DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Technical Security Evaluation of U.S. Citizenship and Immigration Services Activities at the Chet Holifield Federal Building

OIG-08-02

October 2007

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

Homeland Security

October 15, 2007

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. Citizenship and Immigration Services 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
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ATO	Authorized to Operate
CHFB	Chet Holifield Federal Building
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
FBI	Federal Bureau of Investigation

Table of Contents/Abbreviations

FISMA	Federal Information Security Management Act
HVAC	Heating, Ventilation, and Air Conditioning
ICE	Immigration and Customs Enforcement
ISA	Interconnection Security Agreement
IT	Information Technology
OIG	Office of Inspector General
PIA	Privacy Impact Assessment
PTA	Privacy Threshold Analysis
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 the U. S. Citizenship and Immigration Services operates the California Service Center and the Western Region field office.

Our evaluation focuses on how Citizenship and Immigration Services 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, Citizenship and Immigration Services needs to improve its physical security, environmental, and business continuity controls for its computer room. Citizenship and Immigration Services 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 completing all required certification and 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 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 determined that this technical security evaluation should be performed at a DHS multicomponent location. Based on prior audit coverage of other DHS components, we focused on U. S. Citizenship and Immigration Services (USCIS) locations. Subsequently, we selected the Chet Holifield Federal Building (CHFB) located in Laguna Niguel, California, where the USCIS California Service Center and the USCIS Western Region field office are both located. While the U. S. Customs and Border Protection and U. S. Immigration and Customs Enforcement (ICE) also operated in this facility, their activities will be addressed in separate evaluation reports.

Results of Review

Systems Did Not Comply Fully With DHS Operational Control Requirements

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

Physical Security Controls

While USCIS has implemented some physical security access controls, including the use of badges, card readers, and locked entrances, physical security could be strengthened at their CHFB computer room. Examples of situations that need attention follow:

- USCIS needs more physical security controls to limit access to stored materials. Currently, once staff enter the controlled area, they have access to controlled paper, sensitive printouts, backup tapes, routers, printers, and servers and the telecommunications closet in the computer room. Figure 1 illustrates how printouts are not segregated and restricted, but are commonly placed on a table near the entrance to the computer room. Nearby, USCIS places daily backup tapes for couriers.

Figure 1: Computer Room printout desk

- Server racks and telecommunication closets are left either unlocked or with the key in the lock. For example, a cabinet containing equipment owned by the Federal Bureau of Investigation (FBI) was closed, but the key was inserted in the lock. Anyone with access to the room had access to the FBI's router, as Figures 2 and 3 below show.

Figure 2: FBI router cabinet with key in door

Figure 3: Inside of FBI router cabinet

- A USCIS official said that the cyber locks for the telecommunications closets have not been changed in 3 years. Using cyber locks that have not been changed on a

regular basis could leave the USCIS IT assets vulnerable to loss, theft, destruction, sabotage, or compromise.

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 CHFB.

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

USCIS should maintain its environmental operational controls at proscribed levels by adjusting the heating, ventilation, and air conditioning (HVAC) temperature controls in the computer and telecommunications rooms, in accordance with agency guidance. This is especially a concern for the USCIS computer room, which had temperatures above 70 degrees in February. After we reported this information to USCIS, immediate action was taken to reset the air conditioning controls appropriately.

Additionally, USCIS' communications equipment was also at risk of failure because of the absence of temperature or humidity sensors in the telecommunications closets.

According to the DHS 4300A Handbook:

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

The absence of temperature and humidity sensors and proper HVAC settings for IT equipment increases the risk that USCIS' IT assets may break down.

Business Continuity

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

- An alternate process site has not been identified;
- There is no backup electrical generator to be used in case of a power failure;
- There is only one electrical conduit providing power to the USCIS server room;
- USCIS has not provided redundancy for several servers;
- Several servers are not being backed up;
- Several servers are not connected to a redundant power distribution unit; and
- One of the power distribution units is not connected to the emergency power-off switch.

To give an example in detail, a power distribution unit's display was broken. However, USCIS could not shut this unit down to replace the display without shutting down some servers. Additionally, the need to connect all power distribution units to the emergency cut-off switch is related to USCIS' 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.

Additionally, there is an increased risk from a hardware failure, e.g., a disk crash, could prevent USCIS employees from performing their assigned duties if servers are not backed up or have other redundant capabilities. Further, USCIS cannot ensure that its IT resources will be available when needed without backup generators and an alternate processing facility.

According to the DHS 4300A Handbook:

> *Care must be taken to ensure systems are designed with no single points of failure…DHS must have the capability to ensure continuity of essential functions under all circumstances.*

Recommendations

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

Recommendation #1: Implement stronger physical security and environmental controls to protect USCIS' 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 USCIS facilities at CHFB, including the installation of a backup power supply, the connection of all power distribution units to the emergency power-off control, and the elimination of single points of failure.

