Department of Homeland Security
Office of Inspector General

Technical Security Evaluation of DHS Components at O'Hare Airport (Redacted)

OIG-12-45

March 2012

Office of Inspector General

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

March 6, 2012

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 the strengths and weaknesses of the information security controls implemented by U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Transportation Security Administration based on guidance provided by the Office of the Chief Information Officer. 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 of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

BIA	Business Impact Assessment
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
DHS	Department of Homeland Security
DHS Directive 4300A	*DHS Sensitive Systems Policy Directive 4300A*
DHS 4300A Handbook	*DHS 4300A Sensitive Systems Handbook*
DVD	Digital Video Disc
FIPS Federal	Information Processing Standards Publication
GAO	U.S. Government Accountability Office
GSS	general support system
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
LAN	local area network
MEF	mission essential functions
NII Systems	Non-Intrusive Inspection Systems
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General

OneNet	DHS One Network
ORD	Chicago O’Hare International Airport
PALS	Portable Automated Lookup System
PIA	Privacy Impact Assessment
POE	port of entry
PTA	Privacy Threshold Analysis
RAC	Resident Agent in Charge
SAC	Special Agent in Charge
SP	Special Publication
STIP	Security Technology Integrated Program
TSA	Transportation Security Administration
TSANet	Transportation Security Administration Network
TSE	transportation security equipment
WAN	wide area network

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 Chicago O'Hare International Airport. U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Transportation Security Administration operate information technology systems that support homeland security operations at this airport.

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

The information technology security controls implemented at these sites have deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' information technology systems. Specifically, these components need to improve their physical security and environmental controls for telecommunications equipment and servers. These components also need to improve their management controls by upgrading system information to document security controls more fully.

Background

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security (DHS) officials with timely information on whether they had properly implemented DHS information technology (IT) security policies at critical sites. Our program is based on *DHS Sensitive Systems Policy Directive 4300A*, version 8.0 (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 nonrepudiation within the DHS IT infrastructure and operations. A companion document, the *DHS 4300A Sensitive Systems Handbook*, version 7.2.1.1 (DHS 4300A Handbook), provides detailed guidance on the implementation of these policies. For example, according to the DHS 4300A Handbook,

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

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

- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. These controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.

- **Technical Controls** – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations and support security requirements for applications and data.

[1] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems.*

- **Management Controls** – Focus on managing both the system information security controls and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.

Our evaluation focused on U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA), which have activities at Chicago O'Hare International Airport (ORD) and rely on a range of IT assets to support their respective missions. As a Category X airport, ORD is one of the airports with the largest number of enplanements, processing approximately 67 million passengers in 2010.[2]

At ORD, 255 CBP Officers and Agricultural Specialists staff 68 primary passenger lanes, review flight data for terrorist-related activities, and process fines and civil penalties. Additionally, 200 CBP staff at nearby locations use IT assets to perform cargo manifest review and targeting, outbound passenger review and targeting, and inbound mail processing.

The following CBP locations were reviewed:

- ORD Terminal 5
- ORD International Mail Branch
- Port Office, Rosemont, IL
- Management Inspection Division and the Office of Professional Responsibility, Rosemont, IL

CBP staff at these locations use the following systems:

- The Central Field Local Area Network (LAN). This system provides the general support network infrastructure for the CBP end-users' electronic communication for the performance of their daily official duties.

- The DHS One Network (OneNet). The DHS OneNet is a general support system (GSS) providing all wide area network communications for the servicewide DHS sensitive but unclassified environment.

[2] 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.

- Global Entry. The Global Entry program benefits preapproved, low-risk air travelers by allowing them to avoid passport control lines through the use of the automated self-service Global Entry kiosk to clear customs, immigration, and agriculture. The Global Entry program also benefits CBP and participating foreign governments by allowing them to focus their efforts on unknown and potentially higher risk air travelers, thereby facilitating the movement of people more efficiently and effectively, while serving as a force multiplier for CBP.

- Non-Intrusive Inspection (NII) Systems. NII Systems enable CBP to perform more effective and efficient nonintrusive inspections and screenings of cars, trucks, railcars, sea containers, personal luggage, packages, parcels, and flat mail. NII Systems are designed to detect illicit goods, such as drugs, money, guns, ammunition, agricultural items, and explosives; and chemical, biological, and nuclear agents.

- TECS.[3] TECS supports enforcement and inspection operations for several components of DHS and is a vital tool for the law enforcement and intelligence communities at the local, state, tribal, and federal government levels. TECS comprises several subsystems that include enforcement, inspection, and intelligence records relevant to the antiterrorist and law enforcement mission of CBP and the other federal agencies it supports.

ICE's office of the Resident Agent in Charge (RAC) identifies and investigates security issues with a foreign nexus at ORD. The RAC's areas of responsibility at ORD include the following:

- Investigations of internal criminal conspiracies involving employees of companies doing business at ORD
- Identification, interdiction, and apprehension of currency smugglers from ORD
- Enforcement activities on internal drug-smuggling carriers arriving at ORD
- Enforcement actions that center on the interception of parcels containing illegal narcotics and initiation of controlled deliveries on these parcels if appropriate

[3] Prior to the government realignment, TECS was owned by the U.S. Department of Treasury, U.S. Customs Service, and operated under the name Treasury Enforcement Communication System. In 2008, the application was renamed "TECS" to eliminate the association with the U.S. Department of Treasury.

- Investigations of illegal workers having unescorted access to secure areas of the airport
- Investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack, or exploitation

The following ICE locations were reviewed:

- Resident Agent in Charge, Des Plaines, IL
- Management Inspection Division and the Office of Professional Responsibility, Rosemont, IL

ICE staff use the Special Agent in Charge (SAC) Midwest GSS. The SAC Midwest GSS supports the ICE Office of Investigations mission by providing access to law enforcement data processing resources available through DHS OneNet. Interconnectivity with DHS OneNet further enhances the mission support capabilities of the SAC GSS by allowing users remote access through secure virtual private networking and access to the public Internet. Local data processing resources directly supported by the SAC Midwest GSS are file sharing and print services.

TSA's activities include screening passengers and baggage on all departing flights at ORD. To support these activities, TSA has operations in each of the terminals at ORD, as well as at a nearby office building.

The following TSA locations were reviewed:

- ORD Terminals 1, 2, 3, and 5
- Office of the Federal Security Director, Rosemont, IL

TSA staff at these locations use the following systems:

- End User Computing. This system provides TSA employees and contractors with desktops, laptops, local printers, and other end user computing applications at the various DHS/TSA locations and sponsored sites.

- Infrastructure Core System. This system provides core services, including file and print services, to the entire TSA user community.

- The Security Technology Integrated Program (STIP). The STIP combines many different types of components, including transportation security equipment (TSE), servers and storage, software/application products, and databases. A user physically accesses the TSE to perform screening or other administrative functions.

- The Transportation Security Administration Network (TSANet). Owing to its geographically dispersed topology, the TSANet GSS is considered a wide area network (WAN). The TSANet GSS consists of the WAN backbone and LAN at each site that connects to the backbone. The TSANet GSS provides connectivity for airports and their users.

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 ORD. For example, CBP could improve environmental controls and the placement of telecommunications equipment. CBP also should scan [redacted] periodically to identify vulnerabilities. Additionally, CBP should update ORD systems documentation in the areas of security categorization, privacy compliance, and business impact analysis. Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at ORD.

Operational Controls

Onsite implementation of operational controls that did not conform fully to DHS policies included inadequate temperature and humidity controls and the inappropriate placement of IT equipment. Additionally, onsite IT assets may be insufficient to ensure continuity of CBP operations at ORD.

Environmental Controls

In three of the five CBP server rooms at ORD, the temperature was higher and the humidity was lower than recommended by the DHS 4300A Handbook. In addition, several of the server rooms and wire closets did not contain temperature or humidity sensors.

According to the DHS 4300A Handbook,

> The following should be considered when developing a strategy for temperature and humidity control:
>
> - Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit. Most systems will continue to function when temperatures go beyond this range, but the associated risk to data is increased. (Check individual system documentation for the proper levels.)
>
> - Humidity should be at a level between 35 percent and 65 percent. Most systems will continue to function when humidity goes beyond this range, but the

> associated risk to data is increased. (Check individual system documentation for the proper levels.)

CBP needs to better monitor and control the humidity and temperature in its server rooms at ORD. Low humidity can result in static, and high temperatures can damage sensitive elements of computer systems.

Inappropriate Placement of Telecommunications Equipment

Telecommunications equipment, including racks, cables, and network switches, connects IT resources to a LAN. In two locations at ORD, CBP has placed telecommunications equipment in rooms containing water heaters (see figure 1). If these water heaters malfunction, there is a risk that CBP's telecommunications equipment could suffer water damage, preventing users from accessing the IT resources they need to perform their mission.

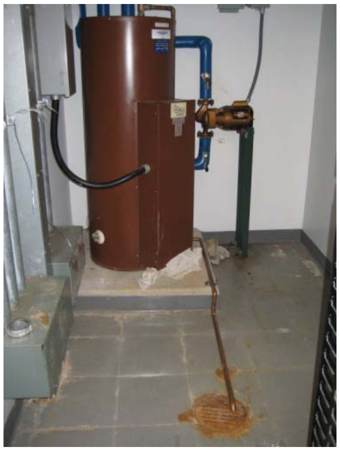


Figure 1: Water heater in room with CBP telecommunications rack.

At another location at ORD, CBP has placed telecommunications equipment in a supply room/office. At this location, there are no barriers protecting the telecommunications equipment. There is a risk that CBP telecommunications equipment could be damaged when supplies are moved into or out of this room.

According to DHS Directive 4300A,

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

CBP's computer infrastructure may deteriorate under adverse environmental conditions, preventing access to automated systems that are necessary for staff to perform their mission.

Redundant Telecommunications Services

In May 2008, we reported that a single point of failure contributed to a network outage at Los Angeles International Airport.[4] We also recommended that CBP determine whether actions taken to reduce the potential for a network outage should also be performed at other locations. In response, CBP established the Systems Availability Project to implement corrective actions at other CBP ports of entry (POEs).

The Systems Availability Project included providing redundant communications, power, and computing capabilities at field locations and central data center facilities. The Systems Availability Project established redundant telecommunications services for a prioritized list of [redacted]

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

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

[4] *Lessons Learned from the August 11, 2007 Network Outage at Los Angeles International Airport* (OIG-08-58), May 2008.

> Risk – NIST 800-53 allows for downgrading this security control for availability. This is appropriate when (1) the availability impact level is upgraded to meet the "high water mark" process, (2) supported by an organizational risk assessment, [and] (3) does not impact the security relevant information at the system level.

CBP should conduct a risk assessment to determine whether redundant telecommunications services would be appropriate for staff at these three locations.

Business Continuity

Airport authorities have contingency plans in place to deal with power outages, including diverting flights to reduce the burden on passengers and the airport's infrastructure. CBP's business continuity plan for dealing with power outages at ORD includes the use of 18 laptops that contain the Portable Automated Lookout System (PALS).[5] However, the 18 PALS laptops may not be sufficient to process passengers through the 68 passenger processing lanes at ORD during an extended power outage. Since the PALS laptops have a battery life of only 2 hours, CBP may not be able to process all incoming passengers during a power outage before the laptops lose battery power.

