

# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

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



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



Homeland  
Security

May 28, 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.

This report addresses the implementation of technical and information security policies and procedures at U.S. Immigration and Customs Enforcement 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.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General

# Table of Contents/Abbreviations

---

Executive Summary .....	1
Background .....	2
Results of Review .....	4
Systems Did Not Comply Fully With DHS Operational Control Requirements .....	4
Recommendations .....	6
Management Comments and OIG Analysis .....	7
Systems Did Not Comply Fully With DHS Technical Control Requirements .....	7
Recommendations .....	9
Management Comments and OIG Analysis .....	10
Systems Did Not Comply Fully With DHS Management Control Requirements .....	10
Recommendations .....	13
Management Comments and OIG Analysis .....	13

## Appendices

Appendix A: Purpose, Scope, and Methodology .....	14
Appendix B: Management Comments to Draft Report .....	16
Appendix C: ICE Novell Servers with Known Vulnerabilities .....	20
Appendix D: ICE Windows Servers with Known Vulnerabilities .....	21
Appendix E: Certification and Accreditation Status .....	23
Appendix F: Status of Privacy Compliance Activities for ICE Systems .....	24
Appendix G: Major Contributors to This Report .....	25
Appendix H: Report Distribution .....	26

# Table of Contents/Abbreviations

---

## Abbreviations

ACL	Administrative Center Laguna
ATO	Authorization to Operate
CHFB	Chet Holifield Federal Building
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSIRC	Computer Security Incident Response Center
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
IT	Information Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
TA-FISMA	Trusted Agent FISMA
USCIS	U.S. Citizenship and Immigration Services

# OIG

---

*Department of Homeland Security  
Office of Inspector General*

## **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 U.S. Immigration and Customs Enforcement operates the West Area Information Technology Field Operations office.

Our evaluation focused on how Immigration and Customs Enforcement 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 department staff, and conducted technical tests of internal controls, e.g., scans for wireless networks. We also reviewed applicable department 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 their information technology systems. Specifically, Immigration and Customs Enforcement needs to improve its physical security, environmental, and business continuity controls for its computer room and telecommunications closets. Immigration and Customs Enforcement also could improve its technical controls by installing the latest patches, disabling unnecessary ports, and by improving network configuration. Additionally, management controls could be improved by implementing procedures to identify and disconnect unused telecommunications lines and by completing all required certification and accreditation activities. Management concurred with all our 10 recommendations and is taking action to resolve them.

---

## Background

We designed our Technical Security Evaluation Program to provide senior Department of Homeland Security (DHS) officials with timely information on whether they had adequately 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 nonrepudiation within the DHS IT infrastructure and operations. A companion document—the *DHS 4300A Sensitive Systems Handbook* (DHS 4300A Handbook)—provides detailed guidance on the implementation of these policies.

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

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

\*\*\*\*\*

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

\*\*\*\*\*

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

---

Based on our internal analysis, we selected the Chet Holifield Federal Building (CHFb) located in Laguna Niguel, California, where the U.S. Immigration and Customs Enforcement's (ICE) West Area 2 Field Operations office is located. The U.S. Citizenship and Immigration Services (USCIS) and U.S. Customs and Border Protection also operate in this facility, and their activities are addressed in separate evaluation reports.

---

## Results of Review

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

Some operational controls that ICE implemented at CHFEB did not conform to DHS policies; these included physical security, environmental controls, and business continuity. Together, these deficiencies could place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed by ICE at CHFEB.

#### Physical Security Controls

While ICE has implemented some physical security access controls, including the use of badges, card readers, and locked entrances, physical security controls could be strengthened at their CHFEB locations. Specifically, ICE needs to limit access to IT assets in the ICE/USCIS shared server room at CHFEB. Examples of situations that need attention follow:



Figure 1 illustrates how ICE IT assets are located directly behind the printout table and accessible to staff who come to pick up printouts.



*Figure 1: Computer Room Printout Desk*



---

The examples mentioned above increase the risk of unauthorized access to potentially sensitive information and accidental loss of power or damage to IT resources at CHFEB.

