DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

# Technical Security Evaluation of U.S. Customs and Border Protection Activities at the Chet Holifield Federal Building (Redacted)

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

OIG-08-37

April 2008

*Office of Inspector General*

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

Homeland
Security

April 8, 2008

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.

Our report addresses the strengths and weaknesses of the implementation of technical and information security policies and procedures at U.S. Customs and Border Protection locations at the Chet Holifield Federal Building, Laguna Niguel, 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

## Abbreviations

| | |
|---|---|
| CBP | U.S. Customs and Border Protection |
| CHFB | Chet Holifield Federal Building |
| CIO | Chief Information Officer |
| CISO | Chief Information Security 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 |
| HVAC | Heating, Ventilation, and Air Conditioning |
| ICE | Immigration and Customs Enforcement |
| ISA | Interconnection Security Agreement |
| IT | Information Technology |
| LAN | Local Area Network |
| OIG | Office of Inspector General |

.

# Table of Contents/Abbreviations

| | |
|---|---|
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PTA | Privacy Threshold Analysis |
| SORN | System of Records Notice |
| SSH | Secure Shell |
| TA-FISMA | Trusted Agent FISMA |
| USCIS | United States Citizenship and Immigration Services |

## Executive Summary

We initiated a program to determine the extent to which critical Department of Homeland Security sites comply with the department's technical and information security policies and procedures. Based on our internal analysis, we selected the Chet Holifield Federal Building located in Laguna Niguel, California where the U.S. Customs and Border Protection's Southern California field support and Human Resources Management staffs are located.

Our evaluation focused on how Customs and Border Protection has implemented computer security operational, technical, and management controls for its information technology resources at this site. We performed onsite inspections of the areas where these resources were located, interviewed departmental staff, and conducted technical tests of internal controls, e.g., scans for wireless networks. We also reviewed applicable departmental policies, procedures, and other appropriate 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 information technology systems. Specifically, Customs and Border Protection needs to improve its environmental, business continuity, and physical security controls for its computer room and telecommunications closets. Customs and Border Protection could also improve its technical controls at this site [redacted]

Additionally, management controls could be improved at this site by implementing effective capital planning and investment control procedures and by completing all required system accreditation activities.

## 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 and 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 and DHS IT security policies are organized under operational, technical, and management controls 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.

Based on our internal analysis, we selected the Chet Holifield Federal Building (CHFB) located in Laguna Niguel, California, where U.S. Customs and Border Protection's (CBP) Southern California field support and Human Resources Management staffs are located. The United States Citizenship and Immigration Services (USCIS) and United States Immigration and Customs Enforcement (ICE) also operated in this facility, and their activities will be addressed in separate evaluation reports.

CBP operates a server/telecommunications room at CHFB and relies on telecommunications lines concentrated in two additional telecommunications closets that are shared with ICE. Additionally, CBP relies on servers and routers operated by ICE in a separate server/telecommunications room. Operational and technical control weaknesses associated with these servers and routers operated by ICE, but used by CBP, will be reported separately in the ICE specific evaluation report.

# Results of Review

## Systems Did Not Comply Fully With DHS Operational Control Requirements

Some operational controls that CBP implemented at CHFB did not always conform to DHS policies; these included environmental, business continuity, and physical security controls.  The environmental and business continuity deficiencies are particularly significant and place CBP at risk of being unable to access IT assets and data at this site when necessary.  Collectively, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by CBP at CHFB.

### Environmental Controls

The air conditioning unit in the CBP server/telecommunications room may be inadequate.  While the air conditioning unit was set to cool the room to 67 degrees, the room temperature was 71 degrees during our visit in February 2007.  See Figure 1 below.

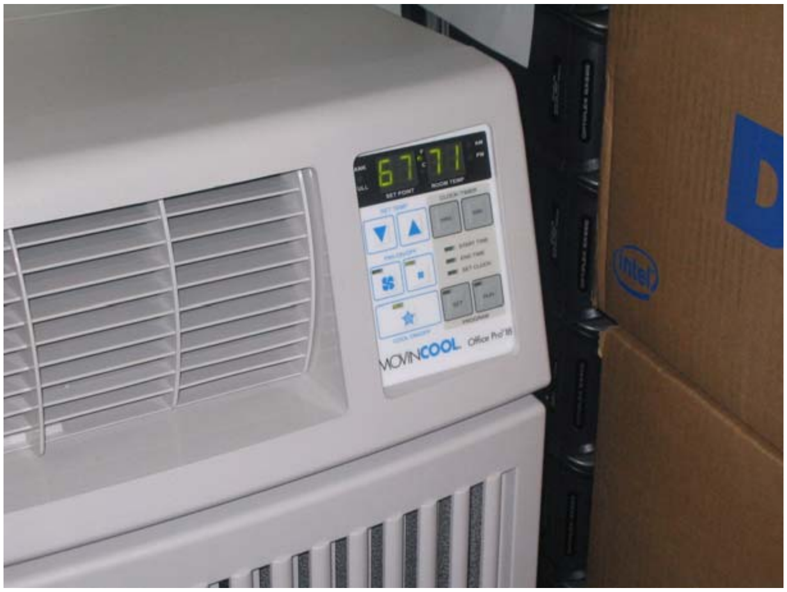


*Figure 1: Air Conditioner Temperature Display*

According to the DHS 4300A Handbook:

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

The absence of adequate heating, ventilation, and air conditioning (HVAC) capabilities for IT equipment increases the risk that CBP's IT assets may malfunction.