According to the DHS 4300A Handbook,

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

CBP staff at ORD proposed, as an interim solution, the purchase of additional long-life batteries.

Technical Controls

In October 2008, we reported that CBP was not regularly scanning [redacted]

[5] PALS is a contingency system used when CBP Inspection Officers do not have connectivity to TECS. PALS utilizes extracts of the TECS database, which identifies individuals who should be denied entry.
[6] *Technical Security Evaluation of DHS Activities at Los Angeles International Airport* (OIG-09-01), October 2008.

CBP will continue migrating users from [redacted] through the end of fiscal year 2011. CBP's plans to address [redacted] are dependent on funding, and the schedule has not yet been determined.

According to the DHS 4300A Handbook,

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

CBP must be able to scan its systems periodically to identify vulnerabilities, and then take corrective actions to reduce these vulnerabilities.

Management Controls

CBP's implementation of management controls for systems operating at ORD did not conform fully to DHS policies. Specifically, CBP could improve the documentation for these systems in the areas of security categorization, privacy compliance, and business impact analysis.

System Security Categorization

CBP has assessed the Central Field LAN's security categorization as moderate for confidentiality, integrity, and availability. However, CBP staff use the Central Field LAN to perform border and transportation security activities. DHS guidance recommends that systems that are used for border and transportation security activities have a high security categorization.

For example, the DHS *FIPS 199 Workbook*, version 8, includes the following descriptions for the border and transportation security integrity impact levels:

> Unauthorized modification or destruction of information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States may seriously affect mission operations or result in the loss of human life. Unauthorized modification or destruction of information affecting antiterrorism information may adversely affect mission operations in a manner that results in unacceptable damage

> to critical infrastructures and/or key national assets or loss of key national assets and/or human life. Consequently, the integrity impact level associated with information that ensures the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is **high**.

Systems that have a high security categorization must have additional security controls. If CBP does not accurately assess the security categorization of the Central Field LAN, appropriate information security controls may not be established for the system.

Additionally, CBP may not have included all of the business activities for which the Central Field LAN is used. Specifically, according to the *FIPS 199 Workbook*, CBP staff use the Central Field LAN information to perform the following two DHS business activities:

- Border and Transportation Security/Verify Identity
- IT Infrastructure Maintenance/Maintain IT Networks

However, CBP staff also use the Central Field LAN to access information in TECS and PALS to identify individuals who should be denied entry. It is our opinion that the DHS law enforcement Business Activity/Function field, *Criminal Apprehension/Detain Person*, should also be identified as an activity of the Central Field LAN. If CBP does not include all the business activities for which the Central Field LAN is used, appropriate information security controls may not be established for the system.

Privacy Compliance

CBP has prepared a Privacy Threshold Analysis (PTA) for the Central Field LAN. This PTA noted that PALS was installed on Central Field LAN servers.[7] In addition, this PTA concluded that no Privacy Impact Assessment (PIA) was required, because the Central Field LAN does not maintain logs or store personally identifiable information. However, this conclusion is incorrect in that PALS, which is installed on the Central Field LAN, utilizes extracts of the TECS database, which identifies individuals who

[7] [redacted]

should be denied entry. Because personally identifiable information is installed on the Central Field LAN, a PIA is needed.

According to DHS' *Privacy Impact Assessments (PIA) Official Guidance*,

> A PIA should be completed for any program, system, technology, or rulemaking that involves personally identifiable information. Personally identifiable information is information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Without identifying whether systems contain personally identifiable information, CBP staff cannot be assured they are addressing all privacy compliance activities.

Business Impact Assessments

Although CBP has prepared a Business Impact Assessment (BIA) for the Central Field LAN, it has not prepared a BIA for the other four systems operating at ORD. According to the DHS 4300A Handbook,

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

The BIA helps to identify and prioritize critical IT systems and components. BIAs are also essential for contingency planning. For example, a BIA would allow CBP to identify maximum tolerable downtime, the resources required to resume mission/business processes, and recovery priorities for system resources.

In response to our requests for the BIAs associated with the identified systems, CBP staff at ORD said that BIAs were required only for Operations.[8] Without performing a BIA, CBP cannot be assured that its backup and recovery plans meet the needs of the

[8] According to NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, "COOP focuses on restoring an organization's *mission essential functions* (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations."

business owners (e.g., recovery time objective and recovery point objective).

Recommendations

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

<u>Recommendation #1</u>: Relocate telecommunications equipment so that the potential for accidental damage is minimized; obtain temperature and humidity sensors, and ensure that server rooms are maintained within DHS' recommended ranges.

<u>Recommendation #2</u>: Explore near- and long-term solutions to its business continuity issues at ORD. Potential solutions would include purchasing additional extended-life laptop batteries, analyzing how many passengers per hour are processed using PALS laptops, and purchasing enough PALS laptops to process ORD passengers within an acceptable timeframe.

<u>Recommendation #3</u>: Determine if it is cost effective to establish redundant telecommunications services at [redacted] identified CBP locations.

<u>Recommendation #4</u>: Perform scans [redacted] periodically to identify vulnerabilities, and then take corrective actions to reduce these vulnerabilities.

<u>Recommendation #5</u>: Update the Central Field LAN's *FIPS 199 Workbook* with all relevant information.

<u>Recommendation #6</u>: Prepare a PIA for the Central Field LAN.

<u>Recommendation #7</u>: Prepare the missing BIAs for the identified CBP systems operating at ORD.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the CBP Assistant Commissioner for Internal Affairs. We have included a copy of the comments in their entirety at appendix B. The CBP Assistant Commissioner concurred with all seven recommendations.

Recommendation 1

In response to recommendation 1, CBP will move two racks, relocate cables, and purchase temperature and humidity sensors. These actions are dependent upon available funding.

OIG Analysis

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

Recommendation 2

[redacted]

OIG Analysis

CBP's actions satisfy the intent of this recommendation. However, CBP needs to address the other issues we raised, including obtaining sufficient resources, such as long-life batteries, to process passengers in a timely manner during an outage. This recommendation is considered resolved, but will remain open until CBP provides documentation to support that the planned corrective actions are completed.

Recommendation 3

In response to recommendation 3, CBP has determined that redundant communications circuits are not needed for locations with fewer than 50 employees. Additionally, according to CBP, it has taken actions at the Port Office to install redundant circuits and will provide evidence to document that this has occurred.

OIG Analysis

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

Recommendation 4

In response to recommendation 4, CBP is routinely performing vulnerability assessment scans of its [redacted] Additionally, CBP is taking actions to decommission and replace these servers.

OIG Analysis

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

Recommendation 5

In response to recommendation 5, CBP has removed PALS data from its Central Field LAN. According to CBP, because the PALS data has been removed, the *FIPS Workbook* data for the Central Field LAN are now accurate. CBP requests that we close this recommendation.

OIG Analysis

We do not agree that CBP has addressed this recommendation in full. The inclusion of PALS data on the Central Field LAN was only one of the reasons to update the *FIPS 199 Workbook*. For example, in this report we also documented that the *FIPS 199 Workbook* may not be accurate as it did not include all activities supported by the Central Field LAN.

[redacted]

Recommendation 5 is considered unresolved and open pending verification that the actions being taken satisfy the intent of this recommendation.

[9] *Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport* (OIG-08-58), May 2008.

Recommendation 6

In response to recommendation 6, CBP has removed PALS data from the Central Field LAN. According to CBP, the only privacy data on the Central Field LAN were contained in PALS. Also, there is no need to perform a PIA for the Central Field LAN if PALS is not installed. CBP requests that we close this recommendation.

OIG Analysis

We do not agree that CBP has addressed this recommendation in full. While the removal of PALS data from the Central Field LAN will eliminate identified privacy data, [redacted]

Recommendation 6 is considered unresolved and open pending an assessment by CBP [redacted]

Recommendation 7

In response to recommendation 7, CBP will perform BIAs for specific systems but not for the DHS OneNet. According to CBP, DHS does not have a policy to perform BIAs for general support systems like the DHS OneNet. The completion date for this recommendation is January 31, 2012.

OIG Analysis

We agree that performing BIAs for the identified systems partially satisfies the intent of this recommendation. We also agree that DHS guidance for performance of BIAs is not clear. However, government-wide guidance for the performance of BIAs is provided by NIST Special Publication (SP) 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*. This document also includes a recommended template for a system-based BIA.

This recommendation is considered unresolved and open until CBP provides documentation to support that the planned corrective actions are completed.

ICE Did Not Comply Fully With DHS Sensitive System Policies

ICE could strengthen operational and management controls for its servers and switches operating at facilities near ORD. For example, ICE could improve environmental controls for these systems. ICE should also determine whether redundant telecommunications services are cost effective for its ORD locations. Additionally, ICE should continue efforts to document the systems at ORD more accurately. Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at ORD.

Operational Controls

Onsite implementation of operational controls that did not conform fully to DHS policies included inadequate temperature and humidity controls and the inappropriate placement of IT equipment.

Environmental Controls

ICE's operational controls over wire closets and server rooms at ORD locations could be strengthened. For instance, one of ICE's server rooms did not have automated fire suppression or a smoke detector. Additionally, there was excess storage in this room (see figure 2). Further, there were no temperature or humidity sensors. At this location, the humidity and temperature were not within the ranges recommended by DHS server room guidance.

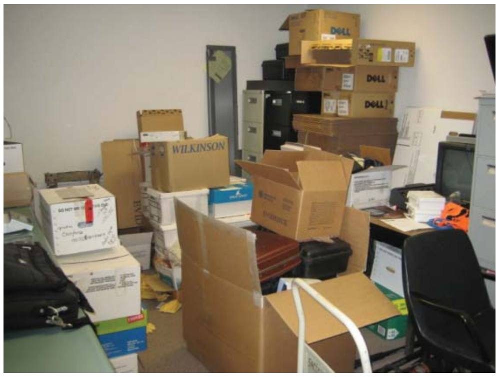


Figure 2: Storage in room with ICE IT equipment.

ICE plans to relocate equipment at this site to a more appropriate facility. However, these plans have been delayed owing to budget constraints. Additionally, according to ICE staff, this site is exempted from government fire suppression requirements because ICE is occupying less than 35,000 square feet and the offices are not above the fifth floor.

Although the humidity in an ICE server room at a second location was within DHS server room guidance, no humidity sensor was present.

According to DHS Directive 4300A,

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

According to the DHS 4300A Handbook,

> The following should be considered when developing a strategy for temperature and humidity control:
>
> - Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit. Most systems will continue to function when temperatures go beyond this range, but the associated risk to data is increased. (Check individual system documentation for the proper levels.)
>
> - Humidity should be at a level between 35 percent and 65 percent. Most systems will continue to function when humidity goes beyond this range, but the associated risk to data is increased. (Check individual system documentation for the proper levels.)

ICE needs to better monitor and control the humidity and temperature in its server rooms at ORD. Low humidity can result in static, and high temperatures can damage sensitive elements of computer systems.