Management Comments and OIG Analysis

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

In the comments, the CIO concurred with findings and recommendations one and two in our report. The CIO also stated that USCIS has a plan to improve operational and physical security for IT at CHFB. However, USCIS also stated that, "The plan will be executed when funding is available." This recommendation will be considered resolved but open pending verification of planned actions.

The USCIS response to recommendation two discussed a Continuity of Operations plan to move processing to a 'devolution' site.' We expect the plan of action and milestones for this recommendation to include the establishment of a devolution agreement with the Vermont Service Center and testing of this capability. We also agree with USCIS that the establishment of an uninterruptible power supply is an issue that all the tenants in the CHFB facility should work to resolve. Finally, upon receiving these management comments, we again contacted the USCIS support staff in CHFB. They confirmed that one of the power distribution units is still not connected to the emergency cut-off switch. This recommendation will be considered resolved but open pending verification of planned actions.

Systems Did Not Comply Fully With DHS Technical Control Requirements

USCIS' implementation of technical controls did not conform to DHS policies involving configuration management of operating systems and their router, as well as password management requirements. These deficiencies increase the risk that USCIS IT systems used at CHFB are vulnerable to internal attacks.

Operating System Configuration Management

Unsupported operating systems were running on USCIS' servers at CHFB. Specifically, some USCIS servers were running a release of the Novell operating system that has not been supported by Novell since 2004. Other USCIS servers were running Microsoft Windows NT 4.0, which is no longer supported by Microsoft. Operating systems that are not supported by their vendors do not receive updates or "patches" when a vulnerability or exploitation has been identified.

Additionally, our technical scans identified USCIS servers with known vulnerabilities.[1] For example, even though all DHS components were required by the DHS Computer Security Incident Response Center (CSIRC) to apply the patch MS06-040 by August 17, 2006, we identified 26 servers that were missing this patch.

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.*

According to the DHS 4300A Handbook:

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

[1] See Appendices C and D for an inventory of USCIS servers with known vulnerabilities.

Router Configuration Management Controls

USCIS' router at CHFB is vulnerable to a wide range of attacks because they were running older versions of the Simple Network Management Protocol. Further, this router was not properly configured to prevent an "insider" from gaining unauthorized privileges and information. For example, telnet was being used on the USCIS router. However, telnet does not encrypt login and password credentials. This may allow an attacker to capture login credentials and remotely take control of the router and change or delete configuration files.

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.*

Password Management Requirements

USCIS' password policies did not conform to DHS Directive 4300A or were not consistently applied to all USCIS' servers. Specifically, the policies for password length, history, and age were not consistent on all USCIS servers. Additionally, there were accounts where the password had never been changed, or where the password would never expire.

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.*

Recommendations

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

Recommendation #3: Develop a migration plan to transition from unsupported operating systems to new 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 their servers.

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

Management Comments and OIG Analysis

In the comments, the CIO concurred with these recommendations and also reported steps that USCIS has taken to resolve these issues. We believe that the actions that USCIS has taken and plans to take will resolve the reported issues. These recommendations will be considered resolved but open pending verification of reported actions.

Systems Did Not Comply Fully With DHS Management Control Requirements

USCIS' implementation of management controls at CHFB did not conform to DHS policies. Specifically, there are deficiencies in system accreditation, implementation of wireless devices, missing interconnection security agreements (ISA), and privacy compliance activities related to personal information.[2] These management control deficiencies increase the risk to USCIS IT investments, systems, and data from new threats and vulnerabilities for which safeguards have not been implemented.

[2] 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.

System Accreditation Deficiencies

USCIS currently is using 21 systems at CHFB.[3] However, only 7 of the 21 (33%) are currently authorized to operate.[4] The authorization to operate has expired for nine (43%) systems and USCIS has not started the accreditation process for the remaining five (24%) systems. See Figure 4 below.

