DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Security Weaknesses Increase Risks to Critical United States Citizenship and Immigration Services Database (Redacted)

Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552(b)(2). A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-05-42 September 2005

Office of Inspector General

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

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 DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses the strengths and weaknesses of database security controls over United States Citizenship and Immigration Services (USCIS) database resources. It is based on interviews with USCIS officials, direct observations, technical tests, 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 our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ATL	Advanced Technology Laboratory
ATO	Authority to Operate
C&A	Certification and Accreditation
CIO	Chief Information Officer
DBMS	Database Management System
DHS	Department of Homeland Security
DHS Handbook	DHS Sensitive Systems Handbook
DHS Policy	DHS Sensitive Systems Policy Publication 4300A
DOJ	Department of Justice
FISMA	Federal Information Security Management Act of 2002
ICE	United States Immigration and Customs Enforcement
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones

Table of Contents/Abbreviations

USCIS	United States Citizenship and Immigration Services
SP	Special Publication

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We audited the Department of Homeland Security (DHS) and its organizational components' security program to evaluate the security and integrity of select sensitive but unclassified mission critical databases.[1] This audit included reviews of access controls, change management, and continuity of operations policies and procedures. This report assesses the strengths and weaknesses of security controls over United States Citizenship and Immigration Services (USCIS) database resources.

Our objective was to determine whether USCIS had implemented adequate and effective controls over sensitive data contained in its Central Index System. Information contained in the Central Index System is used to assist in the enforcement of United States immigration laws. We interviewed USCIS officials, reviewed database security documents, and performed technical tests of the Central Index System mainframe computer.

Although USCIS has not established adequate or effective database security controls for the Central Index System, it has implemented many essential security controls such as procedures for controlling temporary or emergency system access, a configuration management plan, and procedures for implementing routine and emergency changes. Further, we did not identify any significant configuration weaknesses during our technical tests of the Central Index System. However, additional work remains to implement the access controls, configuration management procedures, and continuity of operations safeguards necessary to protect sensitive Central Index System data effectively. Specifically, USCIS has not: 1) implemented effective user administration

[1] DHS "organizational components" are defined as directorates, including organizational elements and bureaus, and critical agencies.

procedures; 2) reviewed and retained [redacted] effectively;[2] 3) ensured that system changes are properly controlled; 4) developed and tested an adequate Information Technology (IT) contingency plan; 5) implemented [redacted]; or, 6) monitored system security functions sufficiently. These database security exposures increase the risk that unauthorized individuals could gain access to critical USCIS database resources and compromise the confidentiality, integrity, and availability of sensitive Central Index System data. [redacted]

Following the completion of our review, USCIS officials stated that they have already taken or plan to take corrective action to address some of the weaknesses we identified. As our fieldwork was complete, we did not verify that the weaknesses had been remedied.

We recommend that USCIS Director instruct the Chief Information Officer (CIO) to:

- Ensure that adequate controls for granting, monitoring, and removing user access to the Central Index System are implemented.
- Review and retain [redacted] on the Central Index System.
- Ensure that system changes to the Central Index System are adequately controlled.
- Develop and test a Central Index System IT contingency plan.
- Examine methods to implement [redacted].
- Monitor system security functions for the Central Index System.

In addition, to comply with the Office of Management and Budget's (OMB) *Federal Information Security Management Act of 2002* (FISMA) reporting requirements, we evaluated the effectiveness of the USCIS' information security program and practices as implemented for the Central Index System.[3] USCIS has not aligned fully its security program with DHS' overall policies, procedures, or practices. For example, security controls are not routinely tested and evaluated; a contingency plan has not been established and tested; and,

[2] Audit trails maintain a record of system activity both by system and application processes and by users of the systems and applications. The audit trail is the evidence that demonstrates how a specific transaction was initiated, processed, and summarized. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

[3] FISMA is included under Title III of the E-Government Act of 2002 (Public Law 107-347).

system and database administrators have not obtained specialized security training. Appendix C summarizes the results of our FISMA evaluation.