<u>Redundant Telecommunications Services</u>

ICE has not established redundant telecommunications services at its ORD locations. Specifically, only one telecommunications circuit services the users at each of the two locations. As a result, performance of mission-critical activities at these locations is vulnerable to disruptions in the event of a telecommunications failure.

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

> Risk and Infrastructure – A risk-based management decision is made on the requirements for telecommunication services. The availability requirements for the system will determine the time period within which the system connections must be available. If continuous availability is required, redundant telecommunications services may be an option. Once a decision is made on the requirements for telecommunications services, agreements must be made between the appropriate officials involved.
>
> Risk – NIST 800-53 allows for downgrading this security control for availability. This is appropriate when (1) the availability impact level is upgraded to meet the "high water mark" process, (2) supported by an organizational risk assessment, [and] (3) does not impact the security relevant information at the system level.

ICE should conduct a risk assessment to determine whether redundant telecommunications services would be appropriate for staff at these two locations.

Management Controls

ICE's implementation of management controls for systems operating at ORD did not conform fully to DHS policies. Specifically, ICE should establish BIAs for its systems operating at ORD and also better document the accreditation boundaries for these systems.

Missing Business Impact Assessment

ICE had not prepared a BIA for SAC Midwest GSS. According to the DHS 4300A Handbook,

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

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

Accreditation Boundaries

ICE is using a "type" accreditation process for its SAC Midwest GSS.[10] However, not all ICE locations and IT equipment within the geographical boundary of the SAC Midwest GSS are included within its accreditation package. Specifically, a telecommunications switch at one location and the subnet at the other ICE location within our audit scope were not included in the SAC Midwest GSS system accreditation documentation. If ICE does not accurately document the assets that are a part of the SAC Midwest GSS, appropriate information security controls may not be established for the system.

According to DHS Directive 4300A, 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 [Certification and Accreditation] package.

According to ICE staff at ORD, ICE is aware that the SAC Midwest GSS accreditation package does not include all the sites and IT equipment within its geographic boundaries. ICE officials said that the SAC Midwest GSS was set up as an interim system to represent the ICE IT assets within its geographical boundaries. They also said that they are in the process of establishing three new certification packages that will resolve issues related to this system and other ICE GSSs around the country. These three ICE-wide packages will be under the ICE Office of the CIO and will include systems for (1) the file and print servers, (2) the workstations and laptops, and (3) network infrastructure.

[10] According to DHS Directive 4300A, "Type *Security Authorization Process* shall consist of a master *Security Authorization Process* package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites."

Recommendations

We recommend that the ICE CIO:

Recommendation #8: Improve physical security and environmental controls at ORD sites by obtaining smoke detectors and humidity/temperature sensors; ensure that server rooms are maintained within DHS' recommended temperature and humidity ranges; and provide barriers protecting IT infrastructure from being inadvertently damaged in a supply room.

Recommendation #9: Determine if it is cost effective to establish redundant telecommunications services at the two identified ICE locations.

Recommendation #10: Prepare a BIA for the SAC Midwest GSS.

Recommendation #11: Continue to establish nationwide systems to resolve known deficiencies with the ICE Midwest GSS accreditation boundaries.

Management Comments and OIG Analysis

We obtained comments on a draft of this report from ICE's Chief Financial Officer. We have included a copy of the comments in their entirety at appendix B. Separately, ICE provided evidence that a fire extinguisher is now outside the server room. This action will be included in the body of the report and the wording "fire extinguisher" will be removed from the recommendation.

ICE did not concur with recommendations 8, 9, and 10. ICE concurred with recommendation 11.

Recommendation 8

ICE did not concur with this recommendation. In response to recommendation 8, ICE acknowledged the physical and environmental deficiencies in its office. However, ICE cannot require building management to retrofit one suite in the dual-use facility, and the building manager did not agree to renovate the ICE suite. Further, according to ICE, there are no funds available to relocate. ICE requests that OIG consider this recommendation closed.

OIG Analysis

We do not agree that this recommendation should be closed. Although ICE may not currently have the funding to relocate to a more appropriate facility, ICE should enact compensating physical and environmental controls. For example, ICE should assess the feasibility of installing smoke detectors. Recommendation 8 is considered unresolved and open until ICE provides documentation to support that the planned corrective actions are completed.

Recommendation 9

ICE did not concur with this recommendation. In response to recommendation 9, ICE documented its Office of the Chief Information Officer Enterprise Operations process for determining which sites require redundant communications. According to ICE, most RAC offices are near a SAC office where redundancy exists. Additionally, to provide redundancy at well over 600 field sites would cost millions of dollars. Further, a Continuity of Operations Plan (COOP) is currently in place should the need arise. ICE requests that OIG consider this recommendation closed.

OIG Analysis

We agree with ICE's response and have closed this recommendation.

Recommendation 10

ICE did not concur with recommendation 10. According to ICE, DHS does not provide a BIA template and ICE does not have a requirement for a BIA for individual systems. ICE's Disaster Recovery Branch maintains an enterprise-level BIA and updates it as necessary. Further, ICE will have a BIA when the new nationwide Type Accreditation package receives an authorization to operate. ICE requests that OIG consider this recommendation closed.

OIG Analysis

We do not agree that this recommendation should be closed. Although DHS guidance is not clear concerning BIAs, NIST has provided government-wide guidance and templates in this area.[11] For example, according to NIST SP 800-34,

[11] NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems.*

> COOP functions are subject to a process-focused BIA; federal information systems are subject to a system-focused BIA.

Recommendation 10 is considered unresolved and open until ICE provides documentation to support that the planned corrective actions are completed.

Recommendation 11

In response to recommendation 11, ICE is currently developing a new security authorization package to address the IT assets at Chicago O'Hare. ICE will assess the accreditation boundary at ORD and other sites before obtaining the new authorization to operate. The estimated completion date is December 2011.

OIG Analysis

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

TSA Did Not Comply Fully With DHS Sensitive System Policies

TSA could strengthen operational, technical, and management controls for its servers operating at facilities near ORD. For example, TSA could improve environmental and contingency planning controls. TSA should also perform vulnerability scans on all servers at ORD. Additionally, TSA should prepare BIAs for the IT systems operating at ORD. Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by TSA at ORD.

Operational Controls

Onsite implementation of operational controls that did not conform fully to DHS policies included inadequate temperature and humidity controls. Additionally, onsite IT assets may be insufficient to ensure continuity of TSA operations at ORD.

Environmental Controls

TSA's operational controls over server rooms could be strengthened. Specifically, during our fieldwork, all seven server rooms had lower humidity than recommended by DHS guidance. Further, only one of the seven server rooms' temperature was within the range recommended by DHS guidance.

According to the DHS 4300A Handbook,

> The following should be considered when developing a strategy for temperature and humidity control:
>
> - Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit. Most systems will continue to function when temperatures go beyond this range, but the associated risk to data is increased. (Check individual system documentation for the proper levels.)
>
> - Humidity should be at a level between 35 percent and 65 percent. Most systems will continue to function when humidity goes beyond this range, but the associated risk to data is increased. (Check individual system documentation for the proper levels.)

TSA needs to better monitor and control the humidity and temperature in its server rooms. Low humidity can result in static, and high temperatures can damage sensitive elements of computer systems.

After our fieldwork, TSA decommissioned servers and removed them from two of the server rooms. Additionally, TSA has adjusted the temperature and humidity in two of the other server rooms to ensure that they are within DHS guidance. Further, TSA is working to bring the temperature and humidity in the remaining three server rooms to within DHS guidance.

<u>Redundant Telecommunications Services</u>

[redacted]

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

> Risk and Infrastructure – A risk-based management decision is made on the requirements for telecommunication services. The availability requirements for the system will determine the time period within which the system connections must be available. If continuous availability is required, redundant telecommunications services may be an option. Once a decision is made on the requirements for telecommunications services, agreements must be made between the appropriate officials involved.
>
> Risk – NIST 800-53 allows for downgrading this security control for availability. This is appropriate when (1) the availability impact level is upgraded to meet the “high water mark” process, (2) supported by an organizational risk assessment, [and] (3) does not impact the security relevant information at the system level.

Currently, TSA is investigating the use of a local metropolitan area network at ORD to improve reliability and also to reduce costs by consolidating the number of circuits by interconnecting the terminals via optical fiber.

As noted earlier in this report, CBP has established redundant telecommunications services for its ORD Terminal 5 location. TSA may utilize the same redundant DHS OneNet circuits being used by CBP as its alternative circuits to provide cost-effective redundancy at TSA's ORD terminal locations.

Technical Controls

Some of TSA's servers at ORD are part of the STIP IT system (see figure 3). These STIP servers are not attached to a wide area network and have not been scanned for vulnerabilities. TSA's Assessment and Authorization process had not completely assessed these stand-alone systems. Further, a recent TSA Technical Vulnerability Audit of the TSA network did not document the existence of these servers as they were not within the audit scope. As a result, TSA had not performed vulnerability scans on these servers at the time of our fieldwork. Without performing scans to identify vulnerabilities, TSA may not be taking the necessary corrective actions to reduce the impact of these vulnerabilities. After our fieldwork, TSA Information Assurance and Cyber Security Division staff scanned the STIP servers for vulnerabilities and are working to resolve them.

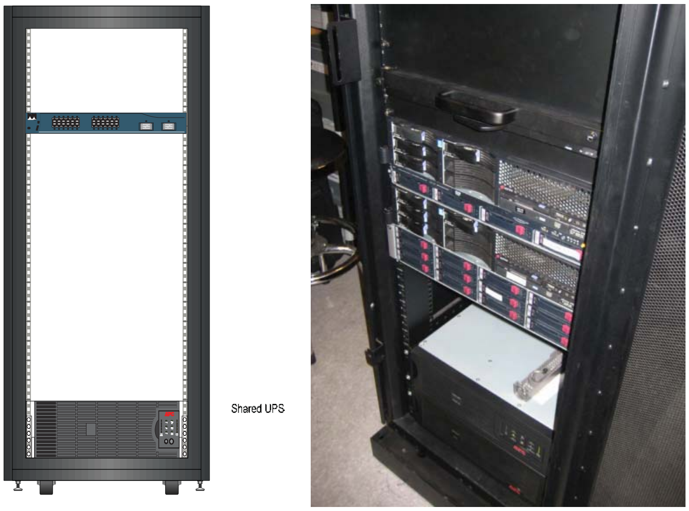


Figure 3: TSA rack diagram from internal TSA report (left) and picture of the same TSA cabinet onsite (right).

According to the DHS 4300A Handbook,

> Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or

> whenever significant changes are made to the information systems.

Management Controls

TSA's implementation of management controls for systems operating at ORD did not conform fully to DHS policies. Specifically, TSA should prepare BIA documentation for these systems.

Missing Business Impact Assessments

TSA has not prepared BIAs for the four systems operating at ORD. According to the DHS 4300A Handbook,

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

The BIA helps to identify and prioritize critical IT systems and components. BIAs are also essential for contingency planning. For example, a BIA would allow TSA to identify maximum tolerable downtime, the resources required to resume mission/business processes, and recovery priorities for system resources.