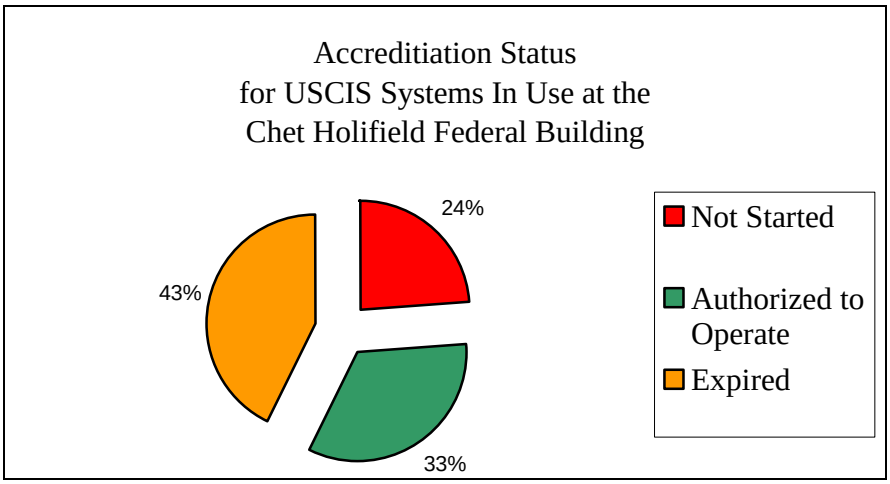

Figure 4

Additionally, 3 of the 7 (43%) systems that are authorized to operate have expired risk assessments. USCIS Designated Accrediting Authorities (DAA) cannot determine if security controls for USCIS systems and data are adequate unless risk assessments are performed regularly.

[3] An additional system, the Laguna Administrative Center, is currently in the USCIS TA-FISMA Inventory. However, this system was not included in this report's inventory because ICE and USCIS are in the process of determining who has responsibility for this system.

[4] See Appendix E, Accreditation and Risk Assessment Status for USCIS Systems, for details.

According to DHS Directive 4300A:

> *Components shall conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment have been made, or every 3 years, whichever occurs first.*

Further, USCIS management cannot be assured that IT systems and data are adequately secured unless the various activities leading to accreditation are performed and the DAA has accepted in writing the risks associated with operating the systems.

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 four additional IT resources that USCIS had not previously included in the DHS' Trusted Agent FISMA (TA-FISMA) reporting tool.[5] Staff from USCIS and the office of the DHS Chief Information Security Officer (CISO) are in the process of determining if these IT resources should be part of the accreditation process.[6] IT resources that are not included in the accreditation process may not be adequately secured, increasing the risk to USCIS 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.*

[5] 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.
[6] See Appendix F, USCIS IT Resources In Use But Not Included In Trusted Agent-FISMA, for names of these IT resources.

Misconfigured Wireless Devices

USCIS' onsite implementation of management controls at CHFB did not ensure that its wireless devices were properly configured. Specifically, wireless keyboards and mice were attached to devices belonging to the Western Region Office, which is one of the IT Resources not in TA-FISMA. These wireless devices were running Wired Equivalent Privacy, which is the oldest version of the wireless security protocol. This security protocol version is vulnerable to both replay attacks and integrity violations.

According to the DHS 4300A Handbook Attachment Q1, Sensitive Wireless Systems:

> *[Wireless Local Area Network] WLAN systems should meet the Wi-Fi Alliance Wireless Protected Access 2 (WPA2) interoperability standard that is based on the Institute for Electrical and Electronics Engineers (IEEE) 802.11i security standard.*

Missing Interconnection Security Agreements

During our fieldwork, we documented several interconnections between USCIS systems and systems operated by other agencies and DHS components. USCIS agrees that the required interconnection security agreements for these systems exist, but they were unable to provide them. Specifically, interconnection security agreements should be established and maintained for connections between the USCIS California Service Center Local Area Network and the following:

- The DHS OneNet,
- The U. S. Coast Guard Marine Information for Safety and Law Enforcement,
- Department of Justice mainframe legacy applications,
- The Executive Office of Immigration Review – Court Inquiry information system,
- The FBI Integrated Automated Fingerprint Information Systems,
- The State Department's Integrated Visa Allocation Management System, and
- The Pitney Bowes mail information database.

Additionally, USCIS should have interconnection security agreements with ICE for IT and telecommunication services.

By not establishing and maintaining interconnection security agreements, USCIS 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 systems…ISAs shall be reviewed as a part of the annual FISMA self-assessment.*

Incomplete Privacy Compliance Activities

USCIS had not completed all privacy compliance activities for USCIS systems in use at CHFB. Specifically, only 3 of 21 (14%) of USCIS systems in TA-FISMA have completed all required privacy compliance activities.[7] Further, the Department has validated only 1 of the 16 (6%) Privacy Impact Assessments (PIA) known to be required for these systems. One of the systems without a PIA is the Offshore Migrant Information Tracking System. This system, which contains actual data, is listed in TA-FISMA as a 'Developmental' system.

According to the DHS Privacy Office's Privacy Impact Assessments Official Guidance:

> *The PIA requirement does not provide an exemption for pilot testing a program or system. If a PIA is ultimately required for a system, any pilot of that system must have the PIA completed prior to the pilot launch. This applies even if the pilot initially plans to use anonymous data but*

[7] See Appendix G, Status of *Privacy Act* Related Activities for USCIS Systems in Use at the Chet Holifield Federal Building, for detailed information on incomplete Privacy Act activities.

will use personally identifiable information as it moves out of pilot.