According to the DHS 4300A Handbook:

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

### **Environmental Controls**

ICE should maintain its environmental operational controls at prescribed levels by adjusting the heating, ventilation, and air conditioning (HVAC) temperature controls in the telecommunications rooms, in accordance with agency guidance.

ICE's telecommunications equipment was also at risk of failure because of the absence of temperature or humidity sensors in the telecommunications closets. Specifically, eleven ICE telecommunications rooms had temperatures that exceeded 70 degrees. We noted that only two of these rooms had any temperature or humidity sensors.

According to the DHS 4300A Handbook:

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

---

## **Business Continuity**

ICE's business continuity capability also needs to be improved at CHFB. We identified several issues involving ICE IT resources in room 2102, including

- [REDACTED]
- [REDACTED]
- The ICE Public Address system rack could be better secured by bracing it to prevent damage during an earthquake.
- One of the power distribution units is not connected to the emergency power-off switch.

Additionally, the need to connect all power distribution units to the emergency cut-off switch is related to ICE's use of a water-based, fire-suppression system. If all power distribution units are not connected to the emergency shut-off switch, the IT resources that are still receiving power when the sprinklers are activated are at increased risk of short circuit during a fire. Further, ICE cannot ensure that its IT resources will be available when needed without backup generators.

According to the DHS 4300A Handbook:

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

## **Recommendations:**

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

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

**Recommendation #2:** Implement business continuity of operations capability for ICE facilities at CHFB

[REDACTED]

---

## Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the ICE Assistant Secretary. We have included a copy of the comments in their entirety at Appendix B.

In the comments, ICE concurred with these recommendations. We agree that the recommendations are resolved and that planned actions are appropriate to address the issues. Recommendations 1 and 2 will be considered resolved but open pending completion and verification of all planned actions.

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

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

### Operating System Configuration Management

Unsupported operating systems were running on ICE's servers at CHFB. [REDACTED]

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

Our technical scans also identified ICE servers with known vulnerabilities.<sup>1</sup> [REDACTED]

---

<sup>1</sup> See Appendices C and D for inventories of ICE servers with known vulnerabilities.

<sup>2</sup> "Cross-site scripting" is a technique by which a malicious web site operator may apply script, and execute code, in another user's web session.

<sup>3</sup> An attacker is able to gain a list of user names, shares, and other potentially sensitive information by creating a Null session.

---

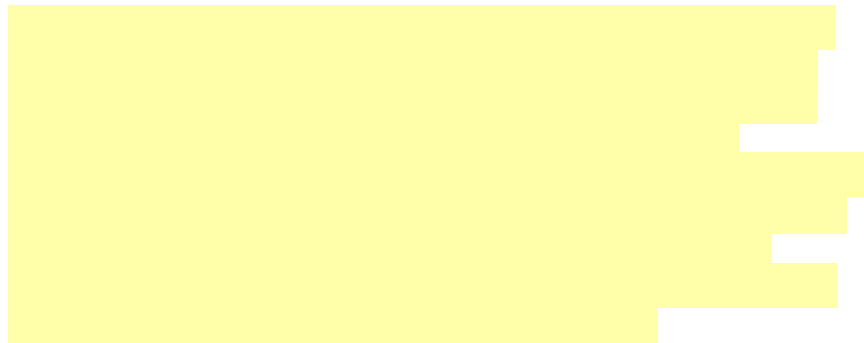
According to DHS Directive 4300A:

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

\*\*\*\*\*

*DHS Components must have provisions for reacting quickly as these critical patches are identified and released by the DHS CSIRC.*

### **Router Configuration Management Controls**



According to DHS Directive 4300A:

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

---

<sup>4</sup>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."

---

## **Password Management Requirements**

ICE password policies did not conform to DHS Directive 4300A or were not consistently applied to all ICE's servers. [REDACTED]

According to the DHS 4300A Handbook:

*Passwords are important because they are often the first line of defense against hackers or insiders who may be trying to obtain unauthorized access to a computer system ... Passwords shall be at least 8 characters in length [and] shall be changed or expire in 180 days or less.*

## **Actions Taken**

ICE took immediate actions to address some of the technical control deficiencies. Specifically, ICE:

- Reconfigured some of the servers from the Windows NT operating system to the Windows 2003 operating system
- Reconfigured its servers from the Novell operating system to Windows 2003 operating system;

[REDACTED]

- [REDACTED]

[REDACTED]

## **Recommendations:**

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

**Recommendation #3:** Develop a migration plan to transition from unsupported operating systems to operating systems for which DHS has a Secure Baseline Configuration Guide.

