

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improvements Needed in Security
Management of the United States
Citizenship and Immigration Services'
CLAIMS 3 Mainframe Financial
Application



Office of Information Technology

OIG-05-28

July 2005

Office of Inspector General

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



**Homeland
Security**

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 by the OIG as part of its DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses access controls in place over DHS' financial systems. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express my 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
Acting Inspector General

Table of Contents

Executive Summary	1
Background.....	3
Results of Audit	5
CLAIMS 3 Mainframe Security Responsibilities.....	5
Security Monitoring of CLAIMS 3 Mainframe Application.....	6
Inappropriate CLAIMS 3 Mainframe Remote Access	8
Weaknesses In CLAIMS 3 Mainframe Password Administration	9
Lack of Preventive Maintenance and System Upgrades	11

Appendices

Appendix A: Purpose, Scope, and Methodology	13
Appendix B: Management’s Response.....	14
Appendix C: Major Contributors To This Report.....	19
Appendix D: Report Distribution.....	20

Table of Contents

Abbreviations

CIO	Chief Information Officer
CLAIMS 3	Computer Linked Application Information Management System 3
DHS	Department of Homeland Security
DOJ	Department of Justice
EMerge2	Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency
FY	Fiscal Year
ICE	Immigration and Customs Enforcement
INS	Immigration and Naturalization Service
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
MD	Management Directive
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
USCIS	United States Citizenship and Immigration Services

Executive Summary

The United States Citizenship and Immigration Services (USCIS) bureau processes all applications and petitions for visas and for various immigrant benefits (e.g. change of status, employment authorization, extension of stay, etc). USCIS utilizes the Computer Linked Application Information Management System 3 (CLAIMS 3) mainframe to track pending customs and immigrations applications. This system also serves as the central repository for entering data into the USCIS' CLAIMS 3 Local Area Network (LAN). A strong set of logical and physical access controls over the CLAIMS 3 mainframe is necessary to prevent the risk of unauthorized system access that could result in potential disclosure of or malicious acts to this sensitive information. Our review focused on the access controls that USCIS has implemented to protect the CLAIMS 3 mainframe information.

We evaluated whether there is adequate management in place over the security of USCIS' CLAIMS 3 mainframe application. We performed our work at locations in Washington, DC; Rockville, Maryland; and at the Department of Justice's (DOJ) Data Center in Dallas, Texas. See Appendix A for a discussion of our purpose, scope, and methodology.

Access controls in place over the CLAIMS 3 mainframe are not sufficient to prevent unauthorized access to or loss of the system's immigration and customs information. Our review disclosed that:

- USCIS does not have a security administrator in place to manage the day-to-day access levels and system parameters for this application,
- USCIS personnel do not review and monitor user access levels to ensure that only authorized individuals have access to this financial system,
- Passwords are not administered in accordance with DHS Security policy,

OIG

*Department of Homeland Security
Office of Inspector General*

- An individual employed at the data center where this mainframe resides can remotely access the CLAIMS 3 mainframe application from his home personal computer, and
- Preventive maintenance and system upgrades are no longer being performed on this application.

We are recommending that the USCIS Chief Information Officer (CIO):

- Designate a USCIS CLAIMS 3 security administrator,
- Develop and implement a set of policies and procedures for a coordinated effort of administering and managing the CLAIMS 3 mainframe security process between USCIS and ICE,
- Establish procedures for a USCIS security administrator to review and monitor access controls security reports on a daily basis,
- Establish procedures for a USCIS security administrator to re-certify user access privileges to the CLAIMS 3 mainframe at least on an annual basis,
- Enforce DHS' remote access policy requiring that DHS systems be accessed only through DHS approved hardware and software,
- Strengthen the CLAIMS 3 mainframe password configurations in accordance with DHS' Security Handbook¹, and
- Re-establish preventive maintenance and system upgrades for the CLAIMS 3 mainframe.

¹ *IT Security Program Handbook* (Management Directive 4300A) version 2, dated December 2003

Background

CLAIMS 3 is a financial application that supports processing of USCIS applications and petitions for various immigrant benefits (e.g. change of status, employment authorization, extension of stay, etc). This mainframe application was developed to meet the information needs of personnel at legacy DOJ's Immigration and Naturalization Service (INS) headquarters, service processing centers, and district offices. At the service processing centers the CLAIMS 3 LAN, located in Rockville, Maryland, has replaced much of this routine processing. The CLAIMS 3 mainframe application also serves as the repository for all data processed in the CLAIMS 3 LAN system through daily batch runs. The USCIS mainframe is housed in DOJ's Dallas Data Center while the application services are provided by DOJ at the Rockville Data Center. DHS' Immigration and Customs Enforcement (ICE) is responsible for maintaining the systems access controls software and establishing user access privileges.