Additionally, while the department has issued three new public notices for systems in use at the CHFB, there are three other legacy System of Records Notices that no longer accurately report the owners of the systems.[8]

USCIS and DHS Privacy Office officials have told us that the Savings Provision of the Homeland Security Act of 2002 allows DHS to rely on legacy system of records notices.[9]

Recommendations

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

Recommendation #8: Complete the activities required to accredit and authorize IT systems that are in use at CHFB.

Recommendation #9: Properly configure wireless devices prior to installation.

Recommendation #10: Establish and maintain the required interconnection security agreements.

Recommendation #11: 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, the CIO concurred with these recommendations and also reported steps that USCIS has taken to resolve these issues. Regarding recommendation eight, USCIS stated that all systems were authorized to operate. However, a review of TA-FISMA showed that the systems that were not authorized to

[8] The three legacy Systems of Records Notices are Justice/INS-013, CLAIMS 3/4 (67 FR 64132), Justice/INS-031 RNACS (67 FR 20996), and DOT/CG 679 MISLE (67 FR 19612).

[9] 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.*

operate during our fieldwork have now been authorized to operate even though the required certification package has not been completed or the Privacy Impact Assessment has not been performed. We have updated the table in Appendix E to reflect actions that USCIS has taken.

Additionally, USCIS reported that APPLES and CASE Status Online were subsystems of CLAIMS 3 LAN. However, a review of TA-FISMA screens, and two CLAIMS 3 LAN artifacts did not list these as subsystems. Separately, USCIS reported that the Western Regional Office is in TA-FISMA. We are aware that USCIS changed the name of the 'Administrative Center Laguna' to 'Western Regional Office' in TA-FISMA in August 2007. However, USCIS has not updated all the TA-FISMA artifacts to reflect this change. Recommendation eight will be considered resolved but open pending verification of planned actions.

In addition to their written comments, USCIS staff also informed us that the new Information Systems Security Officer for the Western Regional Office removed the non-compliant wireless keyboards and mice. Recommendation nine will be considered resolved but open pending verification of planned actions.

USICS also agreed with recommendations 10 and 11. These recommendations will be considered resolved but open pending verification of planned actions

Purpose, Scope, and Methodology

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

We coordinated the implementation of this technical security evaluation program with the DHS CISO. We mutually agreed to the wording for the Rules of Behavior for the technical testing.[10] Our entrance and exit conferences were held with USCIS 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 USCIS 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 USCIS policies and procedures and USCIS' responses to our site surveys and technical questionnaires. Prior to performing our onsite review, we used USCIS' responses to identify occupied space, server rooms, and telecommunications closets. Our onsite review included a physical review of USCIS space and interviews with USCIS staff. Our technical review included onsite reviews of server security policies as well as scans for DHS wireless devices operating at CHFB. Additionally, we reviewed guidance provided by DHS to the components in the areas of patch management, operation systems, and wireless security.

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

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

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

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

Management's Comments to the Draft Report

U.S. Department of Homeland Security
20 Massachusetts Avenue, NW
Washington, D.C. 20529

U.S. Citizenship and Immigration Services

SEP 14 [redacted]

To: Frank Deffer
Assistant Inspector General
Information Technology

From: Jonathan Scharfen
Deputy Director

Re: OIG Draft Report: Technical Security Evaluation of United States Citizenship and Immigration Services Activities at the Chet Holifield Federal Building

We appreciate the opportunity to review and comment on the subject report and generally agree with your summary of the issues identified in the report. We acknowledge that we still have a great deal to do. I want to assure you that addressing these issues is a high priority for USCIS. Your insight to our challenges and recommendations for improvement will continue to serve us well.

1. Implement physical security and environmental controls to protect USCIS' IT assets from possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

   USCIS formulated a plan during the second quarter FY 2007, prior to the OIG visit, to reconfigure the computer room to include a front desk counter where users will sign for reports. Additionally, there will be one controlled entry/exit. The other set of computer room doors will be exit-only and alarmed. The plan will be executed when funding is made available.

   The temperature controls were addressed while the OIG was on-site. The computer room has temperature and humidity sensors; however, the telecommunications closets are part of the overall building Heating, Ventilation, and Air Conditioning (HVAC) and are not separately controlled.

   To address the issue noted on page five of the draft report, servers owned by the Federal Bureau of Investigation are located in cabinets within a secure, controlled computer room. Only designated personnel have access to the computer room. The keys have been removed from the cabinet doors.

2. Implement business continuity of operations capability for USCIS facilities at CHFB, including the installation of a backup power supply, the connection of all power distribution units to the emergency power-off control, and the elimination of single points of failure.

www.uscis.gov

USCIS' California Service Center (CSC) Continuity of Operations Plan (COOP) addresses movement to an alternate site and to a devolution site to continue essential functions. The COOP will be executed at the discretion of USCIS management should a natural or man-made emergency create a condition where we are not able to continue our essential functions from this site.