Following discussions, CBP staff informed us that this HVAC unit was a temporary solution. Further, the Information Systems Security Officer for the Far West Field Local Area Network (LAN) requested that CBP perform a risk assessment at the CHFB. One of the results of the risk assessment will be the identification of the proper HVAC capabilities necessary for the CBP IT resources at CHFB.

**<u>Business Continuity</u>**

CBP's business continuity capability needs to be strengthened at CHFB. Although CBP had an uninterruptible power supply for the CBP IT assets in the server room, officials reported that the capacity of the device is minimal and will only allow the server to power-off. CBP does not have a backup electrical generator to support the server room. Furthermore, CBP's electronic equipment may be at risk of damage or malfunction due to the lack of an emergency shut-off switch. Without an emergency shut-off switch, the IT resources that are still receiving power when the sprinklers are activated are at increased risk of a short circuit during a fire.

According to the DHS 4300A Handbook:

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

**<u>Physical Security Controls</u>**

The CBP server room has several boxes stored around the air conditioning unit. See Figure 2 below. This increases the risk that CBP's IT assets may inadvertently lose power or be accidentally damaged. CBP could also better protect its IT assets from damage by ensuring that the immediate areas in the server room are not used for general storage.

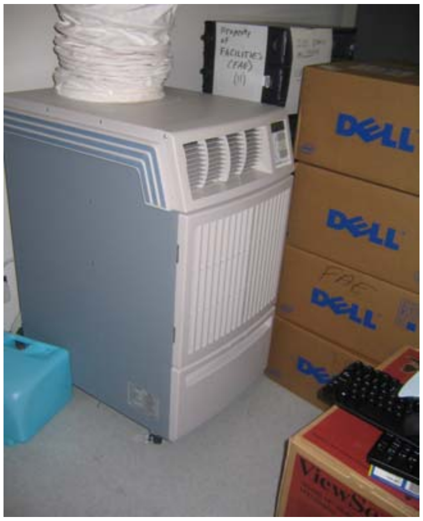


*Figure 2: Air Conditioner and Storage in CBP Server Room*

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.*

CBP staff informed us that this storage was a temporary arrangement and they have removed these boxes from their server room.

CBP is also not in compliance with its own security guidelines for IT resources. Specifically, in a room shared with ICE, there is a CBP server stored in a locked cabinet and CBP telecommunications assets sharing one of two telecommunications racks with ICE equipment. See Figures 3 and 4 below. Additionally, during our onsite visit, CBP officials had difficulty gaining access to a second room containing CBP telecommunication assets. CBP staff had to contact ICE for entry to this room.

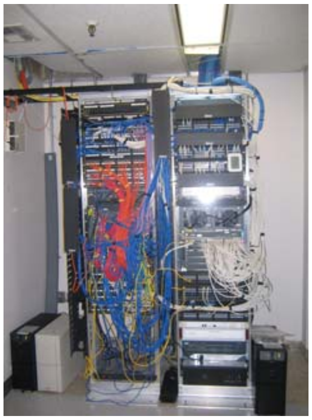


*Figure 3: Shared Telecommunications Rack*

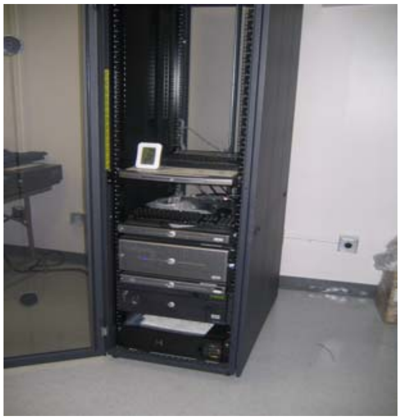


*Figure 4: CBP-Operated Server*

According to CBP's Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C, Section 5.3.1:

> *Rooms containing information systems hardware and software, such as Local Area Network (LAN) rooms or telephone closets, must be secured and accessible by authorized CBP personnel only.*

During discussions, staff from the office of the DHS Chief Information Security Officer (CISO) suggested that CBP review their security guidelines. CBP is now in the process of reviewing and updating their security policies to allow sharing facilities with authorized DHS components.

## Recommendations:

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

**Recommendation #1**: Implement stronger physical security and environmental controls to protect CBP's IT assets from possible destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

**Recommendation #2:** Implement business continuity of operations capability for CBP facilities at CHFB, [redacted]

## Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the CBP Office of Policy and Planning.  We have included a copy of the comments in their entirety at Appendix B.

In the comments, CBP concurred with findings and recommendations one and two in our report.  Specifically, CBP has updated policy and taken several steps towards improving physical and environmental security of IT at CHFB.  Recommendation one will be considered resolved but open pending verification of all planned actions.

As stated above, CBP has concurred with recommendation two.  In its comments, CBP stated that the IT contingency plan has been provided for updating the CHFB Continuity of Operations Plan. CBP is also working to provide an emergency backup electrical generator and an emergency shut-off switch to support its server room. [redacted] Therefore, recommendation two will be considered resolved but open pending verification of all planned actions.

## Systems Did Not Comply Fully With DHS Technical Control Requirements

CBP's implementation of technical controls did not conform to DHS policies involving configuration management of CBP's server and router. These deficiencies increase the risk that CBP IT systems used at CHFB are vulnerable to internal attacks.

### Server Configuration Management

CBP's server was not properly configured to prevent an "insider" from gaining unauthorized privileges and information.[1] For example, the following services with known vulnerabilities were enabled or provided unnecessary information to anonymous requests:

- **Blah11 (1042/tcp) –** Our scan reported that Blah11 was implemented. This scan report needs to be investigated further to determine whether it was an incorrect report or if a known Trojan horse is operating on this host. [2]

[redacted]

[1] 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."

