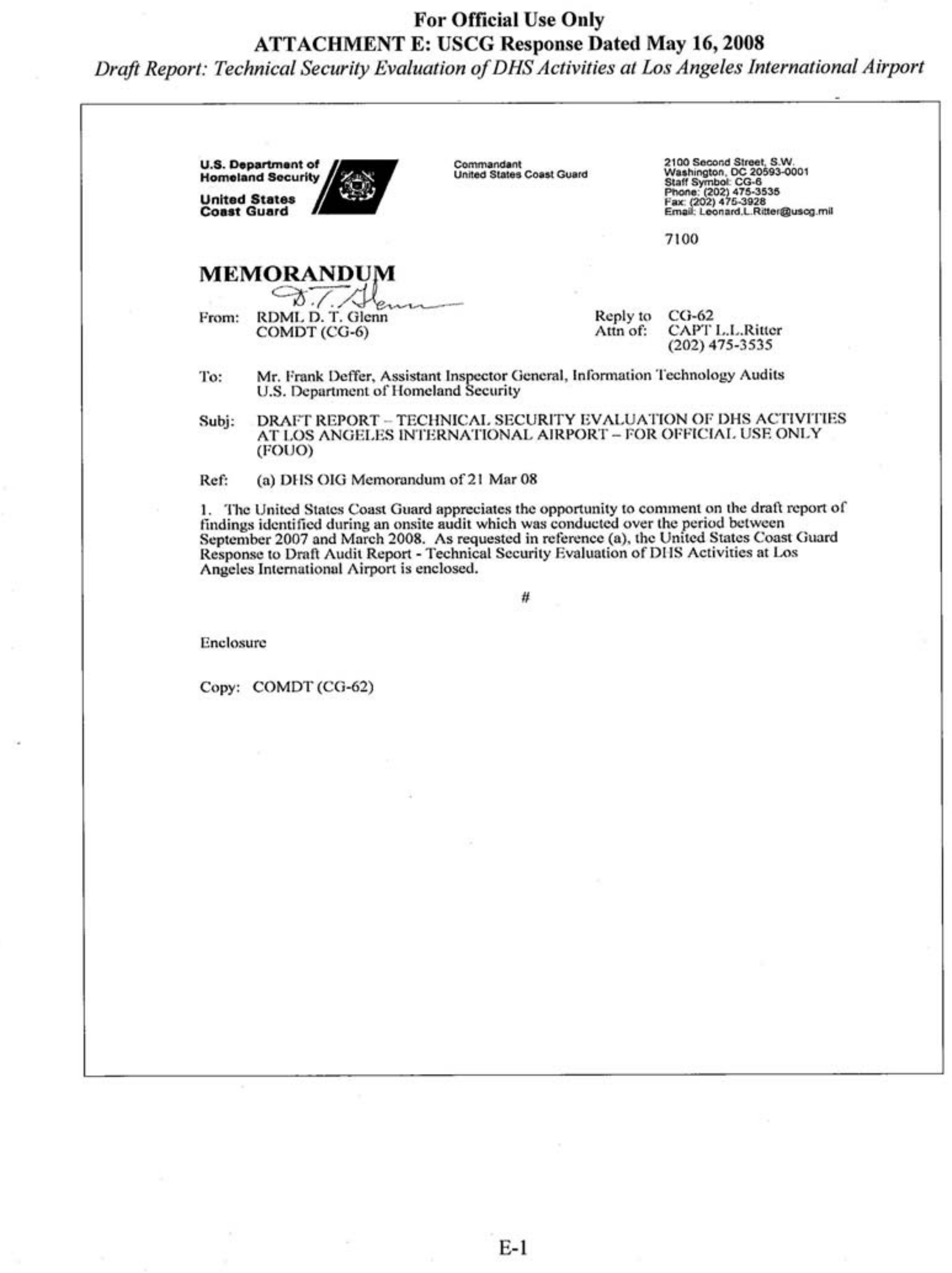
<u>Recommendation 17:</u> Eliminate or disable unnecessary ports from servers, router, and switches.

<u>TSA Concurs</u>. TSA concurs and has already begun implementing this recommendation.