The Western Region Office's COOP addresses movement to an alternate site to continue the essential functions and can be implemented when needed.

The draft report seems to indicate that all servers should be identified as "Essential" and therefore DHS Sensitive Systems Policy Management Directive 4300A requires that "Essential" functions not have a single point of failure. Not all servers in the Chet Holifield Federal Building have been identified as "Essential" that require a real-time failover capability. The ability to reconstitute and recover within the normal area of operations, plus 30-days plan, under the COOP is inherent. Providing real-time failover to remove non-essential single points of failure is a very high cost and un-needed standard that is not in alignment with MD4300A. However, when discussing a mirror replacement of the CSC power requirement, the CSC is within the area of normal operations, plus 30-days plan, under the COOP. For this reason, the issue of redundant, uninterrupted power for OIT systems at the Chief Holifield Federal Building is best discussed as a facilities issue, rather than a COOP issue. It is more relevant to day-to-day operations, and not COOP.

All power distribution units are connected to the emergency cut-off switch, including the newest unit noted on page seven of the draft report.

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

   The Novell operating system has been removed from both the California Service Center and Western Region Office LAN. The operating system for both of these USCIS LAN's is no longer a hybrid Microsoft Active Directory/Novell operating system. The Biometrics Retrieval Unit servers running Microsoft Windows NT 4.0 have been targeted for replacement. The CLAIMS 4 servers have been upgraded to Windows 2003 servers with appropriate patches in place.

4. Implement the password policy established by DHS directive 4300A.

   The password policy non-conformance cited on page nine of the draft report related specifically to the Novell servers. The Novell servers have been turned off. The Chet Holifield Federal Building is in compliance with the DHS 4300A password policy guidance.

5. Use a connection protocol that employs secure authentication.

   The router referenced on page nine of the draft report that uses telnet is identified as a U.S. Immigration and Customs Enforcement (ICE) router. USCIS infrastructure is in transition to separate from ICE as part of the Basic Automation Support Infrastructure for Citizenship Services (BASICS). All routers within the Chet Holifield Federal Building will be replaced as part of the BASICS Program.

6. Eliminate or disable unnecessary services from their server.

   The unnecessary service that was identified on the web server has been turned off.

7. Develop a process for implementing identified patches in a timely fashion.

   The Citrix servers identified were patched in July 2007. Research was required to ensure the patches would not negatively impact the server operation. All other Windows patches are installed upon notification by the DHS Computer Security Incident Response Center and completion of Change Management verification as required by DHS 4300A.

8. Complete the activities required to accredit and authorize IT systems that are in use at CHFB.

   Systems identified in Appendix E in the draft report, with the exception of the Automated Premium Process LAN E-Mail System (APPLES), CASE Status Online, and the Center Activity Tracking Systems (CATS), are Authorized to Operate.

   APPLES is a subsystem of CLAIMS 3 LAN and is not a standalone system that requires certification and accreditation.

   CASE Status Online is a subsystem of CLAIMS 3 LAN and is not a standalone system that requires certification and accreditation.

   CATS records an adjudicators' and clerks' time and daily activities. This includes the number of all forms and reports processed, IBIS checks, and e-mail's handled, meetings attended, etc., for G22 reporting purposes. An evaluation of this system is underway to determine if it should be added to the Trusted Agent (TA) FISMA inventory and undergo certification and accreditation.

   Systems identified in Appendix F of the draft report are under evaluation. The Enterprise Digital Mail Meter system will be accounted for under the local General Support System. The Western Regional Office is in the TA FISMA inventory. Project Aware and CIS training calendar are under review.

9. Properly configure wireless devices prior to installation.

   The wireless mice and keyboard devices identified as a deficiency on page 12 in the draft report are running the "Wired Equivalent Privacy" protocol and do not meet the wireless standard adopted by DHS which is the Wi-Fi Alliance Wireless Protected Access 2 (WPA2) standard based upon the Institute of Electrical and Electronics Engineers (IEEE) 802.11i security standard. The current wireless equipment can not be upgraded to meet the IEEE 802.11i standard.

   DHS 4300A Attachment Q1 states: "In accordance with DHS Sensitive Systems Policy Directive 4300A, DHS Wireless Communications Policy stipulates that wireless communications technologies are prohibited from use within DHS unless the appropriate Designated Accrediting Authority specifically approves the technology and application."

   USCIS is investigating the options to either a.) eliminate the use of wireless mice and keyboards, or b.) use wireless equipment in compliance with WPA2 in accordance with the DHS 4300A.