The CLAIMS 3 mainframe application has two primary objectives:

- To serve effectively the operational and management needs of USCIS personnel accepting and adjudicating applications and petitions for benefits in district offices, service processing centers and headquarters offices, and
- To provide the capability to extract data on immigration and customs benefits and to produce aggregate statistical reports.

CLAIMS 3 has two primary components: (1) online data entry, query, and adjudication system and (2) a system of batch runs that extract and report data and provide interfaces with other systems. Data for the CLAIMS 3 system is entered at the service processing centers.

A strong set of access controls over the CLAIMS 3 mainframe application is important to ensure that individuals outside of USCIS do not gain unauthorized access to this system's sensitive immigration and customs

OIG

*Department of Homeland Security
Office of Inspector General*

information. OMB Circular A-130² requires government agencies to provide adequate security that is “commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.” In addition, agencies should also “assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.”

A strong set of access controls over the CLAIMS 3 application is also important as DHS moves towards the consolidation and merger of its financial systems. DHS’ Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency (eMerge2) project will bring together the Department’s legacy financial systems from 22 agencies. A prerequisite to any merger of systems is to ensure that existing weaknesses in a system are not transferred over to the new system environment.

Finally, DHS’ FY 2004 financial statement audit³ disclosed over 35 access control related issues from the review of financial systems at major DHS components. Some of these issues were in existence before the establishment of DHS and were transferred to DHS from legacy agencies like DOJ. These issues along with the other information technology issues noted in the audit report contributed to the independent auditor’s declaration of a material weakness for DHS’ IT environment.

² Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources Appendix III, Security of Federal Automated Information Resources.

³ Independent Auditors’ Report on DHS’ FY 2004 Financial Statements, Office of Audits, Office of Inspector General, Department of Homeland Security, OIG-05-05, December 2004.

Results of Audit

CLAIMS 3 Mainframe Security Responsibilities

USCIS does not control or manage security over its CLAIMS 3 mainframe application. Although the USCIS CIO relies on ICE security administrators to monitor and administer the day-to-day security responsibilities of the CLAIMS 3 mainframe, this office does not have access to security reports and user access lists to ensure that CLAIMS 3 mainframe security is being properly administered. When the CLAIMS 3 mainframe application, containing immigration and customs information, was transferred from DOJ to DHS' USCIS bureau in March 2003, responsibility for monitoring and reviewing security for this system remained with DHS' ICE bureau. As a result, USCIS, the owners of the CLAIMS 3 mainframe application, must rely on ICE to monitor system security issues and user access permissions on its behalf. Further, DHS' IT Security Handbook⁴ requires system owners to re-certify user access on an annual basis but this process cannot occur if the system owners and users do not have access to the tools necessary to perform the monitoring. This approach to managing security of the CLAIMS 3 mainframe leaves the control environment surrounding sensitive immigration and customs information in the hands of non-system users who do not have a need to know or need to access this information.

Recommendation:

We recommend that the USCIS CIO:

1. Designate a USCIS CLAIMS 3 security administrator.

USCIS CIO Comments and OIG Analysis

The USCIS CIO agreed with our recommendation and stated that her office is currently in the process of implementing revised procedures and controls, defining and re-defining the responsibilities of the CLAIMS 3 security

⁴ *IT Security Program Handbook* (MD 4300A), Attachment J, Section 3.0, version 2, dated December 2003.

administrator, and conducting the formal appointment process for this position. We accept USCIS' response and consider this recommendation resolved.

Security Monitoring of CLAIMS 3 Mainframe Application

USCIS security administrators do not review and monitor CLAIMS 3 mainframe security reports. This situation is occurring, in part, because responsibility for security remained with ICE security administrators following the creation of DHS. As a result, USCIS does not have the ability to generate access controls security reports for its CLAIMS 3 mainframe application because only ICE personnel have security administrator privileges to this system. Further, ICE security administrators do not provide copies of these CLAIMS 3 Mainframe security reports to USCIS security administrators.