[2] According to the DHS 4300 Handbook:

> *A Trojan horse is a computer program that is apparently or actually useful but performs another function. A Trojan horse generally provides remote control access to an unauthorized person. A Trojan horse can be used to modify databases, write checks, send e-mail, or destroy files. It could be imbedded by a programmer or downloaded from the Internet.*

[redacted]

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.*

Following presentation of these scans, CBP performed further research and determined that Blah11 was falsely reported, as it was not installed on their system. Further, CBP is evaluating the need for port 1042/tcp.

**<u>Router Configuration Management Controls</u>**

CBP's router at CHFB was not properly configured to prevent an "insider" from gaining unauthorized privileges and information [redacted]

As a result of our scans, CBP officials began to reevaluate their policy for internal routers and their associated open/unfiltered ports. CBP is currently evaluating an updated security profile for several of the ports and accessible services.

[redacted] This may allow an attacker to capture login credentials and remotely take control of the router and change or delete configuration files.

According to DHS Directive 4300A:

> *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.*

CBP has informed us that [redacted] will be disabled and SSH will be implemented after the entire CBP component is migrated to the DHS OneNet.  The date for this is November 2, 2007.

## Recommendations:

We recommend that the CBP CIO take the following actions for CBP activities at CHFB:

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

**Recommendation #4:**  Eliminate or disable unnecessary services from the server and router.

## Management Comments and OIG Analysis

In the comments, CBP concurred with these two recommendations and also reported steps that it plans to take to resolve these issues. These recommendations will be considered resolved but open pending verification of reported actions.

## Systems Did Not Comply Fully With DHS Management Control Requirements

CBP's implementation of management controls at CHFB did not conform to DHS policies. Specifically, there are deficiencies in capital planning and investment controls, system accreditation, establishment of interconnection security agreements (ISA), and privacy compliance activities related to personal information[3] These management control deficiencies increase the risk to CBP's IT investments, systems, and data from new threats and vulnerabilities for which safeguards have not been implemented.

**<u>Capital Planning and Investment Control</u>**

CBP did not adequately consider shared infrastructure when it installed a new server room and telecommunications lines at CHFB.[4] Specifically, CBP did not perform a formal analysis of the benefits of using the DHS operated, shared server room in CHFB Use of this shared infrastructure would also support the department's commitment to functional integration. CBP cannot be certain that the approach it has adopted is the most cost effective solution.

According to DHS Management Directive 0007.1, *Information Technology Integration And Management:*

> *<u>Functional integration</u>: Is a transformation process that enhances efficient and effective use of resources by establishing unified policies and business processes, the use of shared or centralized services and standards and automated solutions. Functional integration is a structured cooperation and collaboration among DHS Components and LOB [Line of Business] chiefs for the purpose of achieving functional excellence in support of Departmental mission and objectives. This is accomplished by decreasing fragmentation and duplication, providing*

[3] Laws that govern DHS' use of personal information include the Homeland Security Act of 2002, § 222, 6 U.S.C. § 142; the Privacy Act of 1974, 5 U.S.C. § 552a; and the E-Government Act of 2002, § 208, 44 U.S.C. § 3501 note.

[4] This new server room was established to support CBP employees that were to be transferred from ICE due to a DHS re-organization.

> *enhanced integrated services and increasing efficiency and quality of management lines of business.*

CBP did not originally connect their new server equipment to the shared DHS OneNet infrastructure as required by the October 19, 2006, memorandum from the DHS Deputy Secretary.[5] However, during the course of our audit fieldwork, CBP connected this server to the DHS OneNet and has issued disconnect orders for the unnecessary high-speed telecommunications lines that the DHS OneNet replaces.

[5] In the Memorandum of October 19, 2006, *Integration of Component Infrastructures Into the Infrastructure Transformation Program (ITP),* the Deputy Secretary directed the department's components to integrate their infrastructure requirements into the department's Infrastructure Transformation Program, which includes the DHS OneNet.

## System Accreditation

CBP staff at CHFB is currently using three systems. However, only two of the three (66%) are currently authorized to operate. Specifically, CBP has not included one of the systems in the department's system inventory, Trusted Agent FISMA (TA-FISMA), and has not started risk assessment and accreditation process for this system.[6] See Figure 5 below.

| System Name | TA-FISMA Identifier | Risk Assessment Status | Accreditation Status |
|---|---|---|---|
| **DHS OneNet**<br>**(CBP Steward)** | **CBP-00044-GSS-00044** | **Completed** | **Authorized to Operate** |
| **Far West Field LAN** | **CBP-00029-GSS-00029** | **Completed** | **Authorized to Operate** |
| **The Human Resources File Manager System (RECFIND)** | **No Identifier** | **No Status** | **No Status** |

*Figure 5: Certification and Accreditation Status*

Additionally, CBP has not updated TA-FISMA to include the new server room at CHFB. Specifically, CBP staff stated that the new server room at CHFB was part of the Far West Field LAN, which is a "type accreditation" system.[7] However, CBP has not prepared the necessary attachments to its documentation annotating CHFB site-specific physical and logical variations related to a server room that CBP had implemented at CHFB.

[6] 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.

[7] According to DHS 4300A Handbook, Attachment D –Type Accreditation:

> A type certification/accreditation, however, allows for common security controls across the sites to be consolidated and for a single master C&A to be conducted.

According to DHS 4300A 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.*

CBP management cannot be assured that IT systems and data are properly 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.