---

**Recommendation #4:** Implement the password policy established by DHS Directive 4300A.

**Recommendation #5:** Use a connection protocol that employs secure authentication.

**Recommendation #6:** Eliminate or disable unnecessary services from its routers.

**Recommendation #7:** Develop a process for implementing identified patches in a timely fashion.

## **Management Comments and OIG Analysis**

In the comments, ICE concurred with these recommendations. We agree that the recommendations are resolved and that planned actions are appropriate to address the issues. Recommendations 3, 4, 5, 6, and 7 will be considered resolved but open pending completion and verification of all planned actions.

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

ICE'S implementation of management controls at CHFb did not conform to DHS policies. For example, ICE has not maintained accurate IT systems inventories. The lack of an accurate inventory of telecommunications lines places ICE at risk of unnecessary expenditures. Additionally, there are deficiencies in system accreditation, and incomplete privacy compliance activities.<sup>5</sup> These management control deficiencies increase the risk to ICE IT investments, systems, and data from new threats and vulnerabilities for which safeguards have not been implemented.

### **Management of Telecommunications Lines**

ICE did not have an accurate inventory of its telecommunications lines at CHFb. For example, ICE could save \$17,412 annually by disconnecting a nonoperational telecommunications line. Specifically, ICE is paying a \$1,451 monthly fee for a telecommunications line that has not been used since the

---

<sup>5</sup> The Privacy Act of 1974 ("Privacy Act"), 5 U.S.C. § 552a, as amended, provides statutory privacy rights to U.S. citizens and Legal Permanent Residents.

implementation of the DHS OneNet.<sup>6</sup> After determining that this telecommunications line was not being used, we recommended that ICE disconnect the line immediately.<sup>7</sup>

We also identified 33 other active telecommunications lines whose ownership is unknown. If these lines are disconnected, it may result in a monthly cost savings of \$160,220, or \$1.9 million per year. See Figure 2 below for details.

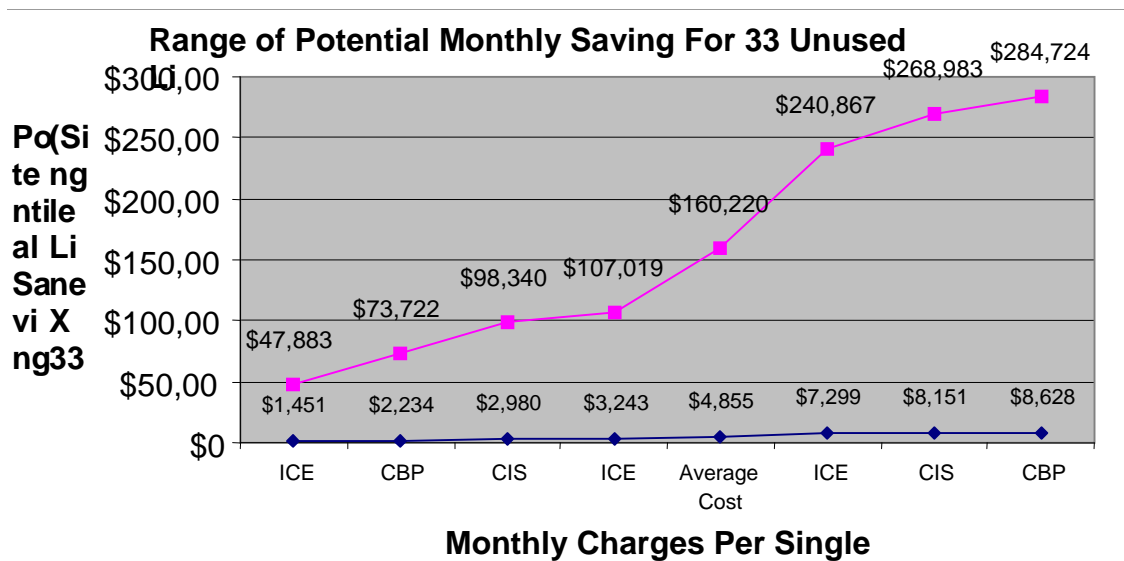


Figure 2: Range of Potential Monthly Savings for 33 Unused Telecommunications Lines<sup>8</sup>