TSA currently has an enterprise-level BIA process to address systems that have been identified as mission critical. TSANet is the only TSA-designated mission-critical system residing at ORD.

Without performing a BIA, TSA cannot be assured that its backup and recovery plans meet the needs of the business owners (e.g., recovery time objective and recovery point objective).

Recommendations

We recommend that the TSA CIO:

Recommendation #12: Take steps to ensure that server rooms are maintained within DHS' recommended temperature and humidity ranges.

Recommendation #13: Continue efforts to improve the reliability of telecommunications circuits at ORD, and work with CBP to determine whether it is cost effective to use the redundant DHS OneNet circuits to provide TSA with alternate telecommunications services at ORD terminal locations.

Recommendation #14: Ensure that all TSA servers at ORD are scanned annually.

Recommendation #15: Prepare the missing BIAs for the identified TSA systems operating at ORD.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from TSA's Administrator. We have included a copy of the comments in their entirety at appendix B. The Administrator concurred with our recommendations and also provided further information on actions that TSA has already taken to resolve reported deficiencies. These recommendations will be considered resolved but open pending verification of all planned actions.

Recommendation 12

In response to recommendation 12, TSA will work with contractors to ensure that the server rooms in its areas operate within DHS recommended temperature and humidity ranges. TSA will also install sensors and warning devices to alert personnel when the operating environment is not within the recommended ranges.

OIG Analysis

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

Recommendation 13

In response to recommendation 13, TSA will determine if it is cost effective to use DHS OneNet circuits or a local metropolitan area network to provide redundant communications.

OIG Analysis

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

Recommendation 14

In response to recommendation 14, TSA scans its servers annually. TSA has also assessed its servers for vulnerabilities and is working to correct them.

OIG Analysis

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

Recommendation 15

In response to recommendation 15, TSA has an enterprise-level BIA process to address mission-critical systems, including the TSANet. Additionally, TSA is starting a review to prioritize the development of BIAs for identified systems. TSA provided information on other supporting documents, including risk assessment, COOPs, and contingency plans.

OIG Analysis

The actions being taken satisfy the intent of this recommendation as they concern mission-critical systems. This recommendation is considered resolved, but will remain open until TSA provides documentation to support that the planned corrective actions are completed.

Appendix A
Purpose, Scope, and Methodology

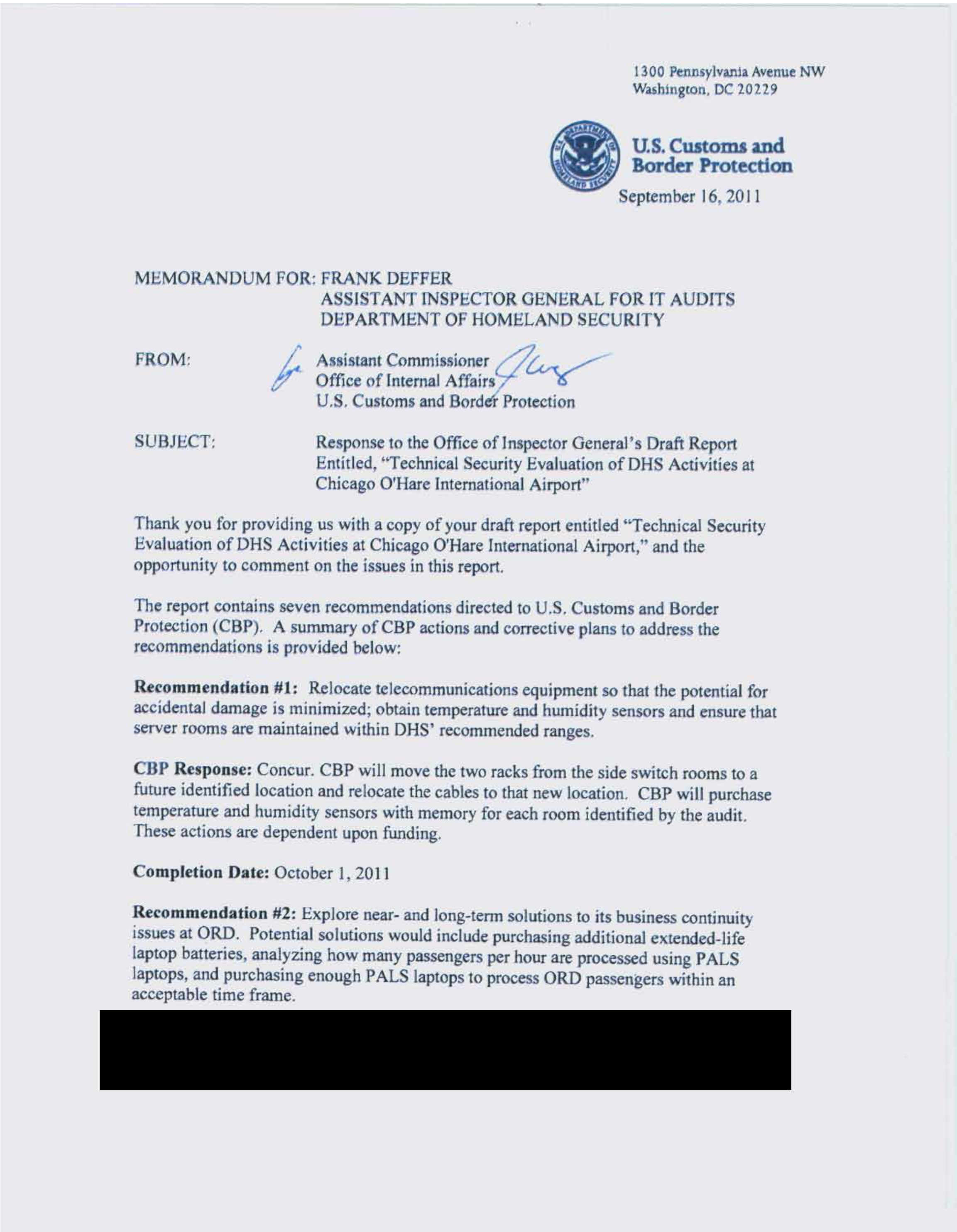
This review is part of a program to evaluate, on an ongoing basis, the implementation of DHS technical and information security policies and procedures at DHS sites. The objective of this program is to determine the extent to which critical DHS sites comply with the department's technical and information security policies and procedures, according to DHS Directive 4300A and its companion document, the DHS 4300A Handbook. Our primary focus was on evaluating the security controls over the servers, routers, switches, and telecommunications circuits comprising the DHS IT infrastructure at this site.

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

We reviewed Trusted Agent *Federal Information Security Management Act of 2002* documentation to ensure that it is current. We reviewed documentation such as the authority-to-operate letter, contingency plans, and BIAs. Additionally, we reviewed guidance provided by DHS to the components in the areas of system documentation, patch management, and wireless security. We reviewed applicable DHS and components' policies and procedures, as well as government-wide guidance.

We conducted this review between February and July 2011. We performed our work according to the *Quality Standards for Inspection and Evaluation* (January 2011) of the Council of the Inspectors General on Integrity and Efficiency and pursuant to the *Inspector General Act of 1978*, as amended. We gave briefings and presentations to DHS staff concerning the results of fieldwork and the information summarized in this report.

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



1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and
Border Protection

September 16, 2011

MEMORANDUM FOR: FRANK DEFFER
ASSISTANT INSPECTOR GENERAL FOR IT AUDITS
DEPARTMENT OF HOMELAND SECURITY

FROM: Assistant Commissioner
Office of Internal Affairs
U.S. Customs and Border Protection

SUBJECT: Response to the Office of Inspector General's Draft Report Entitled, "Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport"

Thank you for providing us with a copy of your draft report entitled "Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport," and the opportunity to comment on the issues in this report.

The report contains seven recommendations directed to U.S. Customs and Border Protection (CBP). A summary of CBP actions and corrective plans to address the recommendations is provided below:

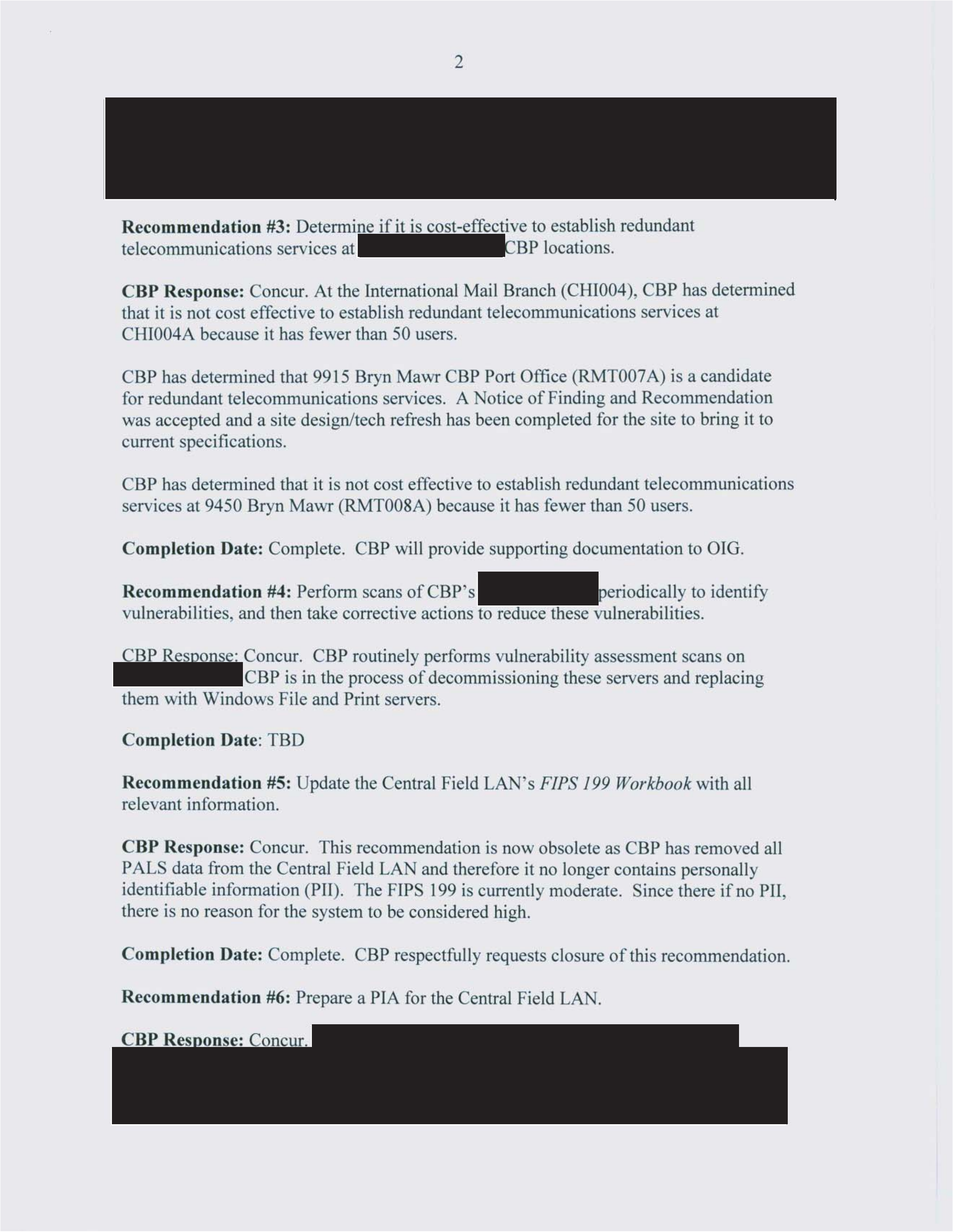
Recommendation #1: Relocate telecommunications equipment so that the potential for accidental damage is minimized; obtain temperature and humidity sensors and ensure that server rooms are maintained within DHS' recommended ranges.