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.*

We also identified three additional IT resources that CBP had not previously included in the DHS' TA FISMA reporting tool. See Figure 6 below.

| IT Resource Name |
|---|
| Common Drive Home Drive, Human Resources Division |
| OCE (desktop publishing application) |
| CcMail |

*Figure 6: CBP IT Resources Not Included in TA-FISMA*

Staffs from CBP and the office of the DHS CISO are in the process of determining if these IT resources should be part of the system accreditation process. IT resources that are not included in the accreditation process may not be properly secured, increasing the risk to CBP systems and data.

According to DHS 4300A Handbook:

> *For operational systems, the DAA makes a risk-based decision either to grant full authorization to operate or deny authorization to operate.*

Following discussions, CBP informed us that they would determine whether CBP staff required the Human Resources File Manager System (RECFIND) to perform their work. Additionally, CBP is in the process of documenting the desktop publishing application. Further, CBP is in the process of eliminating the need for the identified home drives and cc-Mail. Following these actions, CBP will properly certify identified systems.

### <u>Interconnection Security Agreements</u>

CBP and ICE have a service level agreement for services that ICE provides to CBP, including operating servers that support CBP applications and users' data. However, the required ISAs for these systems do not exist. Additionally, CBP, as steward of the DHS OneNet, should have ISAs with ICE and USCIS for telecommunication services.

By not establishing and maintaining ISAs, CBP may not be aware of new threats or vulnerabilities to the confidentiality, integrity, and availability of its systems and data.

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.*
>
> **********
>
> *ISAs shall be reissued every three years or whenever any significant changes have been made to any of the*

*interconnected system. ISAs shall be reviewed as a part of the annual FISMA self-assessment.*

**Privacy Compliance Activities**

CBP has completed all required privacy compliance activities for only 1 of 3 (33%) of its systems in use at CHFB. See Figure 7 below.

| System Name | TA-FISMA Number | Privacy Threshold Analysis (PTA) | Privacy Impact Assessment (PIA) Required? | Has the PIA Been Submitted to the DHS Privacy Office for Validation | Applicable System of Record Notice According to DHS Privacy Office |
|---|---|---|---|---|---|
| DHS OneNet (CBP Steward) | CBP-00044-GSS-00044 | PTA Completed | No PIA required | NA | NA |
| Far West Field LAN | CBP-00029-GSS-00029 | PTA was reviewed in November of 2006. | *PIA is required due to collection of Personally Identifiable Information (PII). | No | DHS/All GITAARS 71 FR 78446 |
| **The Human Resources File Manager System (RECFIND) | None | None | Unknown | No | Justice/ INS-034 67 FR 56585 |
| *The PTA for this system was reissued and a PIA is no longer required.<br>**The Human Resources File Manager System is being retired. | | | | | |

*Figure 7: Status of Privacy Act Related Activities for CBP Systems*

Specifically, the Privacy Threshold Analysis (PTA) for the DHS OneNet determined that it does not collect personally identifiable information (PII); therefore neither a Privacy Impact

Assessment (PIA) nor a System of Records Notice (SORN) is required. While the PTA for the Far West Field LAN determined that PII is collected, the DHS Privacy Office has not yet validated a PIA for this system. Additionally, DHS does not have on file a PTA or a PIA for the Human Resources File Manager System (RECFIND). Further, DHS has not issued an updated SORN to reflect that this system is now operated by DHS and not the Department of Justice. However, use of a legacy SORN is permitted as the Savings Provision of the Homeland Security Act of 2002 allows DHS to rely on legacy SORNs.[8]

## Recommendations:

We recommend that the CBP CIO take the following actions for CBP activities at CHFB:

**Recommendation #5:** Perform an analysis of the cost and benefits of continuing to operate a separate server room in lieu of sharing a DHS-operated server room.

**Recommendation #6:** Complete the activities required to accredit and authorize IT systems that are in use at CHFB.

**Recommendation #7:** Establish and maintain the required interconnection security agreements.

**Recommendation #8:** Complete Privacy Impact Assessments and publish updated System of Records Notices as needed for systems in use at CHFB.

## Management Comments and OIG Analysis

In the comments, except for recommendation #8, CBP concurred with our recommendations and also reported steps taken to resolve these issues. We believe that the actions that CBP has taken and plans to take will resolve the reported issues. These

[8] According to the Homeland Security Act of 2002, Section 1512, Savings Provision:

> *(a) COMPLETED ADMINISTRATIVE ACTIONS. —(1) Completed administrative actions of an agency shall not be affected by the enactment of this Act or the transfer of such agency to the Department, but shall continue in effect according to their terms until amended, modified, superseded, terminated, set aside, or revoked in accordance with law by an officer of the United States or a court of competent jurisdiction, or by operation of law.*

recommendations will be considered resolved but open pending verification of reported actions.

CBP did not concur with recommendation #8. In the comments, CBP stated that the PTA for the Far West Field LAN, the first of two systems applicable to this recommendation, was updated and validated in September 2007, following receipt of our draft report, dated August 10, 2007. We believe that the reported privacy compliance issue for this system has been resolved. Additionally, CBP plans to retire the Human Resource File Management System (RECFIND), which is the second system applicable to this recommendation. Specifically, CBP stated employees would not use the system after October 30, 2007. We also believe that this CBP planned action will resolve privacy compliance issues for this system. This recommendation will also be considered resolved but open pending verification of reported actions.

## 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.

We coordinated the implementation of this technical security evaluation program with the DHS 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 CBP officials at the Office of Information Technology in Washington, DC, and by telephone with CHFB OIT officials.