10. Establish and maintain the required interconnection security agreements.

    We agree that interconnection security agreements should be established and maintained. Many of USCIS' programs are legacy programs prior to the establishment of DHS and USCIS. Additionally, we agree that a review of all interconnection security agreements should be conducted as part of the infrastructure separation from ICE and as a part of the annual FISMA self-assessment per DHS 4300A.

    Interconnections between DHS components require an interconnection security agreement when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. Interconnection security agreements shall be signed by both Designated Accrediting Authorities or by the official designated by the Designated Accrediting Authority to have signatory authority.

11. Complete privacy impact assessments and publish updated System of Records Notices as needed for systems in use at CHFB.

    Of the three purported systems lacking Privacy Impact Assessments, two are subsystems of CLAIMS 3 LAN and do not contain separate databases. The third purported system is CATS. A Privacy Threshold Analysis will be conducted that verifies there is no privacy information recorded in CATS.

In closing, we too express our appreciation for the members of your team who participated in drafting the report. If you have any questions please contact Kathleen Stanley, Chief, Internal Review Division, Office of Security and Integrity, USCIS Audit Liaison, at 202-272-1982.

cc: Inspector General

USCIS Novell Servers with Known Vulnerabilities

Vulnerability	Number of USCIS Servers At CHFB With This Vulnerability
The Lightweight Directory Access Protocol – a Null bind entry that allows a user to access this protocol anonymously to view files on the protocol directory.	1
It is possible to guess the community name of the remote Simple Network Management Protocol.	1
An attacker could access the Lightweight Directory Access Protocol schema to gain information about this protocol server.	1

USCIS Windows Servers with Known Vulnerabilities

Vulnerability	Number of USCIS Servers at CHFB With This Vulnerability
Messenger service is a security hazard – this service may be used to commit a denial of service attack or social engineer on the network.	**1**
Arbitrary code can be executed on the remote host due to a flaw in the Local Security Authority Server Service. This may allow an attacker to execute arbitrary code on the remote host with system privileges.	9
The scanning tool was able to enumerate the network share names by connecting the remote host using a Null or guest session. This can allow an attacker the ability to escalate privileges as well as provide the location of critical files.	1
The Secure Sockets Layer certificate on the remote service expired. This means that the remote management cannot guarantee the validity of the certificate being accepted.	1
Vulnerability exists in the Microsoft Abstract Syntax Notation One library that could allow code execution on an affected system.	9
Buffer overflow vulnerability exists within Microsoft Server Service Remote Code Execution, which may allow for a remote, anonymous attacker to execute arbitrary code on a host.	26
Microsoft SQL System Administrator account was not password protected. This means that a remote attacker can log into the SQL server with administrative privileges.	2
A Null session occurs when an attacker sends a blank username and blank password to try to connect to the Inter Process Communications and then an attacker is able to gain a list of user names, shares, and other sensitive information.	20

Appendix D
USCIS Windows Servers with Known Vulnerabilities

Vulnerability	Number of USCIS Servers at CHFB With This Vulnerability
An unspecified remote code execution exists in the Simple Network Management Protocol service that could allow an attacker to take complete control of the affected system.	7
Account locked out – users account has been locked out due to an excessive number of incorrect login attempts. This may indicate that an attacker is trying to guess the account's password through brute force.	4
Anonymous File Transfer Protocol is enabled. Access to this protocol can lead to attacker gaining information about the system that can possibly allow the attacker to gain access to the system.	3
Buffer overflow exists within Microsoft's Network Connection Manage, which may allow an attacker to send a specially crafted request to a vulnerable host to cause denial of service.	1
Symantec pcAnywhere weak encryption allowed. This service provides connectivity to Microsoft Windows system. PcAnywhere can be configured to allow remote access without encryption or with a weak proprietary encryption scheme.	1
A user account was detected with no required password. This allows an attacker unauthorized access, including the ability to take over and replace processes, and access other computers on the network.	2
It is possible to make the remote File Transfer Protocol server crash by sending the command 'STAT*?AAA…AAA. An attacker may use this flaw to prevent a system from distributing files.	1
It is possible to anonymously read the event logs of the remote Windows 2000. An attacker may use this flaw to anonymously read the system logs of the remote host.	1

Appendix D
USCIS Windows Servers with Known Vulnerabilities

Vulnerability	Number of USCIS Servers at CHFB With This Vulnerability
The Citrix server is configured in a way that may allow an external attacker to enumerate remote services.	8
The echo service was detected as running. This service uses port 7/tcp and can be spoofed into sending data from service on one computer to service on another computer.	1
The service "Routed," was active on the server's router port. This service uses port 520/tcp or an application using routing information protocol, which provides to an attacker a host's routing information.	1