CBP Response: Concur. CBP will move the two racks from the side switch rooms to a future identified location and relocate the cables to that new location. CBP will purchase temperature and humidity sensors with memory for each room identified by the audit. These actions are dependent upon funding.

Completion Date: October 1, 2011

Recommendation #2: Explore near- and long-term solutions to its business continuity issues at ORD. Potential solutions would include purchasing additional extended-life laptop batteries, analyzing how many passengers per hour are processed using PALS laptops, and purchasing enough PALS laptops to process ORD passengers within an acceptable time frame.

[redacted]



[redacted]

Recommendation #3: Determine if it is cost-effective to establish redundant telecommunications services at [redacted] CBP locations.

CBP Response: Concur. At the International Mail Branch (CHI004), CBP has determined that it is not cost effective to establish redundant telecommunications services at CHI004A because it has fewer than 50 users.

CBP has determined that 9915 Bryn Mawr CBP Port Office (RMT007A) is a candidate for redundant telecommunications services. A Notice of Finding and Recommendation was accepted and a site design/tech refresh has been completed for the site to bring it to current specifications.

CBP has determined that it is not cost effective to establish redundant telecommunications services at 9450 Bryn Mawr (RMT008A) because it has fewer than 50 users.

Completion Date: Complete. CBP will provide supporting documentation to OIG.

Recommendation #4: Perform scans of CBP's [redacted] periodically to identify vulnerabilities, and then take corrective actions to reduce these vulnerabilities.

CBP Response: Concur. CBP routinely performs vulnerability assessment scans on [redacted] CBP is in the process of decommissioning these servers and replacing them with Windows File and Print servers.

Completion Date: TBD

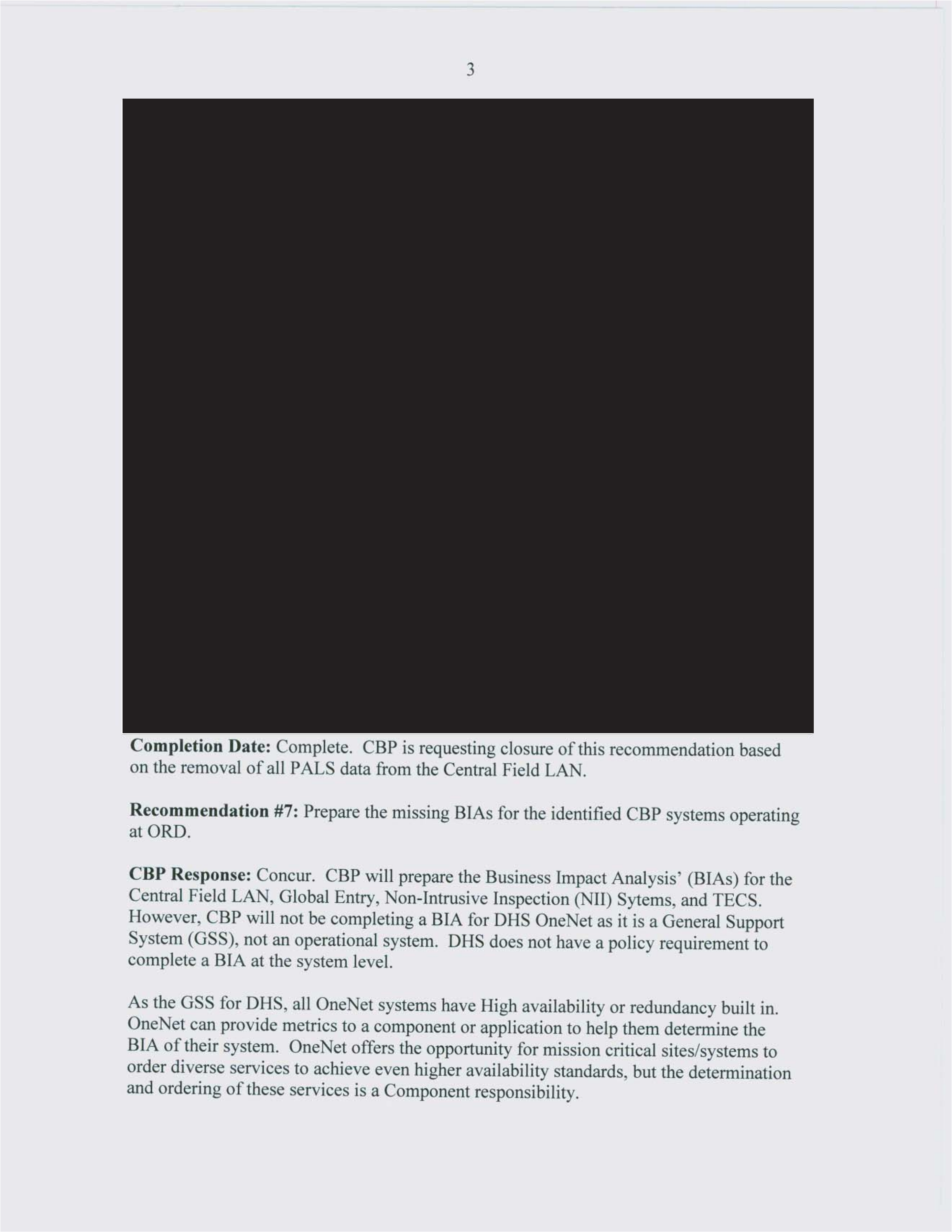
Recommendation #5: Update the Central Field LAN's *FIPS 199 Workbook* with all relevant information.

CBP Response: Concur. This recommendation is now obsolete as CBP has removed all PALS data from the Central Field LAN and therefore it no longer contains personally identifiable information (PII). The FIPS 199 is currently moderate. Since there if no PII, there is no reason for the system to be considered high.

Completion Date: Complete. CBP respectfully requests closure of this recommendation.

Recommendation #6: Prepare a PIA for the Central Field LAN.

CBP Response: Concur. [redacted]



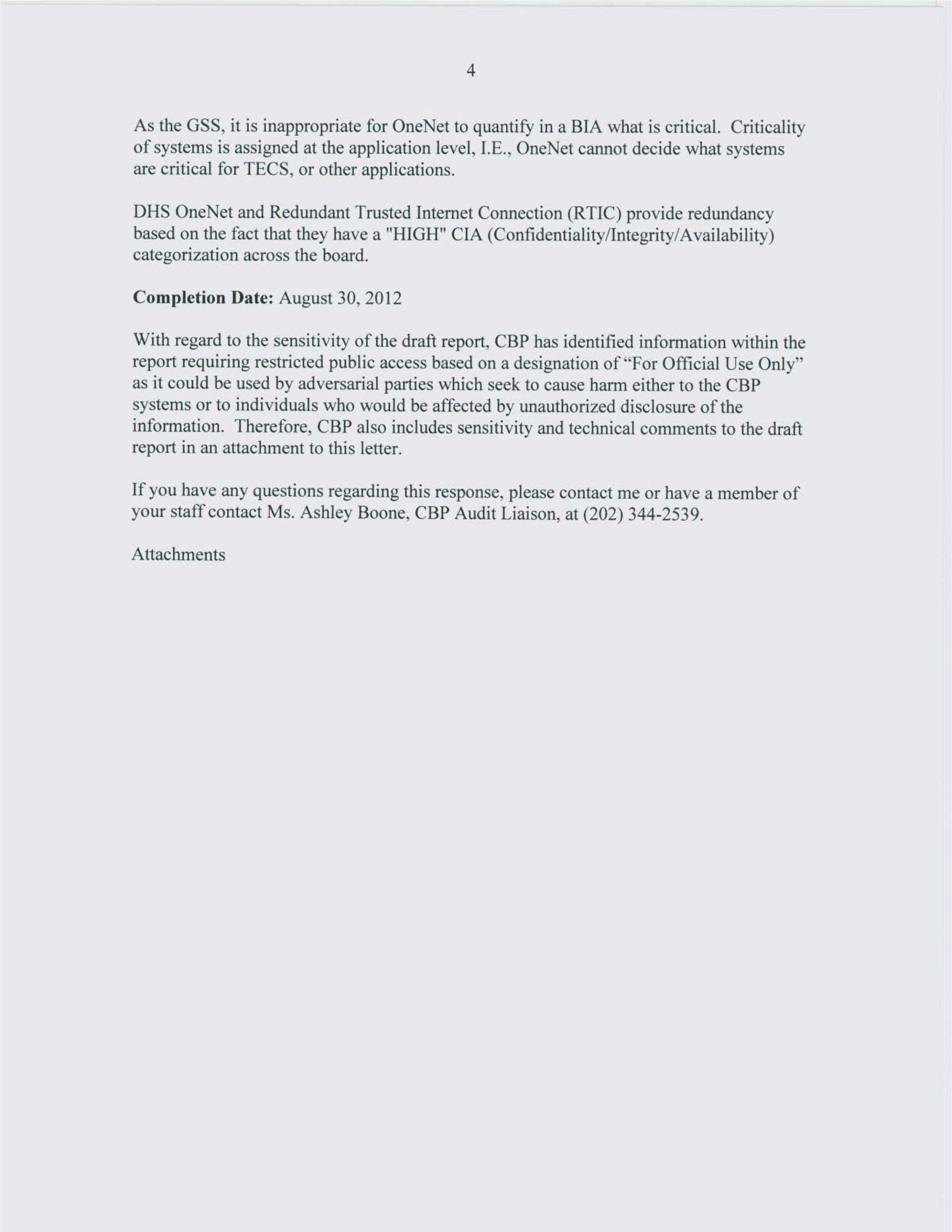
[redacted]

Completion Date: Complete. CBP is requesting closure of this recommendation based on the removal of all PALS data from the Central Field LAN.

Recommendation #7: Prepare the missing BIAs for the identified CBP systems operating at ORD.

CBP Response: Concur. CBP will prepare the Business Impact Analysis' (BIAs) for the Central Field LAN, Global Entry, Non-Intrusive Inspection (NII) Sytems, and TECS. However, CBP will not be completing a BIA for DHS OneNet as it is a General Support System (GSS), not an operational system. DHS does not have a policy requirement to complete a BIA at the system level.