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

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

We reviewed applicable DHS and CBP policies and procedures and CBP's responses to our site surveys and technical questionnaires. Prior to performing our onsite review, we used CBP's responses to identify occupied space, server rooms, and telecommunications closets. Our onsite review included a physical review of CBP space and interviews with CBP staff. (Our technical review included onsite reviews of server security policies as well as scans for DHS wireless devices operating at CHFB.[10] Additionally, we reviewed guidance provided by DHS to the components in the areas of patch management and operating systems.

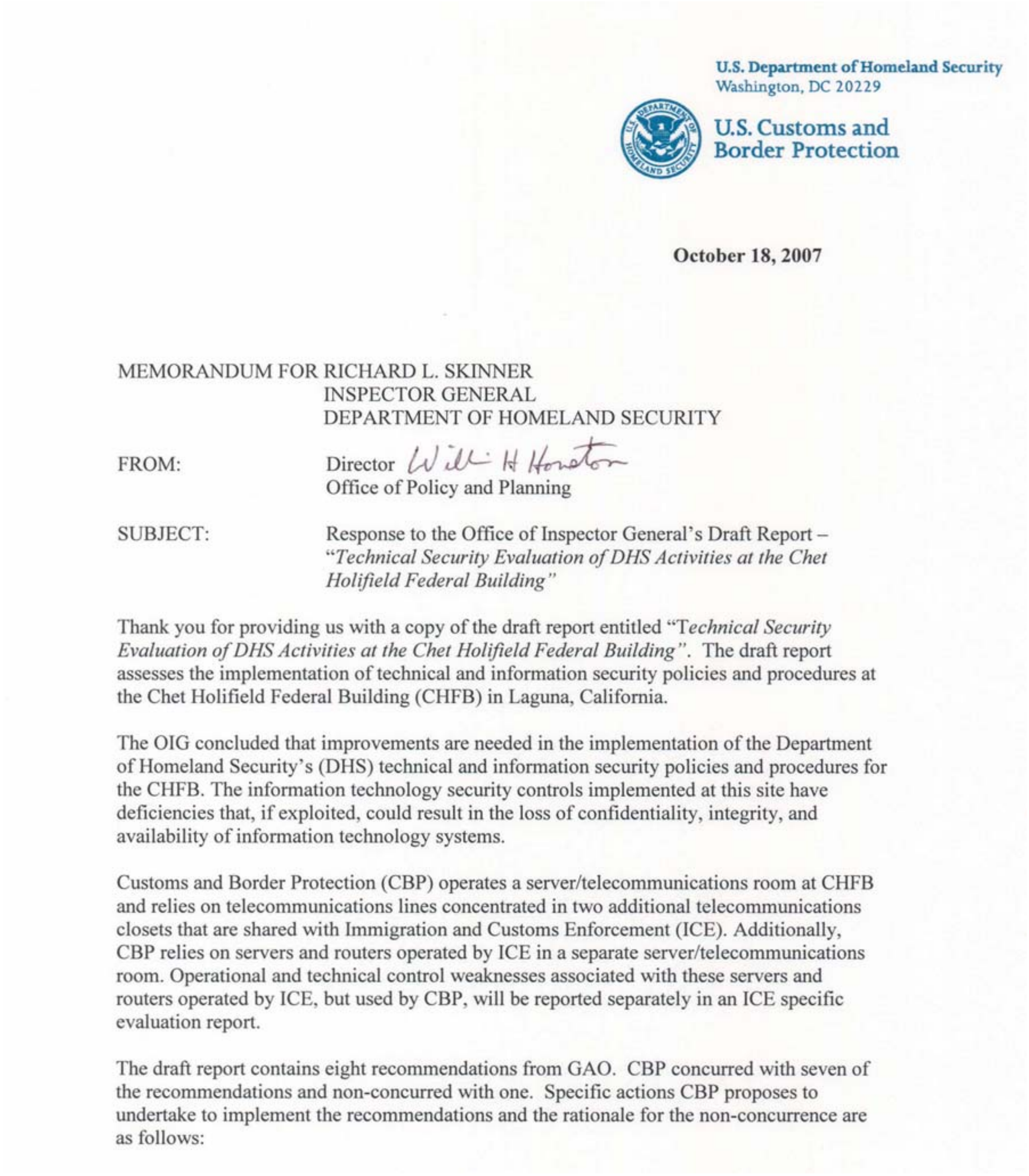
[9] The Rules of Behavior established the boundaries and schedules for the technical evaluations.
[10] We did not find any wireless devices being used by CBP at CHFB.

We provided CBP with briefings concerning the results of fieldwork and the information summarized in this report. We conducted this review between February and August 2007.

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 Office of Inspector General contributors to the review are identified in Appendix C.

## Appendix B
## Management Comments to the Draft Report



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

U.S. Customs and
Border Protection

October 18, 2007

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Director Willi H Honston
Office of Policy and Planning

SUBJECT: Response to the Office of Inspector General's Draft Report – "*Technical Security Evaluation of DHS Activities at the Chet Holifield Federal Building*"