According to DHS 4300A Handbook, component CIOs are to:

*Ensure that an accurate IT systems inventory is established and maintained.*

<sup>6</sup> The DHS OneNet was installed at the CHFB in February 2006 and activated in June 2006.

<sup>7</sup> According to the DHS Infrastructure Project Office, the components are responsible for disconnecting telecommunications lines when the DHS OneNet is installed. Additionally, the DHS Infrastructure Project Office was unable to provide us with documentation of actual cost-savings due to the disconnection of telecommunications lines following the DHS OneNet implementation at any site.

<sup>8</sup> The average monthly fee for seven telecommunications lines at CHFB is \$4,855. The estimated monthly charges for the 33 unclaimed telecommunications lines, based on the average monthly fee, is \$160,215 (33 lines times an average cost of \$4,855 per line). Therefore the potential annual savings is approximately \$1.9 million (\$160,220 x 12 months)

---

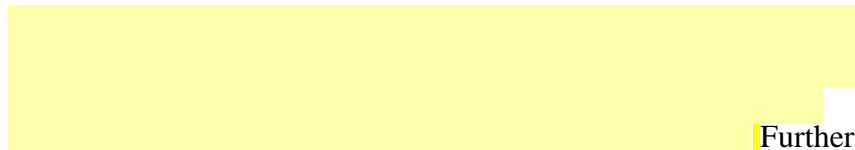
Without an adequate inventory of telecommunications lines, ICE may not know who is accessing their IT resources. Additionally, ICE may be spending money for unnecessary resources

### **System Accreditation Deficiencies**

ICE has not maintained an accurate inventory of the IT systems in use at CHF. <sup>9</sup> Specifically, one of the three ICE systems (33%) in use at CHF is not currently included in DHS' Trusted Agent FISMA (TA-FISMA) reporting tool. <sup>10</sup> At the start of our audit fieldwork, the ICE infrastructure at CHF was included under the Administrative Center Laguna (ACL) entry in TA-FISMA. However, in July 2007, USCIS changed the name of the ACL system to the Western Region and made the system account unavailable to ICE.

According to DHS 4300A Handbook, component CIOs are to:

*Ensure that an accurate IT systems inventory is established and maintained.*

 Further, the authorization to operate for the ICE infrastructure at CHF has expired.

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.*

### **Incomplete Privacy Compliance Activities**

ICE had not completed all privacy compliance activities for ICE systems in use at CHF. Specifically, ICE has completed all required privacy compliance activities for only 1 of 3 (33%) systems in use at CHF. <sup>11</sup> Further, the department has not

---

<sup>9</sup> See Appendix E, *Certification and Accreditation Status*, for the ICE systems that are in operation at CHF.

<sup>10</sup> 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.

<sup>11</sup> See Appendix F, *Status of Privacy Compliance Activities for ICE Systems*, for further information.



---

validated the one Privacy Impact Assessment known to be required.

### **Recommendations:**

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

**Recommendation # 8:** Implement procedures to identify and disconnect unused telecommunications line.

**Recommendation # 9:** Complete the activities required to accredit and authorize IT systems that are in use at CHF B.

**Recommendation # 10:** Complete Privacy Impact Assessments and publish updated System of Records Notices, as needed, for systems in use at CHF B.

### **Management Comments and OIG Analysis**

In the comments, ICE concurred with these recommendations. We agree that the recommendations are resolved and that planned actions are appropriate to address the issues. Recommendations 8, 9, and 10 will be considered resolved but open pending completion and verification of all planned 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 Sensitive Systems Policy Directive 4300A and its companion document, the DHS 4300A Sensitive Systems Handbook.