As the GSS for DHS, all OneNet systems have High availability or redundancy built in. OneNet can provide metrics to a component or application to help them determine the BIA of their system. OneNet offers the opportunity for mission critical sites/systems to order diverse services to achieve even higher availability standards, but the determination and ordering of these services is a Component responsibility.



As the GSS, it is inappropriate for OneNet to quantify in a BIA what is critical. Criticality of systems is assigned at the application level, I.E., OneNet cannot decide what systems are critical for TECS, or other applications.

DHS OneNet and Redundant Trusted Internet Connection (RTIC) provide redundancy based on the fact that they have a "HIGH" CIA (Confidentiality/Integrity/Availability) categorization across the board.

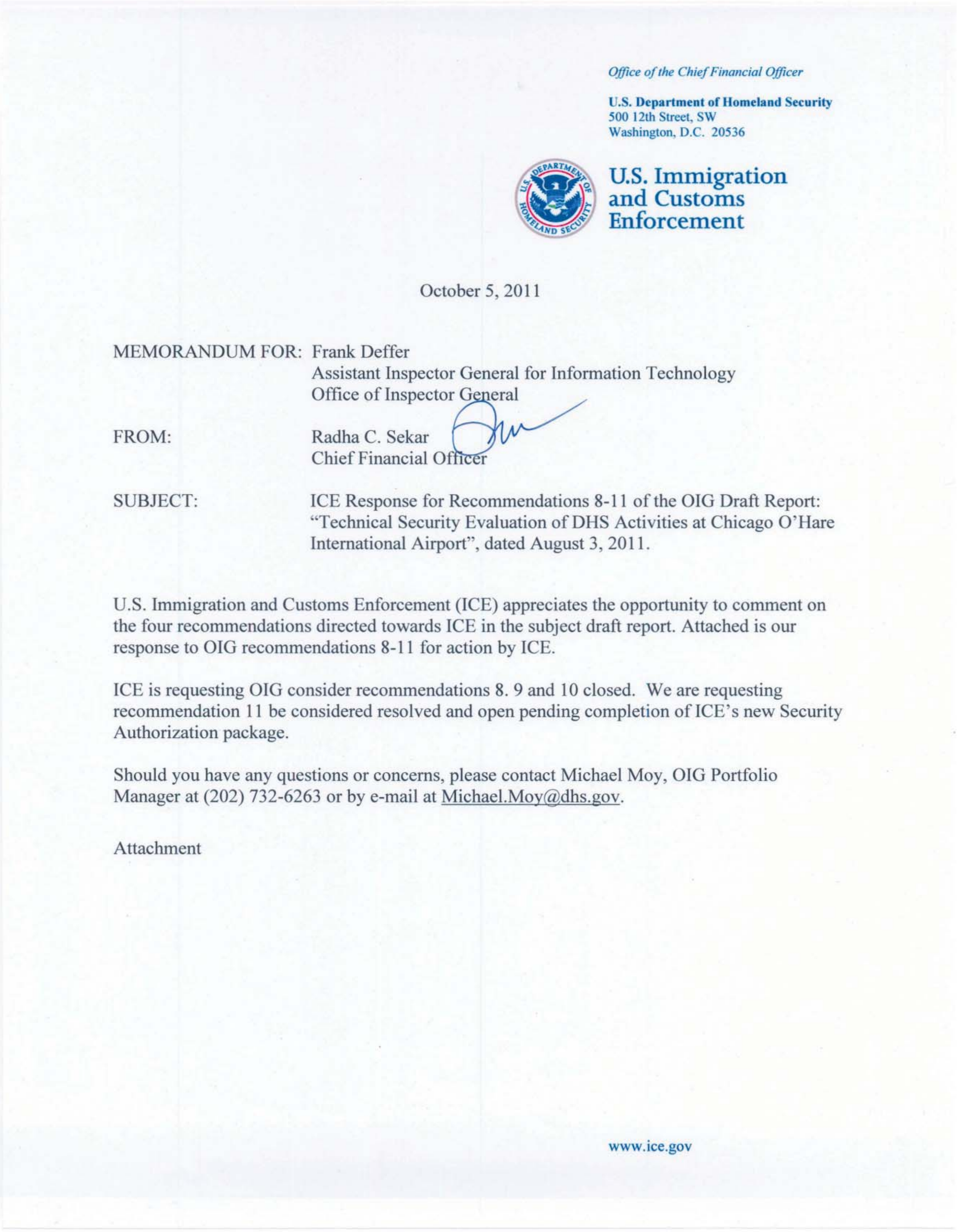
Completion Date: August 30, 2012

With regard to the sensitivity of the draft report, CBP has identified information within the report requiring restricted public access based on a designation of “For Official Use Only” as it could be used by adversarial parties which seek to cause harm either to the CBP systems or to individuals who would be affected by unauthorized disclosure of the information. Therefore, CBP also includes sensitivity and technical comments to the draft report in an attachment to this letter.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Ashley Boone, CBP Audit Liaison, at (202) 344-2539.

Attachments

Appendix B
Management Comments to the Draft Report



Office of the Chief Financial Officer

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536

U.S. Immigration
and Customs
Enforcement

October 5, 2011

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology
Office of Inspector General

FROM: Radha C. Sekar
Chief Financial Officer

SUBJECT: ICE Response for Recommendations 8-11 of the OIG Draft Report: "Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport", dated August 3, 2011.

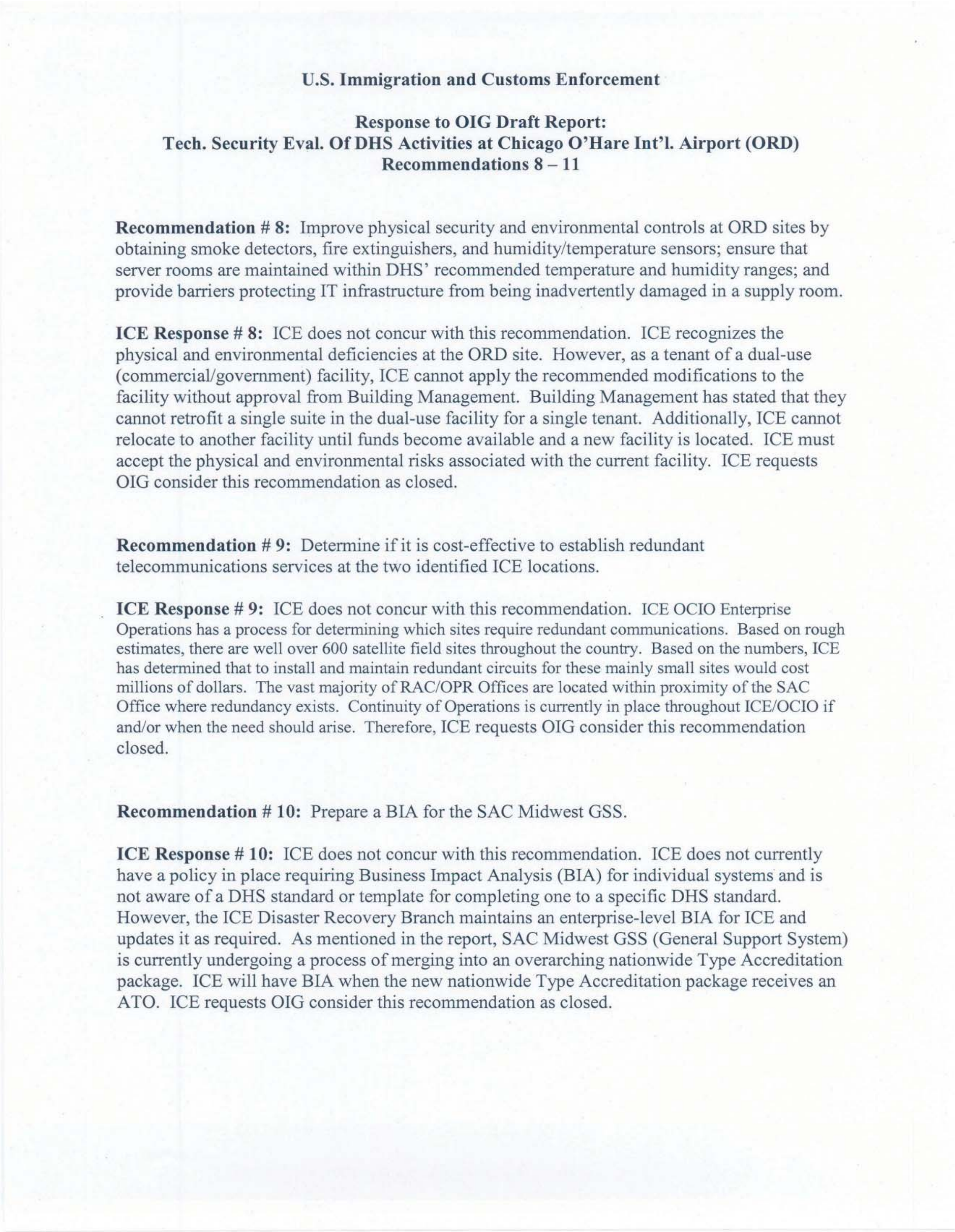
U.S. Immigration and Customs Enforcement (ICE) appreciates the opportunity to comment on the four recommendations directed towards ICE in the subject draft report. Attached is our response to OIG recommendations 8-11 for action by ICE.

ICE is requesting OIG consider recommendations 8. 9 and 10 closed. We are requesting recommendation 11 be considered resolved and open pending completion of ICE's new Security Authorization package.

Should you have any questions or concerns, please contact Michael Moy, OIG Portfolio Manager at (202) 732-6263 or by e-mail at Michael.Moy@dhs.gov.

Attachment

www.ice.gov



U.S. Immigration and Customs Enforcement

Response to OIG Draft Report:
Tech. Security Eval. Of DHS Activities at Chicago O'Hare Int'l. Airport (ORD)
Recommendations 8 – 11

Recommendation # 8: Improve physical security and environmental controls at ORD sites by obtaining smoke detectors, fire extinguishers, and humidity/temperature sensors; ensure that server rooms are maintained within DHS' recommended temperature and humidity ranges; and provide barriers protecting IT infrastructure from being inadvertently damaged in a supply room.