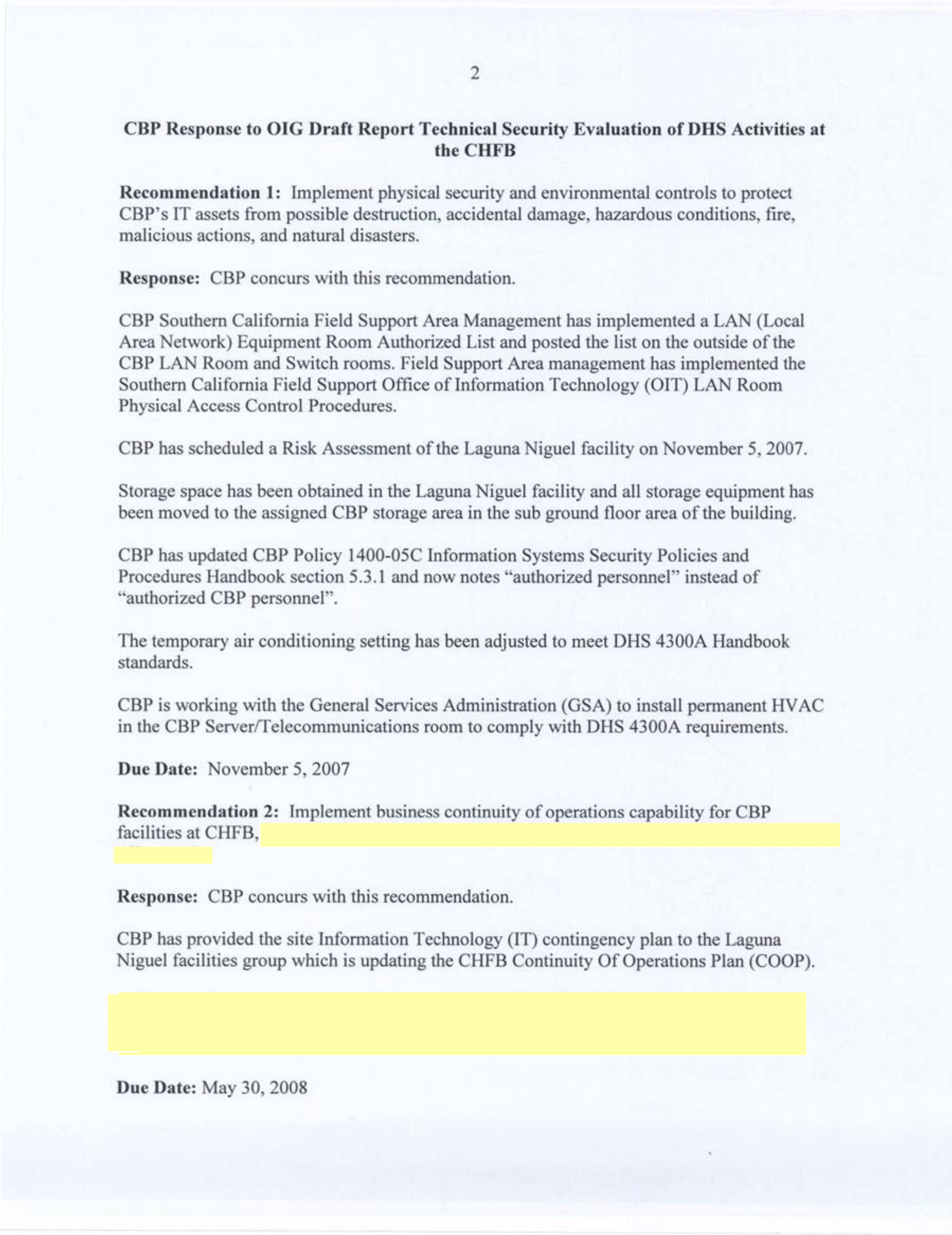
Thank you for providing us with a copy of the draft report entitled "T*echnical Security Evaluation of DHS Activities at the Chet Holifield Federal Building*". The draft report assesses the implementation of technical and information security policies and procedures at the Chet Holifield Federal Building (CHFB) in Laguna, California.

The OIG concluded that improvements are needed in the implementation of the Department of Homeland Security's (DHS) technical and information security policies and procedures for the CHFB. 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 information technology systems.

Customs and Border Protection (CBP) operates a server/telecommunications room at CHFB and relies on telecommunications lines concentrated in two additional telecommunications closets that are shared with Immigration and Customs Enforcement (ICE). Additionally, CBP relies on servers and routers operated by ICE in a separate server/telecommunications room. Operational and technical control weaknesses associated with these servers and routers operated by ICE, but used by CBP, will be reported separately in an ICE specific evaluation report.

The draft report contains eight recommendations from GAO. CBP concurred with seven of the recommendations and non-concurred with one. Specific actions CBP proposes to undertake to implement the recommendations and the rationale for the non-concurrence are as follows:

## Appendix B
## Management Comments to the Draft Report



**CBP Response to OIG Draft Report Technical Security Evaluation of DHS Activities at the CHFB**

**Recommendation 1:** Implement physical security and environmental controls to protect CBP's IT assets from possible destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

**Response:** CBP concurs with this recommendation.

CBP Southern California Field Support Area Management has implemented a LAN (Local Area Network) Equipment Room Authorized List and posted the list on the outside of the CBP LAN Room and Switch rooms. Field Support Area management has implemented the Southern California Field Support Office of Information Technology (OIT) LAN Room Physical Access Control Procedures.

CBP has scheduled a Risk Assessment of the Laguna Niguel facility on November 5, 2007.

Storage space has been obtained in the Laguna Niguel facility and all storage equipment has been moved to the assigned CBP storage area in the sub ground floor area of the building.

CBP has updated CBP Policy 1400-05C Information Systems Security Policies and Procedures Handbook section 5.3.1 and now notes "authorized personnel" instead of "authorized CBP personnel".

The temporary air conditioning setting has been adjusted to meet DHS 4300A Handbook standards.

CBP is working with the General Services Administration (GSA) to install permanent HVAC in the CBP Server/Telecommunications room to comply with DHS 4300A requirements.