Appendix E
Certification and Accreditation Status

Green: Authorized to Operate (during fieldwork)	Yellow: Authorization had expired (during fieldwork)	Red: Authorization work has not started

Certification and Accreditation Status

TA-FISMA Identifier	System Name	Risk Assessment Status	Accreditation Status	Current Accreditation Status
CIS-00054-MAJ-00054	Benefits Biometrics Support System (BBSS)	Completed	Authorized to Operate (ATO)	ATO
CIS-00057-MAJ-00057	Citizenship and Immigration Service Centralized Oracle Repository (CISCOR)	Completed	ATO	ATO
CIS-00081-MAJ-00081	National File Tracking System (NFTS)	Completed	ATO	ATO
CIS-00087-MAJ-00087	Scheduling and Notification of Applicants for Processing (SNAP)	Completed	ATO	ATO
CIS-00084-MAJ-00084	RAFACS - Receipt and Alien File Accountability and Control System, Version 2.9	Expired	ATO	ATO
CIS-00085-MAJ-00085	Reengineered Naturalization Application Casework System (RNACS)	Expired	ATO	ATO
CIS-00086-MAJ-00086	Refugee, Asylum, and Parole System (RAPS)	Expired	ATO	ATO

Appendix E
Certification and Accreditation Status

Green: Authorized to Operate (during fieldwork)	Yellow: Authorization had expired (during fieldwork)	Red: Authorization work has not started

TA-FISMA Identifier	System Name	Risk Assessment Status	Accreditation Status	Current Accreditation Status
CIS-00073-MAJ-00073	Integrated Card Production System (ICPS) (formerly Integrated Document Production (IDP)). Subsystem: National Production Results (NPR)	Completed	Expired	ATO signed on 7/30/2007 without complete certification package
CIS-00109-MAJ-00109	Fraud Detection and National Security Data System (FDNS DS)	Completed	Expired	ATO signed on 7/30/2007 without complete certification package
CIS-00056-MAJ-00056	Alien File/Central Index System (A-File/CIS)	Expired	Expired	ATO signed on 7/30/2007 without complete certification package
CIS-00058-MAJ-00058	CLAIMS 3 Mainframe - Computer Linked Application Information Management System Mainframe	Expired	Expired	ATO signed on 7/31/2007 without complete certification package
CIS-00059-MAJ-00059	CLAIMS3 LAN - Computer Linked Application Information Management System 3 LAN.	Expired	Expired	ATO signed on 8/01/2007 without complete certification package

Appendix E
Certification and Accreditation Status

Green: Authorized to Operate (during fieldwork)	Yellow: Authorization had expired (during fieldwork)	Red: Authorization work has not started

TA-FISMA Identifier	System Name	Risk Assessment Status	Accreditation Status	Current Accreditation Status
CIS-00060-MAJ-00060	CLAIMS4 - Computer Linked Application Information Management System 4	Expired	Expired	ATO signed on 7/30/2007 without complete certification package
CIS-00062-MAJ-00062	Customer Relationship Interface System (CRIS)	Expired	Expired	ATO signed on 7/31/2007 without complete certification package
CIS-00092-GSS-00092	California Service Center (CSC).	Expired	Expired	ATO signed on 7/30/2007 without complete certification package
CIS-00064-MAJ-00064	Electronic Filing System (E Filing)	In Progress	Expired	Two year ATO signed on 7/31/2007 without a validated Privacy Impact Assessment[11]
CIS-00153-MAJ-00153	Alien Change of Address (AR-11)	Completed	Not Started	ATO signed on 7/30/2007 without complete certification package

[11] According to the DHS 4300A Handbook, interim authorizations to operate are only allowed for systems in development testing and prototype systems.

Appendix E
Certification and Accreditation Status

Green: Authorized to Operate (during fieldwork)	Yellow: Authorization had expired (during fieldwork)	Red: Authorization work has not started

TA-FISMA Identifier	System Name	Risk Assessment Status	Accreditation Status	Current Accreditation Status
CIS-03370-MAJ-03370	Offshore Migrant Information Tracking System (OMITS)	Not Started	Not Started	Not Started
(Not in TA FISMA)	Automated Premium Process LAN E-Mail System (APPLES)			
(Not in TA FISMA)	CASE Status Online			
(Not in TA FISMA)	Center Activity Tracking System (CATS)			

USCIS IT Resources in Use but Not Included in Trusted Agent FISMA

IT Resource Name
CIS Training calendar
Project Aware
CIS Western Region Office[12]
Enterprise Digital Mail Meter System

[12] USCIS has created an entry in TA-FISMA for this system but has not updated all the associated artifacts.

Appendix G
Status of Privacy Compliance Activities for USCIS Systems

Green: In compliance.	Yellow: DHS work has been started.	Red: DHS work has not started.