Fieldwork was conducted from January to May 2005 at USCIS and United States Immigration and Customs Enforcement (ICE) facilities in Washington, DC; the Department of Justice (DOJ) *Justice Data Centers* in ------------------ and -------------; and, the Office of Inspector General's (OIG) Advanced Technology Laboratory (ATL).[4] See Appendix A for our purpose, scope, and methodology.

In response to our draft report, the USCIS Acting Deputy Director concurred with our recommendations and is in the process of implementing corrective measures. In addition, USCIS is in the process of building an IT Security Office and implementing security, privacy, systems development, and continuity of operations best practices. USCIS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

A database is one or more large structured sets of data (fields, records, and files) organized so that the data can be easily accessed, managed, and updated. Most often, databases are associated with software used to update and query the data, called a database management system (DBMS). The DBMS can be an extremely complex set of software programs that controls the organization, storage, and retrieval of data in a database. In addition, the DBMS, in conjunction with its host operating system, controls access to the data and ensures the security and integrity of the database. DBMS' can be classified according to their architectural model (e.g., relational, hierarchical, or network), and can be centralized on one platform or distributed across multiple servers.

Databases and DBMS' have become a more frequent target of attack for malicious users. Such an attack can result in financial loss, loss of privacy, or a breach of national security as well as the many other varieties of corruption that result from unauthorized access to sensitive data. To counter this threat, a number of security options are available to protect the data housed in databases. For these measures to be effective, however, DBMS security controls must be properly configured and maintained. In addition, as database products have become more complex and the attacks against them have increased, a number of

[4] The ATL supports our capability to perform effective and efficient technical assessments of DHS information systems and diverse operating environments. The ATL is a collection of hardware and software that allows the simulation, testing, and evaluation of the computing environments that are most commonly used within DHS.

vulnerabilities have been identified that could be exploited by attackers. DBMS vendors have responded by issuing patches or fixes for discovered vulnerabilities. These patches must be applied—quickly and appropriately—to ensure that critical data is protected adequately.

The Central Index System was established in 1985 to assist in the enforcement of the immigration laws of the United States. The system contains information on the status of approximately 55 million individuals, including permanent residents, naturalized citizens, border crossers, apprehended aliens, aliens issued employment authorization, and others of interest to the federal government. This system helps ensure proper entry decisions by providing DHS field offices, ports of entry, and examination and inspection sites prompt access to biographical and status information on those seeking legal entry to or residence in the United States. Also, the Central Index System assists the department in the identification of individuals who violate the terms of their stay, who enter the United States illegally, or who are otherwise not entitled to entry or benefits.

The Central Index System resides on a mainframe computer at the DOJ *Justice Data Center* in [redacted]. The system employs a [redacted] using [redacted] DBMS, [redacted] operating system, and [redacted] security software. Currently, there are over 33,000 Central Index System users, including officials from DHS, the Central Intelligence Agency, Drug Enforcement Administration, Federal Bureau of Investigation, Department of State, and congressional committees. Central Index System users access the system through a wide area network connection from locations throughout the country as well as some overseas sites.

DHS Sensitive Systems Policy Publication 4300A (DHS Policy) provides direction to DHS components regarding the management and protection of sensitive systems. Also, this policy outlines the management, operational, and technical controls necessary to ensure confidentiality, integrity, availability, and authenticity within the DHS IT infrastructure and operations. DHS Policy requires that its components ensure that strong access controls, IT contingency planning safeguards, and change and configuration management procedures are implemented for all systems processing sensitive but unclassified information. The department developed the DHS Sensitive Systems Handbook (DHS Handbook) to provide components with specific techniques and procedures for implementing the requirements of this policy.

The National Institute of Standards and Technology (NIST) has issued several publications related to database system access controls, change and configuration management, and IT contingency planning. Specifically, NIST

Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance for establishing adequate access controls for sensitive government systems, including the use of strong passwords, encryption, and user administration practices. Also, NIST SP 800-12 provides guidance on effectively controlling changes to sensitive information systems. Further, NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, provides instructions, recommendations, and considerations for government IT contingency planning.