USCIS cannot be assured that only authorized users have access to its system and that access privileges are proper because ICE does not provide security reports or any other form of confirmation to USCIS to ensure that CLAIMS 3 mainframe security is being reviewed on a daily basis. User access privileges should be monitored on a daily basis by system administrators to ensure that user access levels are current and are necessary for users to perform their current job responsibilities. When user access levels are not monitored on a regular basis the potential exists that inactive accounts may remain on the system over time increasing the possibility that unauthorized users may access these accounts and potentially modify sensitive information. A review of access control security reports helps to ensure that inactive accounts are removed in a timely manner and that only authorized USCIS users have access to CLAIMS 3 information.

DHS' IT Security Handbook⁵ requires system owners to re-certify user access privileges on an annual basis. Because users need to access information changes over time, supervisors need to review access lists to ensure that they

⁵ *IT Security Program Handbook* (MD 4300), Attachment J, Section 3.0, version 2, dated December 2003.

are current and up-to-date. If user accounts are not re-validated on a regular basis there is the potential that users may be granted access beyond their current needs, thus elevating the risk that system data could be compromised, and inappropriate actions (e.g., unauthorized access to funds control, processing payments, inventory management) could be made.

As a part of our review to ensure that adequate access security controls are in place over the CLAIMS 3 mainframe we requested copies of CLAIMS 3 mainframe security reports so that we could validate user access privileges and access controls software parameters. However, ICE security personnel were unable to provide them to us. In addition, through the interview process with both USCIS and ICE security personnel we also confirmed that there is no process in place to ensure that accounts are disabled when users have three unsuccessful logon. When user accounts are not locked out of the system after several unsuccessful password attempts, the system becomes more susceptible to successful hacking attempts. Guidance from the National Institute of Standards and Technology (NIST) indicates that organizations should limit the number of logon attempts to ensure that user passwords are changed frequently.

Recommendations:

We recommend that the USCIS CIO:

2. Develop and implement a set of policies and procedures for a coordinated effort of administering and managing the CLAIMS 3 mainframe security process between USCIS and ICE.
3. Establish procedures for a USCIS security administrator to review and monitor access controls security reports on a daily basis.
4. Establish procedures for a USCIS security administrator to re-certify user access privileges to the CLAIMS 3 mainframe at least on an annual basis.

USCIS CIO Comments and OIG Analysis

The USCIS CIO agreed with our recommendations. According to the CIO, policies and procedures for administering and managing the CLAIMS 3 mainframe security process including procedures for the review and monitoring of access controls security reports will be in place by April 30, 2006. Procedures for a USCIS security administrator to re-certify user access privileges for the CLAIMS 3 mainframe will be in place by October 31, 2005. We accept USCIS' response and consider these recommendations resolved.

Inappropriate CLAIMS 3 Mainframe Remote Access

DOJ personnel at the Dallas data center have inappropriate remote access privileges to the CLAIMS 3 mainframe. The CLAIMS 3 mainframe system resides in DOJ's Dallas data center. During our visit to Dallas we were informed that a DOJ employee has the ability to access the CLAIMS 3 mainframe from his home personal computer. According to DHS' IT Security Handbook⁶ no dial-in access will be used to access DHS applications or general support systems, unless authorized in writing by the employee's Information Systems Security Officer (ISSO). In addition, DHS' IT Security Handbook⁷ requires that a work from home agreement should be in place that identifies what government equipment and supplies will be needed by the employee at home, and how the equipment and supplies will be transferred and accounted for. Neither ICE nor USCIS provided us with any agreements authorizing this employee to remotely access the CLAIMS 3 mainframe. These types of access privileges increase the risk of unauthorized access to USCIS' CLAIMS 3 mainframe system and could lead to unauthorized modifications to the system.

Recommendation:

We recommend that the USCIS CIO:

⁶ *IT Security Program Handbook* (MD 4300), Attachment D, Section 4.2, version 2, dated December 2003.

⁷ *IT Security Program Handbook* (MD 4300), Attachment D, Section 4.1, version 2, dated December 2003.

5. Enforce DHS' remote access policy requiring that DHS systems be accessed only through DHS approved hardware and software.

USCIS CIO Comments and OIG Analysis

The USCIS CIO agrees with this recommendation. USCIS recognizes that the laptops used by DOJ personnel for remote access are inconsistent with DHS remote access requirements. When DHS renews the Memorandum of Understanding with DOJ, DHS security requirements will be incorporated into the documentation. USCIS anticipates that these negotiations will be complete by April 26, 2006. We accept USCIS' response and consider this recommendation resolved.