<u>Recommendation 18</u>: Ensure that all IT systems are included in TSA's inventory.

<u>TSA Concurs</u>. TSA concurs and has already begun implementing this recommendation. TSA's FY 08 Inventory Plan includes making an inventory of IT hardware and adding it to Sunflower (TSA's Asset Management System). LAX is scheduled to be inventoried in April 2008.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



For Official Use Only
ATTACHMENT E: USCG Response Dated May 16, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

U.S. Department of
Homeland Security
United States
Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-6
Phone: (202) 475-3535
Fax: (202) 475-3928
Email: Leonard.L.Ritter@uscg.mil

7100

MEMORANDUM

D.T. Glenn

From: RDML D. T. Glenn
COMDT (CG-6)

Reply to Attn of: CG-62
CAPT L.L.Ritter
(202) 475-3535

To: Mr. Frank Deffer, Assistant Inspector General, Information Technology Audits
U.S. Department of Homeland Security

Subj: DRAFT REPORT – TECHNICAL SECURITY EVALUATION OF DHS ACTIVITIES AT LOS ANGELES INTERNATIONAL AIRPORT – FOR OFFICIAL USE ONLY (FOUO)

Ref: (a) DHS OIG Memorandum of 21 Mar 08

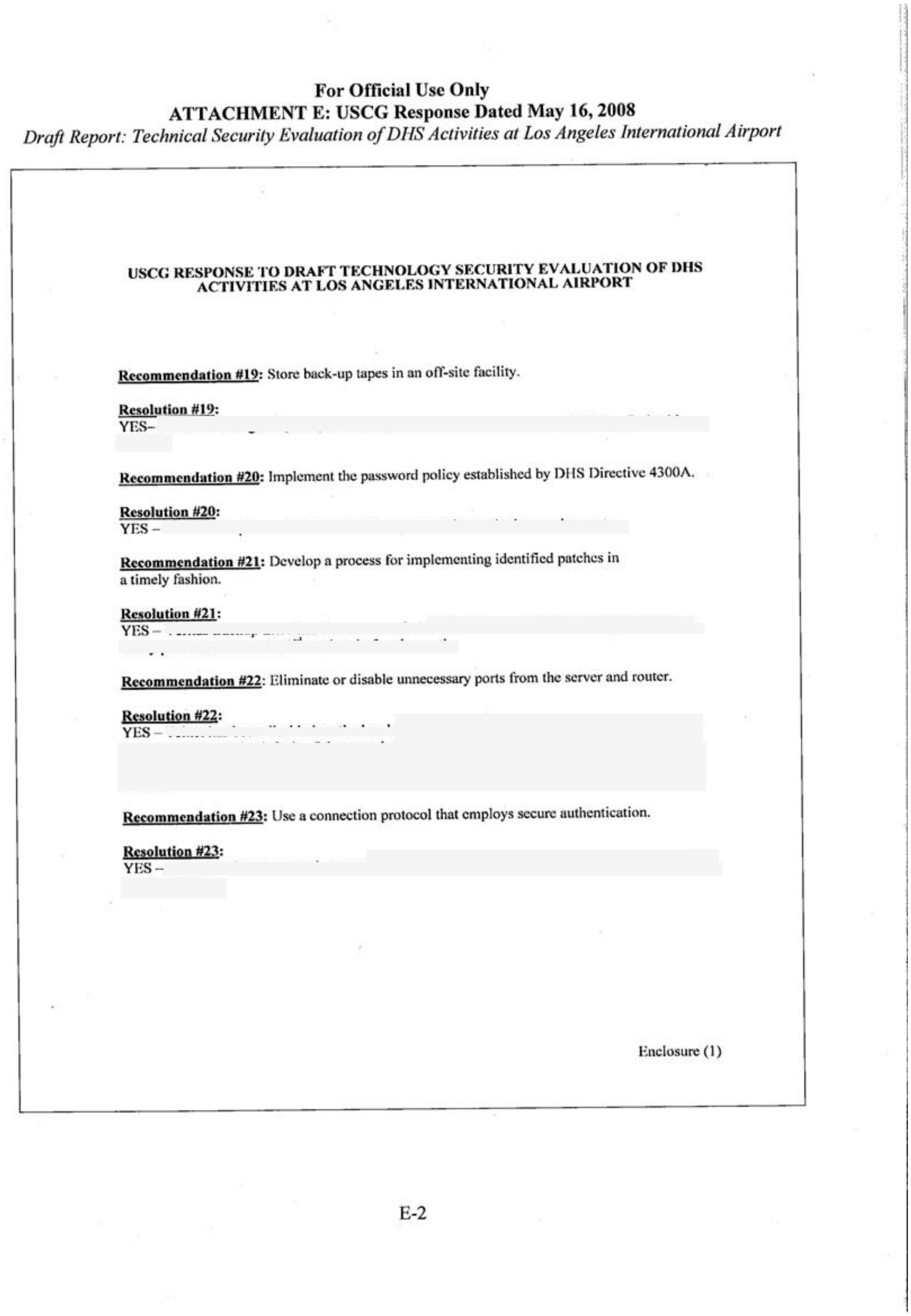
1. The United States Coast Guard appreciates the opportunity to comment on the draft report of findings identified during an onsite audit which was conducted over the period between September 2007 and March 2008. As requested in reference (a), the United States Coast Guard Response to Draft Audit Report - Technical Security Evaluation of DHS Activities at Los Angeles International Airport is enclosed.