**Due Date:** November 5, 2007

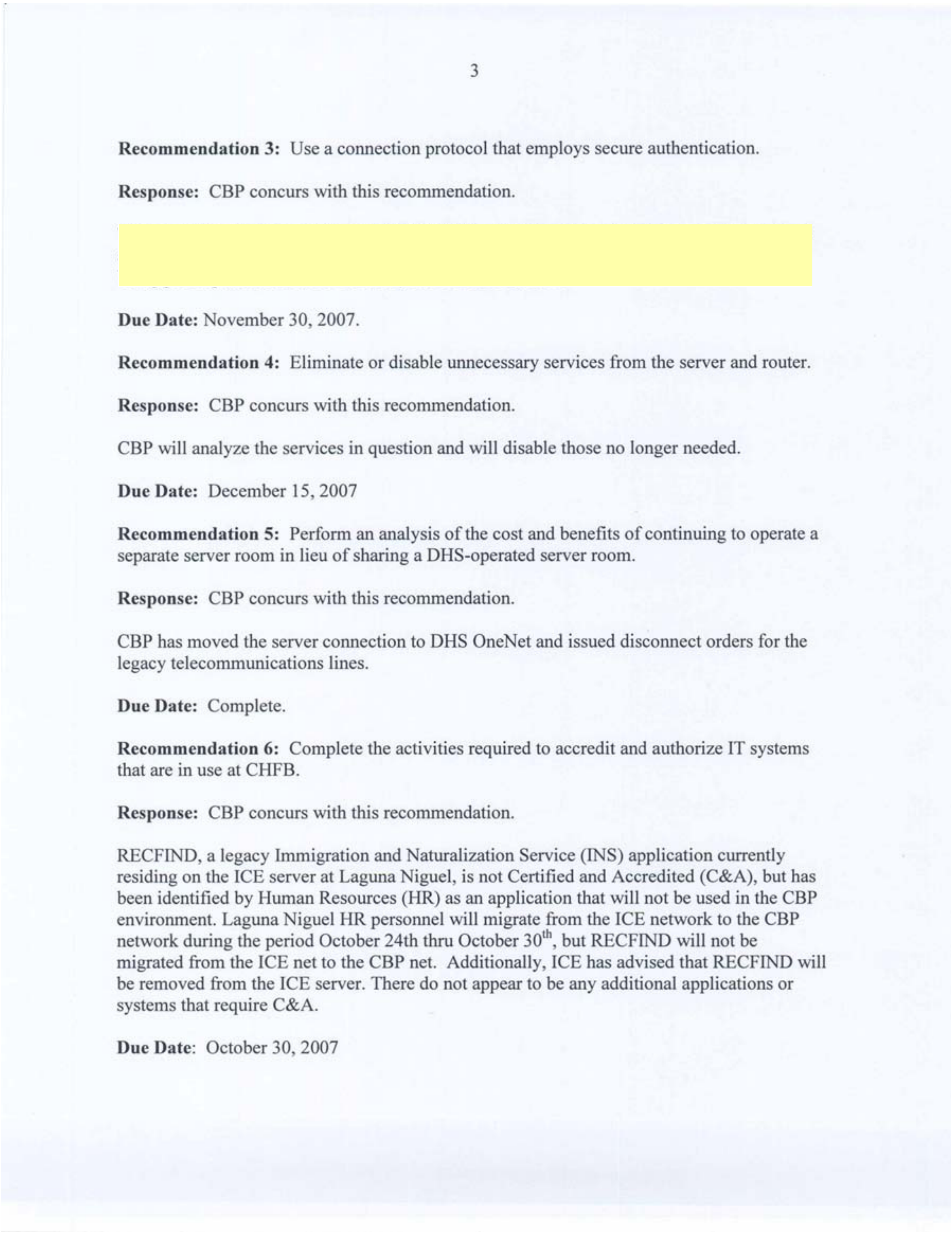
**Recommendation 2:** Implement business continuity of operations capability for CBP facilities at CHFB, [redacted]

**Response:** CBP concurs with this recommendation.

CBP has provided the site Information Technology (IT) contingency plan to the Laguna Niguel facilities group which is updating the CHFB Continuity Of Operations Plan (COOP).

[redacted]

**Due Date:** May 30, 2008



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

**Response:** CBP concurs with this recommendation.

[redacted]

**Due Date:** November 30, 2007.

**Recommendation 4:** Eliminate or disable unnecessary services from the server and router.

**Response:** CBP concurs with this recommendation.

CBP will analyze the services in question and will disable those no longer needed.

**Due Date:** December 15, 2007

**Recommendation 5:** Perform an analysis of the cost and benefits of continuing to operate a separate server room in lieu of sharing a DHS-operated server room.

**Response:** CBP concurs with this recommendation.

CBP has moved the server connection to DHS OneNet and issued disconnect orders for the legacy telecommunications lines.