Weaknesses in CLAIMS 3 Mainframe Application Password Administration

USCIS' CLAIMS 3 mainframe continues to have weaknesses in its password configurations. Our follow up of prior year issues relating to password configuration and administration for the CLAIMS 3 mainframe indicated that weaknesses in passwords that were identified during the FY 2003 financial statement audit continue to exist. Specifically:

- Users are not required to select a new password upon initial access to the system.
- Configuration of user passwords is not in agreement with DHS security policy. (Passwords are not required to be alpha numeric, at least 8 characters in length, contain no dictionary words, be encrypted, and not be reusable in fewer than six iterations)
- Privileged account passwords are not limited to a maximum lifetime of 30 days

- Upon the expiration of user ids, the system does not inform users of the password formatting requirements for the creation or changing of a password.
- Users are not notified in advance before their passwords expire.

The continued use of these weak password configurations does not comply with DHS' IT Security Handbook⁸ which requires components to enforce strong passwords for authentication to DHS IT Systems.

Recommendation:

We recommend that the USCIS CIO:

6. Strengthen the CLAIMS 3 mainframe password configurations in accordance with DHS' IT Security Handbook.

USCIS CIO Comments and OIG Analysis

The USCIS CIO concurs in part with this recommendation. Although USCIS agrees that password configurations need to be upgraded, they do not agree that a substantial investment should be made in the CLAIMS 3 mainframe application since this system will be replaced during a multi-year IT Transformation Program. With this IT Transformation Program, the CLAIMS 3 mainframe would be retired and replaced with new technology.

We recognize that USCIS plans to retire the CLAIMS 3 mainframe application during the IT Transformation Program; however, no date has been set for this retirement. Until a date for the CLAIMS 3 mainframe retirement has been determined, USCIS needs to implement a strong password configuration for the CLAIMS 3 mainframe to ensure that adequate controls are in place to prevent unauthorized access to sensitive immigration information.

⁸ *IT Security Program Handbook* (MD 4300), Attachment J, Sections 2.0 and 3.0, version 2, dated December 2003.

Lack of Preventive Maintenance and System Upgrades

Computer software systems require constant maintenance and upgrades to stay current with changing technologies. Maintenance on computer systems should be performed on a regular/scheduled basis to: update system license information, maintain consistency across various systems, ensure that systems are compatible and work is not being duplicated, monitor available system resources, and to identify and repair ‘bugs’ or faults in software. According to personnel at the data center where this mainframe resides, funding for the preventive maintenance and system upgrades was discontinued because of the pending DHS data center consolidation. This consolidation will bring together DHS’ data center computer hardware and software. Although several sites have been considered for this consolidation, there is no set timeframe for when the actual consolidation of equipment and resources will occur. Guidance on Financial Management Systems requires that all documentation associated with systems and software be continually updated to provide sufficient detail to obtain a comprehensive knowledge and understanding of an agency’s operation.

Recommendation:

We recommend that the USCIS CIO:

7. Re-establish preventive maintenance and system upgrades for the CLAIMS 3 mainframe.

USCIS CIO Comments and OIG Analysis

The USCIS CIO concurs in part with this recommendation. The CIO agrees that maintenance and system upgrades are sound strategies; however, this official does not believe there is a business case to continue additional maintenance and system upgrades on a system that will be retired during the multi-year USCIS IT Transformation Program.

We recognize that USCIS plans to retire and replace the CLAIMS 3 mainframe application during the IT Transformation Program; however, no

OIG

*Department of Homeland Security
Office of Inspector General*

date has been set for this retirement. Until a date for the CLAIMS 3 mainframe retirement has been determined, USCIS needs to continue maintenance and system upgrades for this system in order to ensure that immigration information is accurately processed.

Purpose, Scope, and Methodology

The overall objective of our audit was to determine whether there is adequate management in place over the security of USCIS' CLAIMS 3 mainframe application. The scope of our testing included the following:

- Perform a physical security analysis of sites associated with the CLAIMS 3 Mainframe application.
- Provide update on security concerns identified during prior access controls audits at USCIS.
- Review OS/390 mainframe operating system and subsystems used for the CLAIMS 3 application.
- Review the parameters utilized by the access control software program, including user profiles and access privileges.

We conducted our audit between July 2004 and December 2004 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards. The fieldwork for our audit was conducted at the following DHS locations:

- Bureau of Citizenship and Immigration Services (CIS)
 - Headquarters location
- Department of Justice (DOJ)
 - Dallas Data Center
 - Rockville Data Center

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, (202) 254-4041; and Roger Dressler, Director, Information Systems and Architecture, (202) 254-5441. Major OIG contributors to the audit are identified in Appendix C.