Results of Audit

Strengthening of Database Security Procedures Is Needed

USCIS has not developed or implemented the security controls necessary to protect the Central Index System and its data. In assessing the procedures governing the security of sensitive data contained in the Central Index System, we identified user administration, auditing, change management, IT contingency planning, [redacted] system security monitoring weaknesses. Therefore, there is significant risk that the security procedures protecting the Central Index System may not prevent unauthorized access to its systems and data. In addition, USCIS may not be able to recover Central Index System operations following a disaster or disruption.

User Administration Procedures Are Incomplete

USCIS has implemented a process to grant, monitor, and remove Central Index System user access, which includes controls to protect access to the system and its data. For example, USCIS has established a process to control emergency and temporary user access, as well as a process to disable accounts after [redacted] days of inactivity. However, additional procedures must be implemented to ensure that access to the Central Index System is restricted appropriately. From a random sample of 20 active Central Index System user accounts, we identified three users who had access rights that had not been authorized, including one user with administrator rights to the system. Central Index System officials stated that the access permissions for two of the accounts were not updated because of a system administrator error. In addition, the supervisor for the user with privileged access stated that she had verbally requested that this access be revoked. However, since a formal access change form had not been submitted, the user's administrator rights were not rescinded.

DHS Policy requires that access is controlled and limited based on positive user identification and authentication mechanisms, which support the minimum requirements of access control, least privilege, and system integrity.[5] Since Central Index System user administration procedures have not been fully implemented, there is increased risk that inappropriate individuals may access sensitive Central Index System data. As a result, sensitive system information may not be protected adequately.

Central Index System Auditing Is Inadequate

USCIS does not have procedures to periodically review [redacted] for the Central Index System. USCIS records pertinent information related to certain [redacted]. While [redacted], [redacted]. In addition, although [redacted] are retained, [redacted] are kept for only two years because the Central Index System mainframe administrators were not aware of DHS audit trail retention requirements.

Audit trails help ensure individual accountability by tracking a user's activities while accessing an automated system. However, to be effective, significant security events must be recorded and the audit trails must be reviewed and retained. According to the DHS Handbook, the review of audit trail information is essential because unauthorized access, modification, or destruction of data may be discovered only through the review process. Also, the DHS Handbook requires that Information Systems Security Officers (ISSO) review audit trail information weekly or in accordance with the system security plan, and that audit trail information be retained for seven years. Due to the lack of adequate audit review and retention procedures, inappropriate access to sensitive data or malicious changes to the Central Index System may not be detected or investigated.

A Central Index System Upgrade Was Not Adequately Controlled

USCIS has established a configuration management plan and change management procedures for controlling routine and emergency changes to the

[5] The principle of least privilege requires that users be given the most restrictive set of privileges needed to perform authorized tasks.

Central Index System. Further, USCIS has implemented a process to conduct annual reviews of a sample of changes to Central Index System applications. However, USCIS has not ensured that all changes to the Central Index System go through the established change management process. Specifically, we identified an upgrade to the Central Index System DBMS, conducted in April 2005, which, due to an administrative error, did not go through the established review and approval process for system changes. USCIS officials stated that they are working to ensure that similar omissions do not occur in the future.

DHS Policy requires that organizational components establish, implement, and enforce change management and configuration management controls on all IT systems and networks. Further, the DHS Handbook requires that the initial configuration of a system be documented in detail, and that all subsequent changes to any components of the system be controlled through a complete and robust change management process. Because the Central Index System upgrade did not go through the established change management process, there was greater risk that the confidentiality, availability, or integrity of the system and its data would be compromised.