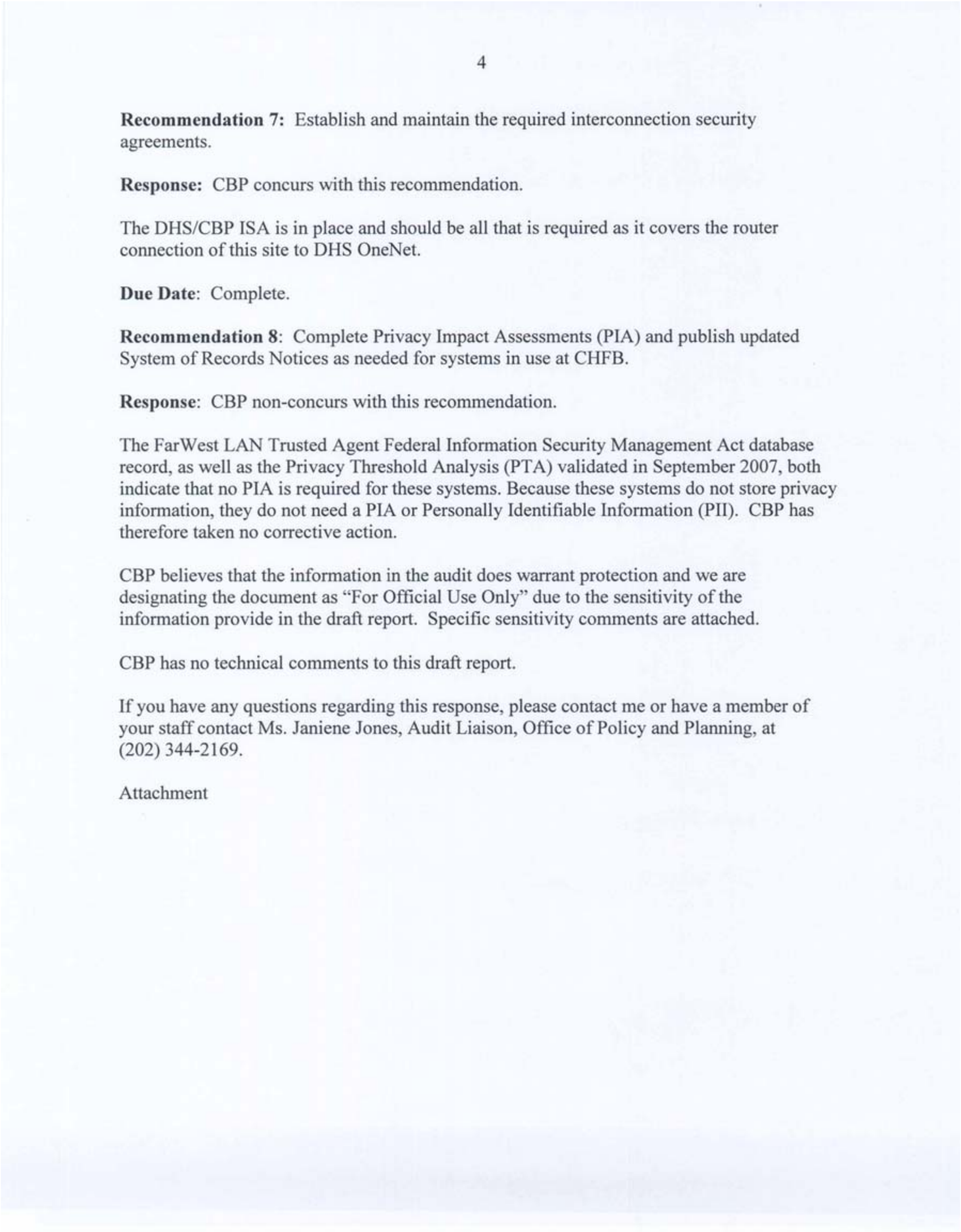
**Due Date:** Complete.

**Recommendation 6:** Complete the activities required to accredit and authorize IT systems that are in use at CHFB.

**Response:** CBP concurs with this recommendation.

RECFIND, a legacy Immigration and Naturalization Service (INS) application currently residing on the ICE server at Laguna Niguel, is not Certified and Accredited (C&A), but has been identified by Human Resources (HR) as an application that will not be used in the CBP environment. Laguna Niguel HR personnel will migrate from the ICE network to the CBP network during the period October 24th thru October 30th, but RECFIND will not be migrated from the ICE net to the CBP net. Additionally, ICE has advised that RECFIND will be removed from the ICE server. There do not appear to be any additional applications or systems that require C&A.

**Due Date:** October 30, 2007



**Recommendation 7:** Establish and maintain the required interconnection security agreements.

**Response:** CBP concurs with this recommendation.

The DHS/CBP ISA is in place and should be all that is required as it covers the router connection of this site to DHS OneNet.

**Due Date**: Complete.

**Recommendation 8**: Complete Privacy Impact Assessments (PIA) and publish updated System of Records Notices as needed for systems in use at CHFB.

**Response**: CBP non-concurs with this recommendation.

The FarWest LAN Trusted Agent Federal Information Security Management Act database record, as well as the Privacy Threshold Analysis (PTA) validated in September 2007, both indicate that no PIA is required for these systems. Because these systems do not store privacy information, they do not need a PIA or Personally Identifiable Information (PII). CBP has therefore taken no corrective action.

CBP believes that the information in the audit does warrant protection and we are designating the document as “For Official Use Only” due to the sensitivity of the information provide in the draft report. Specific sensitivity comments are attached.

CBP has no technical comments to this draft report.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Janiene Jones, Audit Liaison, Office of Policy and Planning, at (202) 344-2169.

Attachment

## 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

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

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

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

Basil Marcus Badley, Technical Evaluator, Department of Homeland Security, Information Technology Audits

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

Samer El-Hage, Management and Program Assistant, Department of Homeland Security, Information Technology Audits

Maria Rodriguez, Referencer, Department of Homeland Security, Information Technology Audits

## Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Under Secretary, Management
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Chief Information Officer
Chief Privacy Officer
Deputy CIO
Chief Information Security Officer
Information Systems Security Manager, CBP
CISO, CBP
DHS Audit Liaison
CBP 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, 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.**