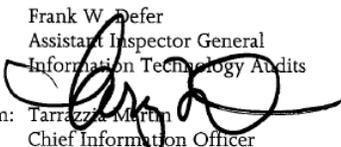
Appendix B
Management's Response

U.S. Department of Homeland Security
111 Massachusetts Avenue, NW
Washington, DC 20001-1461



U.S. Citizenship
and Immigration
Services

To: Frank W. Defer
Assistant Inspector General
Information Technology Audits

From: 
Tarranza Martin
Chief Information Officer
U.S. Citizenship & Immigration Services (USCIS)
Department of Homeland Security

HQ CIO 40/2

Date: July 15, 2005

Subject: Draft Audit Report: Improvements Needed in Security Management of the United States Citizenship and Immigrations Services (USCIS) CLAIMS 3 Mainframe Financial Application (IT-A-04-010)

USCIS appreciates the opportunity to comment on the subject report. USCIS is committed to protecting the integrity, availability, and confidentiality of the CLAIMS 3 mainframe application and its data.

We would like to inform you that USCIS plans to retire the CLAIMS 3 Mainframe at the earliest opportunity as part of the USCIS IT Transformation Program. To this end, USCIS plans are to minimize CLAIMS 3 Mainframe upgrade investments and focus our resources to USCIS' IT Transformation Program. We have taken these plans into consideration when determining how best to respond to the matters raised by your report.

USCIS has embarked on a multi-year holistic IT Transformation Program envisioned to transition USCIS into a person-centric digital-based organization. Adding additional security, privacy, and information sharing governance and oversight through the OCIO; stabilizing and upgrading the IT Infrastructure; implementing an enterprise application integration foundation; and developing enhanced and new business capabilities such as digitization, case management, and biometrics, are part of this long term program.

An integrated, enterprise-wide Case Management application is central to our transformation efforts. The OCIO has chosen Siebel eBusiness applications as the foundation software product with which we will base our new e-Adjudication Case Management application. All eAdjudication or case management development work (with

Improvements Needed in Security Management of the United States Citizenship and Immigration Services' CLAIMS 3 Mainframe Financial Application

Appendix B
Management's Response

the exception of O&M on the legacy Case Management systems) should be consistent with and supportive of our Siebel-based strategy. Any proposed exceptions to this strategy must be reviewed and validated by my office. By standardizing on a COTS set of tools, we reduce risks, better ensure consistency across the enterprise, and allow for better review and enforcement of controls associated with security and privacy requirements.

Should you have any questions regarding the corrective actions to the report recommendations, please contact Tarrazzia Martin, Chief Information Officer, USCIS, at 202-272-1700.

Attachment

Appendix B
Management's Response

The following list contains USCIS' responses to the Department of Homeland Security (DHS) Office of the Inspector General's Draft Audit report recommendations, as well as USCIS status and response.

Recommendation 1: The USCIS CIO should designate a USCIS CLAIMS 3 security administrator.

USCIS Status: Concur. We are currently in the process of implementing revised procedures and controls, defining and refining responsibilities for the CLAIMS 3 Security Administrator, and conducting the formal appointment process for this position. USCIS designated a USCIS CLAIMS 3 security administrator in writing. Ray Hawkins has been appointed as the Information Systems Security Officer (ISSO) for CLAIMS 3. He has been instructed on his role as ISSO and will attend formal ISSO training on September 30, 2005.

Recommendation 2: The USCIS CIO should develop and implement a set of policies and procedures for a coordinated effort of administering and managing the CLAIMS 3 mainframe security process between USCIS and ICE.

USCIS Status: Concur. USCIS is developing policies and procedures for the coordinated effort of administering and managing the CLAIMS 3 Mainframe security process that will be in place by April 30, 2006. Since the OIG review began, USCIS has established a team located in Burlington, Vermont, to manage USCIS Password Issuance Control System (PICS) accounts. This has enabled USCIS to establish control over USCIS applications including CLAIMS 3 and to produce reports on which users have application access.

USCIS has assumed responsibility for the administration of USCIS personnel user accounts including monitoring of security reports as noted above. CLAIMS 3 Security Administration responsibilities for USCIS users are accomplished through PICS. Security responsibilities for CLAIMS 3 Mainframe have been reassigned from ICE personnel to USCIS staff.

Recommendation 3: The USCIS CIO should establish procedures for a USCIS security administrator to review and monitor access controls security reports on a daily basis.