We coordinated the implementation of this technical security evaluation program with the DHS Chief Information Security Officer (CISO). We mutually agreed to the wording for the Rules of Engagement for the technical testing.<sup>12</sup> Our entrance and exit conferences were held with ICE officials at the Office of Information Technology (OIT) in Washington D.C. and by telephone with CHF B OIT officials.

We performed technical evaluations only after the DHS CISO and ICE agreed to our negotiated Rules of Engagement. These technical evaluations included:

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

We reviewed applicable DHS and ICE policies, procedures, and ICE's responses to our site surveys and technical questionnaires. Prior to performing our onsite review, we used ICE's responses to identify occupied space, server rooms, and telecommunications closets. Our onsite review included a physical review of ICE space, and interviews with ICE staff. Our technical review included onsite reviews of server security policies as well as scans for DHS wireless devices operating at CHF B.<sup>13</sup> Additionally, we reviewed guidance provided by DHS to the components in the areas of patch management, operation systems, and wireless security.

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

---

<sup>12</sup> The Rules of Engagement established the boundaries and schedules for the technical evaluations

<sup>13</sup> We did not find any wireless devices being used by ICE at CHF B.

## Appendix A Purpose, Scope, and Methodology

---

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

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

## Appendix B Management Comments to the Draft Report

---

Office of the Assistant Secretary

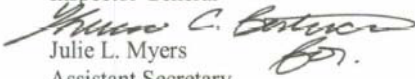
U.S. Department of Homeland Security  
425 I Street, NW  
Washington, DC 20536



U.S. Immigration  
and Customs  
Enforcement

January 4, 2008


MEMORANDUM FOR: Richard L. Skinner  
Inspector General

FROM:   
Julie L. Myers  
Assistant Secretary

SUBJECT: Response to Recommendations: OIG Draft Report "Technical Security Evaluation of U.S. Immigration and Customs Enforcement (ICE) Activities at the Chet Holifield Federal Building" For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)

The following comments are provided to the subject report:

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

ICE Response: ICE concurs with Recommendation 1. ICE is working with U.S. Citizenship and Immigration Services (USCIS), which manages the computer room at the Chet Holifield Federal Building (CHFB), to limit access to only ICE personnel. 



ICE requests that this recommendation be considered resolved and open 





## Appendix B Management Comments to the Draft Report

---

SUBJECT: Response to Recommendations: OIG Draft Report "Technical Security Evaluation of U.S. Immigration and Customs Enforcement Activities at the Chet Holifield Federal Building," For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)  
Page 2 of 4

**Recommendation 2: "Implement business continuity of operations capability for ICE facilities at CHFB, [REDACTED]"**

ICE Response: [REDACTED]

ICE requests that this recommendation be considered resolved and closed.

**Recommendation 3: "Develop a migration plan to transition from unsupported operating systems to operating systems for which DHS has a Secure Baseline Configuration Guide."**

ICE Response: ICE concurs with Recommendation 3. As of December 27, 2007, all unsupported operating systems have been upgraded or retired.

ICE requests that this recommendation be considered resolved and closed.

**Recommendation 4: "Implement the password policy established by DHS Directive 4300A."**

ICE Response: ICE concurs with Recommendation 4. As of December 27, 2007, all systems with password controls that were identified as out of compliance with DHS Directive 4300A have been brought into compliance.

ICE requests that this recommendation be considered resolved and closed.

**Recommendation 5: "Use a connection protocol that employs secure authentication."**

ICE Response: ICE concurs with Recommendation 5. As of December 27, 2007, all insecure connection protocols have been disabled.

ICE requests that this recommendation be considered resolved and closed.

**Recommendation 6: "Eliminate or disable unnecessary services from its routers."**

ICE Response: ICE concurs with Recommendation 6. [REDACTED]

## Appendix B Management Comments to the Draft Report

---

SUBJECT: Response to Recommendations: OIG Draft Report "Technical Security Evaluation of U.S. Immigration and Customs Enforcement Activities at the Chet Holifield Federal Building," For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)  
Page 3 of 4

ICE requests that this recommendation be considered resolved and open pending verification of completion of the necessary activities.