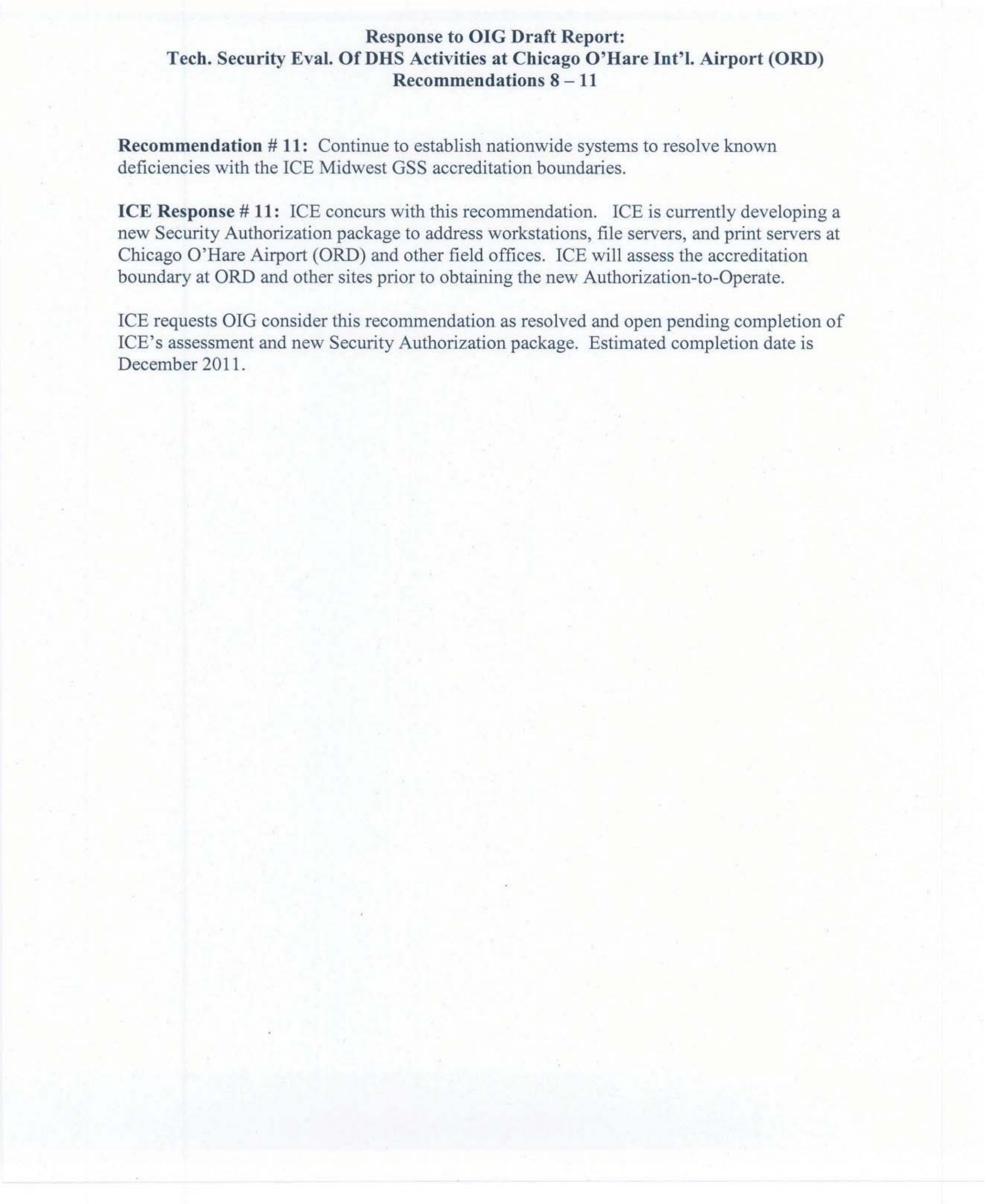
ICE Response # 8: ICE does not concur with this recommendation. ICE recognizes the physical and environmental deficiencies at the ORD site. However, as a tenant of a dual-use (commercial/government) facility, ICE cannot apply the recommended modifications to the facility without approval from Building Management. Building Management has stated that they cannot retrofit a single suite in the dual-use facility for a single tenant. Additionally, ICE cannot relocate to another facility until funds become available and a new facility is located. ICE must accept the physical and environmental risks associated with the current facility. ICE requests OIG consider this recommendation as closed.

Recommendation # 9: Determine if it is cost-effective to establish redundant telecommunications services at the two identified ICE locations.

ICE Response # 9: ICE does not concur with this recommendation. ICE OCIO Enterprise Operations has a process for determining which sites require redundant communications. Based on rough estimates, there are well over 600 satellite field sites throughout the country. Based on the numbers, ICE has determined that to install and maintain redundant circuits for these mainly small sites would cost millions of dollars. The vast majority of RAC/OPR Offices are located within proximity of the SAC Office where redundancy exists. Continuity of Operations is currently in place throughout ICE/OCIO if and/or when the need should arise. Therefore, ICE requests OIG consider this recommendation closed.

Recommendation # 10: Prepare a BIA for the SAC Midwest GSS.

ICE Response # 10: ICE does not concur with this recommendation. ICE does not currently have a policy in place requiring Business Impact Analysis (BIA) for individual systems and is not aware of a DHS standard or template for completing one to a specific DHS standard. However, the ICE Disaster Recovery Branch maintains an enterprise-level BIA for ICE and updates it as required. As mentioned in the report, SAC Midwest GSS (General Support System) is currently undergoing a process of merging into an overarching nationwide Type Accreditation package. ICE will have BIA when the new nationwide Type Accreditation package receives an ATO. ICE requests OIG consider this recommendation as closed.



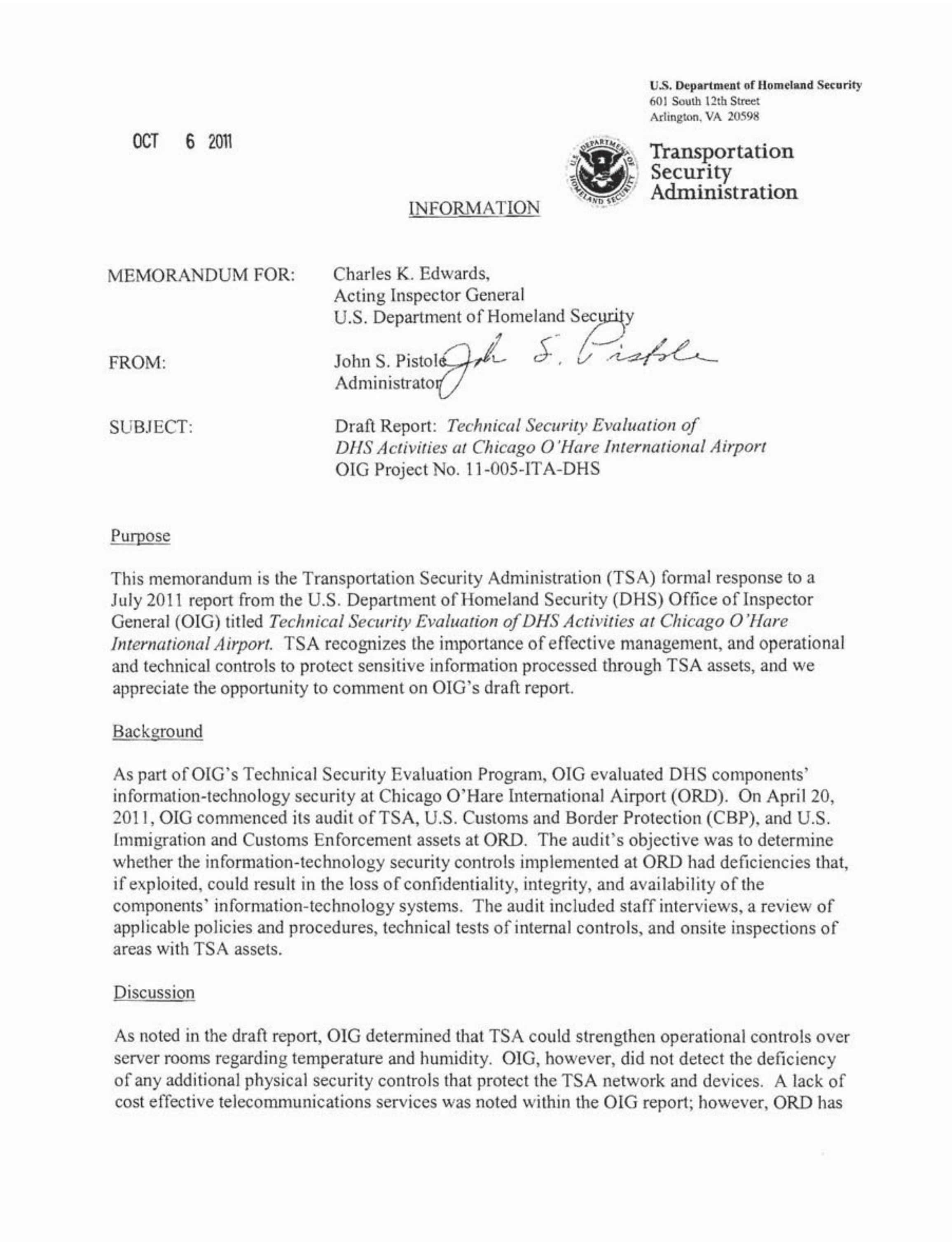
Response to OIG Draft Report:
Tech. Security Eval. Of DHS Activities at Chicago O'Hare Int'l. Airport (ORD)
Recommendations 8 – 11

Recommendation # 11: Continue to establish nationwide systems to resolve known deficiencies with the ICE Midwest GSS accreditation boundaries.

ICE Response # 11: ICE concurs with this recommendation. ICE is currently developing a new Security Authorization package to address workstations, file servers, and print servers at Chicago O'Hare Airport (ORD) and other field offices. ICE will assess the accreditation boundary at ORD and other sites prior to obtaining the new Authorization-to-Operate.

ICE requests OIG consider this recommendation as resolved and open pending completion of ICE's assessment and new Security Authorization package. Estimated completion date is December 2011.

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation
Security
Administration

OCT 6 2011

INFORMATION

MEMORANDUM FOR: Charles K. Edwards,
Acting Inspector General
U.S. Department of Homeland Security

FROM: John S. Pistole John S. Pistole
Administrator

SUBJECT: Draft Report: *Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport*
OIG Project No. 11-005-ITA-DHS