#

Enclosure

Copy: COMDT (CG-62)

E-1



For Official Use Only
ATTACHMENT E: USCG Response Dated May 16, 2008
Draft Report: Technical Security Evaluation of DHS Activities at Los Angeles International Airport

USCG RESPONSE TO DRAFT TECHNOLOGY SECURITY EVALUATION OF DHS ACTIVITIES AT LOS ANGELES INTERNATIONAL AIRPORT

Recommendation #19: Store back-up tapes in an off-site facility.

Resolution #19:
YES– [redacted]

Recommendation #20: Implement the password policy established by DHS Directive 4300A.

Resolution #20:
YES – [redacted]

Recommendation #21: Develop a process for implementing identified patches in a timely fashion.

Resolution #21:
YES – [redacted]

Recommendation #22: Eliminate or disable unnecessary ports from the server and router.

Resolution #22:
YES – [redacted]

Recommendation #23: Use a connection protocol that employs secure authentication.

Resolution #23:
YES – [redacted]

Enclosure (1)

E-2

Appendix C
Major Contributors to This Report

Roger Dressler, Director, Department of Homeland Security, Information Technology Audits

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

Domingo Alvarez, Senior Auditor, Department of Homeland Security, Information Technology Audits

Ernie Bender, Senior Auditor, Department of Homeland Security, Information Technology Audits

Karen Nelson, Senior Auditor, Department of Homeland Security, Information Technology Audits

Matthew Worner, Program Analyst, Department of Homeland Security, Information Technology Audits

Syrita Morgan, Management and Program Assistant, Department of Homeland Security, Information Technology Audits

Richard Saunders, Director, Department of Homeland Security, Advanced Technology Division

Steve Matthews, Manager, Department of Homeland Security, Advanced Technology Division

Jeffrey Devine, Technical Evaluator, Department of Homeland Security, Advanced Technology Division

Sukhonthip Rueangvivatanakij, Technical Evaluator, Department of Homeland Security, Advanced Technology Division

Shannon Frenyea, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Under Secretary, Management
Assistant Secretary, Office of Policy
Assistant Secretary, Office of Public Affairs
Assistant Secretary, Office of Legislative Affairs
Chief Information Officer (CIO), DHS
Chief Privacy Officer
Deputy CIO, DHS
Chief Information Security Officer, DHS
Chief Information Security Officer, CBP
Chief Information Security Officer, ICE
Chief Information Security Officer, TSA
Chief Information Security Officer, USCG
Information Systems Security Manager, CBP
Information Systems Security Manager, ICE
Information Systems Security Manager, TSA
Information Systems Security Manager, USCG
DHS Audit Liaison
CBP Audit Liaison
ICE Audit Liaison
TSA Audit Liaison
USCG Audit Liaison

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.