**Recommendation 7: "Develop a process for implementing identified patches in a timely fashion."**

ICE Response: ICE concurs with Recommendation 7. ICE OCIO is working to bring all systems into compliance with security patches. The completion date is scheduled for March 31, 2008.

ICE requests that this recommendation be considered resolved and open pending verification of compliance with security patches.

**Recommendation 8: "Implement procedures to identify and disconnect unused telecommunications line."**

ICE Response: ICE concurs with Recommendation 8. ICE OCIO will implement procedures by June 30, 2008.

ICE requests that this recommendation be considered resolved and open pending verification of acceptable procedures.

**Recommendation 9: "Complete the activities required to accredit and authorize IT systems that are in use at CHF B."**

ICE Response: ICE concurs with Recommendation 9. [REDACTED]  
[REDACTED] All activities will be completed by June 30, 2008.

ICE requests that this recommendation be considered resolved and open pending completion of required certification and accreditation documents.

**Recommendation 10: "Complete Privacy Impact Assessments and publish updated System of Records Notices, as needed, for systems in use at CHF B."**

ICE Response: ICE concurs with Recommendation 10. [REDACTED]  
[REDACTED]  
[REDACTED] All activities will be completed by June 30, 2008.

ICE requests that this recommendation be considered resolved and open pending verification of a new System of Record Notice.

## Appendix B Management Comments to the Draft Report

---

SUBJECT: Response to Recommendations: OIG Draft Report "Technical Security Evaluation of U.S. Immigration and Customs Enforcement Activities at the Chet Holifield Federal Building," For Official Use Only (FOUO)/Law Enforcement Sensitive (LES)  
Page 4 of 4

ICE will provide a Mission Action Plan to the OIG, to identify assignments, timelines for completion and accountable officials to address those recommendations that are not resolved and closed.

Please contact ICE OIG Audit Portfolio Manager Claude Lucas at (202) 514-9226 if there are any questions or concerns regarding this response.

**Appendix C**  
**ICE Novell Servers with Known Vulnerabilities**

---

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]





**Appendix D**  
**ICE Windows Servers with Known Vulnerabilities**

---

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

**Appendix E**  
**Certification and Accreditation Status**

---

		<b>Risk Assessment Status</b>	<b>Accreditation Status</b>
		<b>Expired</b>	<b>ATO</b>
		<b>Completed</b>	<b>ATO</b>
		<b>Completed</b>	<b>Expired</b>

**Appendix F**  
**Status of Privacy Compliance Activities for ICE Systems**

		<b>Privacy Threshold Analysis (PTA)</b>	<b>Privacy Impact Assessment (PIA) Required?</b>	<b>Has the Privacy Impact Assessment (PIA) Been Submitted to the DHS Privacy Office for Validation?</b>	<b>Has a System of Records Notice Been Published?</b>
		<b>PTA Completed</b>	<b>No PIA required</b>	<b>NA</b>	<b>NA</b>
		<b>PTA completed</b>	<b>PIA required</b>	<b>No</b>	<b>Justice/INS -012 DACS 60-FR-52690, 52698, as modified by subsequent system of records notices.</b>
		<b>PTA not submitted to the DHS Privacy Office for validation.</b>	<b>Unknown</b>	<b>NA</b>	<b>DHS/OS1 HSPD-12 Office of Security Files 71 FR 53700</b>

## **Appendix G**

### **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, Senior Program Analyst, Department of  
Homeland Security, Information Technology Audits

Basil Marcus Badley, Senior Security Engineer, 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

Steven Staats, Referencer Program Analyst, Department of  
Homeland Security, Information Technology Audits

## **Appendix H**

### **Report Distribution**

---

#### **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 (CIO)  
Chief Privacy Officer  
Deputy CIO  
Chief Information Security Officer  
Information Systems Security Manager, ICE  
CISO, ICE  
DHS Audit Liaison  
ICE Audit Liaison

#### **Office of Management and Budget**

Chief, Homeland Security Branch  
DHS Program 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](http://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](mailto: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.**