USCIS Status: Concur. USCIS is currently establishing procedures for the USCIS CLAIMS 3 security administrator to review and monitor access control exception reports and other security reports to capture errors and any other aberrant behavior on a daily basis. These procedures will be in place by April 30, 2006.

Recommendation 4: The USCIS CIO should establish procedures for a USCIS security administrator to re-certify user access privileges to the CLAIMS 3 Mainframe at least on an annual basis.

USCIS Status: Concur. USCIS is currently establishing procedures for the USCIS security administrator to annually re-certify CLAIMS 3 Mainframe user access privileges. USCIS has received a report of all CLAIMS 3 user accounts and is developing a process for user account validation. Once this process is in place, USCIS will use it to validate CLAIMS 3

Appendix B
Management's Response

user accounts as well as user accounts for other applications. WE anticipate this process will be in place by October 31, 2005.

USCIS will require that hard copies of all signed user access request forms be sent to the CLAIMS 3 Security Administrator where they will be maintained. This requirement will apply to initial requests and subsequent modification requests. We will implement a re-certification process for those individuals whose hard copy computer security statements cannot be located. This initiative will be completed by December 31, 2005.

USCIS is establishing formal procedures to ensure that (1) the requestor's name will be validated against a list of persons authorized to request CLAIMS 3 Mainframe access, and (2) that both the employee and the requestor have signed the access request forms. Planned completion date is April 30, 2006.

Additionally, USCIS will negotiate with U.S. Immigration and Customs Enforcement (ICE) to revise the PICS access request form to include the signature of the person granting access and the date access was granted. Planned completion date is April 30, 2006.

Recommendation 5: The USCIS CIO should enforce DHS' remote access policy requiring that DHS systems be accessed only through DHS approved hardware and software.

USCIS Status: Concur. Department of Justice (DOJ) staff has remote access privileges via DOJ provided laptops to the CLAIMS 3 Mainframe. This access is consistent with USCIS' Memorandum of Understanding (MOU) through ICE for mainframe support for USCIS applications.

USCIS recognizes the laptops used by DOJ are inconsistent with DHS remote access requirements. When we renew the data center services MOU between DHS and DOJ, we intend to incorporate DHS security requirements to the maximum extent possible. Since USCIS is not the only DHS component using the DOJ data centers, negotiating this change will require coordination among multiple DHS components. We anticipate these negotiations can be completed by April 2006.

Recommendation 6. The USCIS CIO should strengthen the CLAIMS 3 mainframe password configuration in accordance with DHS' IT Security Handbook.

USCIS Status: Concur in part. While USCIS concurs with this recommendation, we are concerned about the age and architecture of the CLAIMS 3 application. Abating the security vulnerabilities of the CLAIMS 3 Mainframe application would require a substantial investment to implement new capabilities that can address these findings. Rather than dedicate our funds in that manner, USCIS has embarked on a multi-year IT Transformation Program and plans to retire the CLAIMS 3 Mainframe application during the IT Transformation. USCIS has accepted the risk in the context of other priorities; however, USCIS will continue to look for low cost techniques that can mitigate identified risks and whose cost can be justified for system's remaining life.

Additionally, USCIS believes the corrective actions USCIS proposed to other recommendations in this report will assist to abate these findings.

Recommendation 7: The USCIS CIO should re-establish preventive maintenance and system upgrades for the CLAIMS 3 Mainframe.

USCIS Status: *Concur in part.* While we concur that the maintenance practices identified by the finding generally represent sound strategies, when a system has exceeded its useful life it erodes the business case for continued maintenance investment. Such is the case for the CLAIMS 3 Mainframe application. We will continue to evaluate the justification for continued investment in CLAIMS 3 Mainframe but our plan is to minimize investments in favor of the new case management system being developed as part of the IT Transformation program. We will continue to monitor the IT Transformation Program to verify that plans are implemented to retire the CLAIMS 3 Mainframe application.

Office of Information Technology
Information Systems and Architecture Division

Frank Deffer, AIG
Roger Dressler, Director
Sharon Huiswoud, IT Audit Manager
Anthony Nicholson, IT Auditor
Sharell Matthews, Referencer

Information Systems and Architecture Division

Jim Lantzy, Director
Lane Melton, Senior Security Engineer
Karyn Higa, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Acting Director, USCIS
Chief of Staff
General Counsel
Executive Secretariat
DHS Chief Information Officer
DHS Audit Liaison
DHS Public Affairs
Chief Information Officer Audit Liaison
USCIS Chief Information Officer
USCIS 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) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov.

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 the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.