Status of Privacy Compliance Activities for USCIS Systems

TA-FISMA Number	System Name	Privacy Threshold Analysis (PTA)	Privacy Impact Assessment (PIA) Required?	Has the Privacy Impact Assessment (PIA) Been Submitted to the DHS Privacy Office for Validation?	Applicable System of Record Notice According to DHS Privacy Office
CIS-00056-MAJ-00056	Alien File/Central Index System (A-File/CIS)	PTA completed	PIA required	Yes. Reviewed and Approved.	DHS-USCIS-001 A-File – CIS (72 FR 1755) (Supersedes: Justice/INS-001A)
CIS-00092-GSS-00092	California Service Center (CSC).	PTA Completed	No PIA required	NA	NA
CIS-00081-MAJ-00081	National File Tracking System (NFTS)	PTA Completed	No PIA is required	NA	DHS-USCIS-001 A-File – CIS (72 FR 1755)
CIS-03370-MAJ-03370	Offshore Migrant Information Tracking System (OMITS)	PTA completed	PIA required	No	DOT/CG 679 MISLE (67 FR 19612)
CIS-00153-MAJ-00153	Alien Change of Address (AR-11)	PTA completed	PIA required	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00109-MAJ-00109	Fraud Detection and National Security Data System (FDNS DS)	PTA Complete	PIA required	PIA is in progress for FDNS DS	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00087-MAJ-00087	Scheduling and Notification of Applicants for Processing (SNAP)	PTA completed	PIA required, covered by CLAIMS 3	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00086-MAJ-00086	Refugee, Asylum, and Parole System (RAPS)	PTA completed	PIA required	No	DHS-USCIS-001 A-File - CIS (72 FR 1755)

Appendix G
Status of Privacy Compliance Activities for USCIS Systems

Green: In compliance.	Yellow: DHS work has been started.	Red: DHS work has not started.

TAF Number	System Name	Privacy Threshold Analysis (PTA)	Privacy Impact Assessment (PIA) Required?	Has the Privacy Impact Assessment (PIA) Been Submitted to the DHS Privacy Office for Review?	Applicable System of Record Notice According to DHS Privacy Office
CIS-00085-MAJ-00085	Reengineered Naturalization Application Casework System (RNACS)	PTA completed	PIA required	No	Justice/INS-031 RNACS (67 FR 20996)
CIS-00084-MAJ-00084	RAFACS - Receipt and Alien File Accountability and Control System, V 2.9	PTA completed	PIA required	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00073-MAJ-00073	Integrated Card Production System (ICPS) (formerly Integrated Document Production (IDP)).	PTA completed	PIA required	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00062-MAJ-00062	Customer Relationship Interface System (CRIS)	PTA completed	PIA required	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00060-MAJ-00060	CLAIMS4 - Computer Linked Application Information Management System 4	PTA completed	PIA required	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00059-MAJ-00059	CLAIMS3 LAN - Computer Linked Application Information Management System 3 LAN.	PTA completed	PIA required. PIA being drafted.	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00058-MAJ-00058	CLAIMS 3 Mainframe - Computer Linked Application Information Management System Mainframe	PTA completed	PIA required	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00057-MAJ-00057	Citizenship and Immigration Service Centralized Oracle Repository (CISCOR)	PTA completed	PIA required, covered by CLAIMS 3	No	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
CIS-00054-MAJ-00054	Benefits Biometrics Support System (BBSS)	PTA completed	PIA required	*	DHS/USCIS-003 BSS (72 FR 17172)

*** DHS has not provided the Privacy Impact Assessment for this system.**

Appendix G
Status of Privacy Compliance Activities for USCIS Systems

Green: In compliance.	Yellow: DHS work has been started.	Red: DHS work has not started.

TAF Number	System Name	Privacy Threshold Analysis (PTA)	Privacy Impact Assessment (PIA) Required?	Has the Privacy Impact Assessment (PIA) Been Submitted to the DHS Privacy Office for Review?	Applicable System of Record Notice According to DHS Privacy Office
CIS-00064-MAJ-00064	Electronic Filing System (E Filing)	PTA completed	PIA required	PIA not yet validated.	Justice/INS-013, CLAIMS 3/4 (67 FR 64132)
	APPLES- Automated Premium Process LAN E-Mail System	PTA not received as of 6/6/07			
	CASE System Online	PTA not received as of 6/6/07			
	CATS – Center Activity Track System	PTA not received as of 6/6/07			May be covered by Justice/INS-013, CLAIMS 3/4 (67 FR 64132)

Appendix H
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, 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

Meghan Sanborn, 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
Director, USCIS
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Chief Information Officer
Deputy Chief Information Officer
Chief Privacy Officer
Chief Information Security Officer
Information Systems Security Manager, USCIS
DHS Audit Liaison
USCIS 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.