An IT Contingency Plan Has Not Been Developed and Tested

Although USCIS has developed and tested an IT contingency plan for the Central Index System mainframe operating system and general support systems, the IT contingency plan for the system's applications does not contain all of the information necessary to ensure that the system can be recovered. For example, the plan does not include [redacted] Further, the IT contingency plan for the system's applications has not been tested. USCIS officials stated that they are not aware of any plans to update the IT contingency plan for Central Index System applications.

In addition, we identified the following issues related to Central Index System data backup and restoration procedures:

- The backup tapes used for offsite storage of sensitive Central Index System data [redacted] Although adequate physical security measures are maintained at the contracted offsite storage facility, [redacted]

- Although the restoration of operating system files is periodically tested, USCIS has not conducted a formal test of backup and restoration procedures for Central Index System applications and data.

DHS Policy requires that comprehensive IT contingency plans be developed, tested, exercised, and maintained for critical major applications and general support systems. Also, DHS requires that quarterly tests of data backup and restoration procedures be performed.

The non-availability of sensitive information processed and stored by the Central Index System could significantly impact USCIS and DHS missions. Contingency planning is essential because it establishes the plans, procedures, and technical measures necessary to recover a system quickly and effectively following a service outage or disaster. IT contingency plan testing enables deficiencies to be identified and addressed, and helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Formal tests of established data restoration procedures are an integral part of testing the overall contingency plan, and help ensure that all necessary data can be recovered in the event of a disaster. As a result of the lack of adequate contingency planning and testing for the system, including tests of the Central Index System data restoration process, USCIS lacks assurance that it will be able to resume operations following a disaster.

[redacted] Has Not Been Implemented

USCIS has not implemented [redacted] to protect sensitive Central Index System data. Specifically, USCIS is not [redacted]. The component conducted a pilot test of [redacted], but did not purchase the software because of its cost.

According to the DHS Handbook, [redacted] reliable and achievable way to ensure confidentiality for sensitive data. DHS Policy requires that the department's components identify IT systems transmitting sensitive information that may require protection, and develop [redacted] for their sensitive IT systems. In addition, NIST recommends that [redacted] be implemented to protect the integrity and confidentiality of critical data and software programs. As a result of these [redacted], an individual could [redacted].

USCIS Is Not Monitoring System Security Functions Adequately

USCIS is not monitoring sufficiently the security activities performed by ICE and DOJ personnel for the Central Index System.[6] Specifically, USCIS does not have a process to verify that ICE and DOJ information technology staff are performing necessary security or user administration functions for the Central Index System and personnel. For example, USCIS personnel do not [redacted] or perform periodic vulnerability assessments or configuration reviews. Further, USCIS does not ensure that these functions are being performed by ICE and DOJ personnel.

According to officials, USCIS cannot provide security oversight for the Central Index System because of resource constraints; the Central Index System ISSO position is a collateral duty; and, the transition of certain IT functions from ICE to USCIS is still in progress. However, the Information Systems Security Manager stated that USCIS is currently working to address this issue.

FISMA requires that senior agency officials provide security for the information and information systems that support the operations and assets under their control. Without an established process to monitor the quality of user administration and security management functions performed by ICE and DOJ officials, USCIS lacks assurance that sufficient security is provided for the Central Index System and its data.

Recommendations

To protect sensitive Central Index System data, we recommend that the USCIS Director instruct the CIO to:

1. Strengthen procedures to ensure that adequate controls for granting, monitoring, and removing user access to the Central Index System are implemented according to DHS requirements and NIST guidelines.
2. Review and retain [redacted] to facilitate the detection and investigation of inappropriate access or malicious changes to the Central Index System.

[6] USCIS and ICE were part of the former Immigration and Naturalization Service of the DOJ. The Central Index System currently resides on a mainframe computer housed at a DOJ facility. The operating system of the Central Index System mainframe computer is controlled and administered by DOJ personnel. In addition, ICE personnel and contractors provide development and operations support for the Central Index System.