Purpose

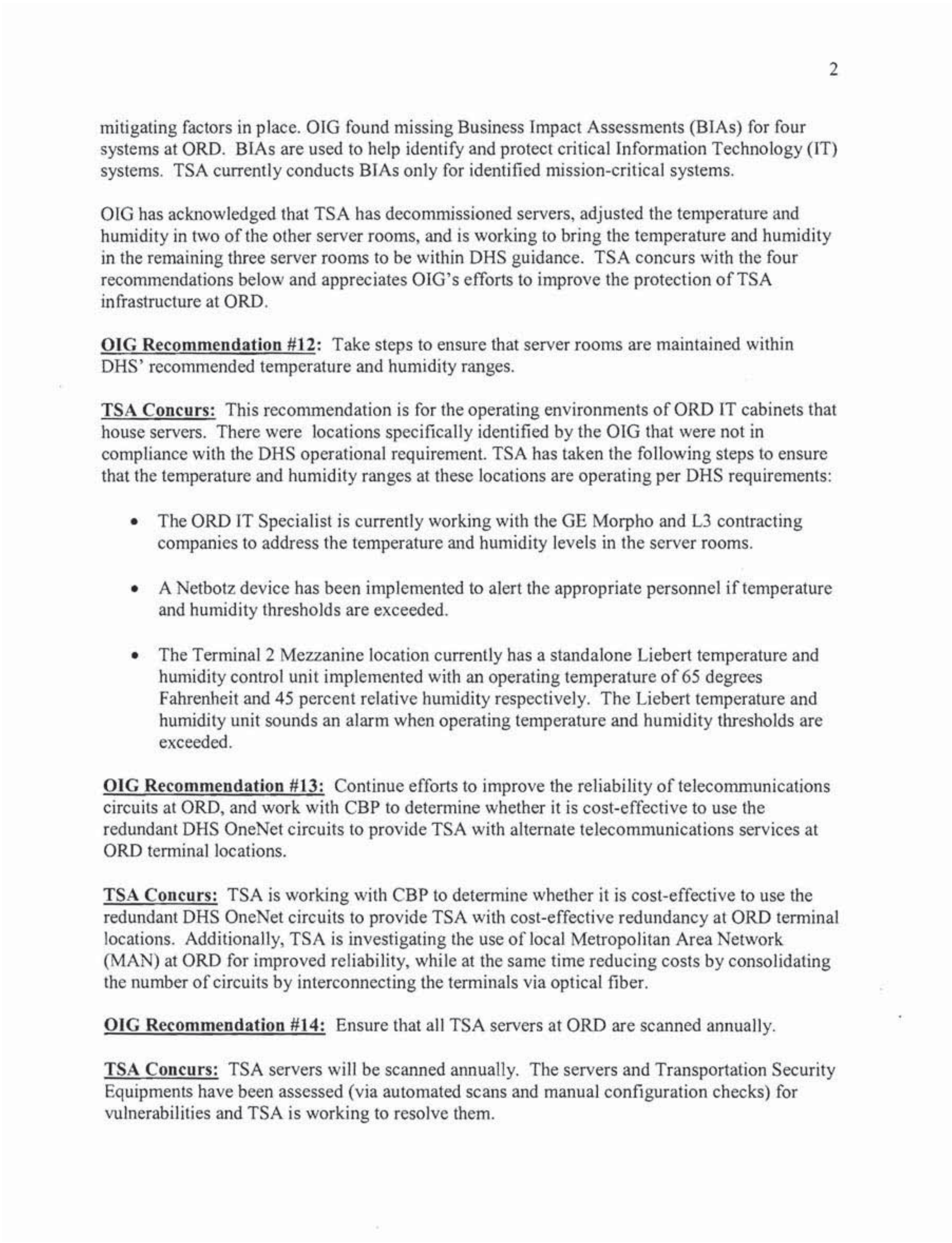
This memorandum is the Transportation Security Administration (TSA) formal response to a July 2011 report from the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) titled *Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport.* TSA recognizes the importance of effective management, and operational and technical controls to protect sensitive information processed through TSA assets, and we appreciate the opportunity to comment on OIG's draft report.

Background

As part of OIG's Technical Security Evaluation Program, OIG evaluated DHS components' information-technology security at Chicago O'Hare International Airport (ORD). On April 20, 2011, OIG commenced its audit of TSA, U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement assets at ORD. The audit's objective was to determine whether the information-technology security controls implemented at ORD had deficiencies that, if exploited, could result in the loss of confidentiality, integrity, and availability of the components' information-technology systems. The audit included staff interviews, a review of applicable policies and procedures, technical tests of internal controls, and onsite inspections of areas with TSA assets.

Discussion

As noted in the draft report, OIG determined that TSA could strengthen operational controls over server rooms regarding temperature and humidity. OIG, however, did not detect the deficiency of any additional physical security controls that protect the TSA network and devices. A lack of cost effective telecommunications services was noted within the OIG report; however, ORD has



mitigating factors in place. OIG found missing Business Impact Assessments (BIAs) for four systems at ORD. BIAs are used to help identify and protect critical Information Technology (IT) systems. TSA currently conducts BIAs only for identified mission-critical systems.

OIG has acknowledged that TSA has decommissioned servers, adjusted the temperature and humidity in two of the other server rooms, and is working to bring the temperature and humidity in the remaining three server rooms to be within DHS guidance. TSA concurs with the four recommendations below and appreciates OIG's efforts to improve the protection of TSA infrastructure at ORD.

OIG Recommendation #12: Take steps to ensure that server rooms are maintained within DHS' recommended temperature and humidity ranges.

TSA Concurs: This recommendation is for the operating environments of ORD IT cabinets that house servers. There were locations specifically identified by the OIG that were not in compliance with the DHS operational requirement. TSA has taken the following steps to ensure that the temperature and humidity ranges at these locations are operating per DHS requirements:

- The ORD IT Specialist is currently working with the GE Morpho and L3 contracting companies to address the temperature and humidity levels in the server rooms.

- A Netbotz device has been implemented to alert the appropriate personnel if temperature and humidity thresholds are exceeded.

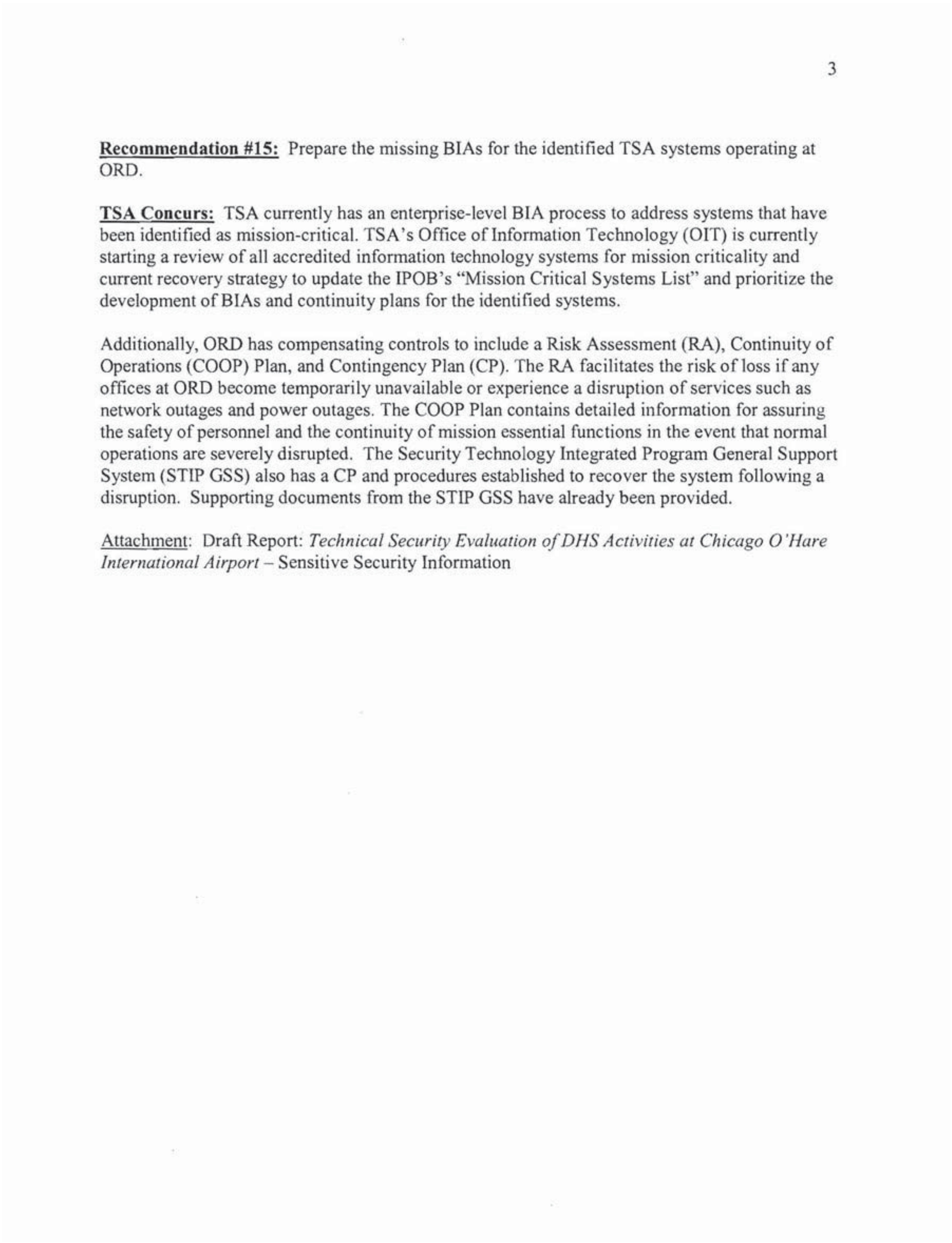
- The Terminal 2 Mezzanine location currently has a standalone Liebert temperature and humidity control unit implemented with an operating temperature of 65 degrees Fahrenheit and 45 percent relative humidity respectively. The Liebert temperature and humidity unit sounds an alarm when operating temperature and humidity thresholds are exceeded.

OIG Recommendation #13: Continue efforts to improve the reliability of telecommunications circuits at ORD, and work with CBP to determine whether it is cost-effective to use the redundant DHS OneNet circuits to provide TSA with alternate telecommunications services at ORD terminal locations.

TSA Concurs: TSA is working with CBP to determine whether it is cost-effective to use the redundant DHS OneNet circuits to provide TSA with cost-effective redundancy at ORD terminal locations. Additionally, TSA is investigating the use of local Metropolitan Area Network (MAN) at ORD for improved reliability, while at the same time reducing costs by consolidating the number of circuits by interconnecting the terminals via optical fiber.

OIG Recommendation #14: Ensure that all TSA servers at ORD are scanned annually.

TSA Concurs: TSA servers will be scanned annually. The servers and Transportation Security Equipments have been assessed (via automated scans and manual configuration checks) for vulnerabilities and TSA is working to resolve them.



Recommendation #15: Prepare the missing BIAs for the identified TSA systems operating at ORD.

TSA Concurs: TSA currently has an enterprise-level BIA process to address systems that have been identified as mission-critical. TSA's Office of Information Technology (OIT) is currently starting a review of all accredited information technology systems for mission criticality and current recovery strategy to update the IPOB's "Mission Critical Systems List" and prioritize the development of BIAs and continuity plans for the identified systems.

Additionally, ORD has compensating controls to include a Risk Assessment (RA), Continuity of Operations (COOP) Plan, and Contingency Plan (CP). The RA facilitates the risk of loss if any offices at ORD become temporarily unavailable or experience a disruption of services such as network outages and power outages. The COOP Plan contains detailed information for assuring the safety of personnel and the continuity of mission essential functions in the event that normal operations are severely disrupted. The Security Technology Integrated Program General Support System (STIP GSS) also has a CP and procedures established to recover the system following a disruption. Supporting documents from the STIP GSS have already been provided.

Attachment: Draft Report: *Technical Security Evaluation of DHS Activities at Chicago O'Hare International Airport* – Sensitive Security Information

Appendix C
Major Contributors to this Report

Sharon Huiswoud, Director
Kevin Burke, Audit Manager
Matthew Worner, Senior Auditor
Charles Twitty, Senior Auditor
Eun Suk Lee, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
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
Under Secretary for Management
DHS CISO
DHS CISO Audit Liaison
CBP CIO
CBP Audit Liaison
ICE CIO
ICE Audit Liaison
TSA CIO
TSA Audit Liaison

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)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603

- Fax the complaint directly to us at (202)254-4292

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigation - Hotline,
  245 Murray Drive SW, Building 410
  Washington, DC 20528

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