3. Strengthen change management procedures to ensure that routine and emergency modifications to the Central Index System are adequately controlled; and, consider strengthening the annual change management review process.
4. Develop an adequate IT contingency plan for Central Index System applications; and, ensure that annual tests of the plan and quarterly tests of data restoration procedures are conducted.
5. Examine methods to implement [redacted]
6. Monitor Central Index System security functions to ensure that adequate security is provided for the system and its data.

Management Comments and OIG Analysis

USCIS concurs with recommendation 1. USCIS plans to assume control of user administration functions for USCIS' major applications, including the Central Index System, in fiscal year 2006.[7] Once implemented, the new user administration procedures will include the documentation and maintenance of system access authorizations at USCIS, ISSO review of access requests, as well as annual recertification of user access privileges by the ISSO.

We accept USCIS' response to enhance its controls for granting, monitoring, and removing user access to the Central Index System.

USCIS concurs with recommendation 2. USCIS plans to address DHS audit file content, review, and retention requirements at the [redacted] layers. In addition, USCIS plans to establish procedures for the Central Index System ISSO to conduct daily reviews of [redacted] and security reports by April 30, 2006.

We accept USCIS' response to implement DHS audit file content and retention requirements, as well as daily reviews of Central Index System [redacted]. However, USCIS should establish a timeline for the implementation DHS' audit retention requirements.

USCIS concurs with recommendation 3. USCIS is in the process of updating its change control/change management process to better address security and emergency changes. USCIS plans to implement the updated process by

[7] ICE personnel currently perform user administration functions for the Central Index System.

October 1, 2005. In addition, the USCIS Office of the CIO will reanalyze recent changes to the Central Index System applications and verify that the changes were properly reviewed, tested, and authorized via the change control process. Beginning in fiscal year 2006, these reviews will be conducted at least every quarter.

We agree that the actions USCIS plans to take satisfy the intent of the recommendation.

USCIS concurs with recommendation 4. USCIS is planning to reassess all of the component's major applications and general support systems, beginning in the first quarter of fiscal year 2006. This process will include an assessment of each system's existing contingency plan, as well as the use of a standard template to develop site and application specific contingency plans. Once the plans have been developed, USCIS will establish a process to conduct annual tests of the plans.

We accept USCIS' response to develop and annually test an IT contingency plan for the Central Index System. However, USCIS did not indicate that quarterly data restoration tests would be performed. We maintain that USCIS should have a process to ensure that quarterly data restoration tests are conducted, in accordance with DHS requirements.

USCIS concurs with recommendation 5. USCIS plans to reexamine its information classification guidelines as well as all information classifications during the first quarter of fiscal year 2006, to ensure that appropriate security controls have been implemented. However, USCIS plans to decommission the Central Index System as part of its IT Transformation Program. The Central Index System will be replaced by one or more systems that include more stringent security controls, - .

We accept USCIS' response to reexamine its information classifications as well as implement - for the Central Index System's replacement systems. However, until ------------ --------- are implemented, USCIS should document the risk associated with ----- ------------------------------------ and ensure that the designated approving authority formally accepts this risk.

USCIS concurs with recommendation 6. USCIS is taking steps to improve security monitoring and incident reporting for the Central Index System. In addition to the corrective actions listed for OIG recommendations 1-5, USCIS has transferred ISSO responsibilities from the Office of Records Services to the Office of the CIO and appointed a new ISSO for the system. USCIS is currently in the process of implementing revised security procedures and controls, as well as defining the duties and responsibilities for the ISSO. USCIS plans to complete these activities by September 30, 2005. In addition, the Office of the CIO plans to reexamine the user administration and management procedures for the Central Index System, beginning in the first quarter of fiscal year 2005.

We agree that the actions USCIS plans to take satisfy the intent of the recommendation.

Purpose, Scope, and Methodology

The objective of this audit was to determine whether DHS has implemented adequate and effective controls over sensitive data contained in its mission critical databases. As part of our audit of DHS database security, we conducted reviews of critical databases at the following DHS components:

- Emergency Preparedness and Response
- United States Citizenship and Immigration Services
- United States Coast Guard
- United States Secret Service

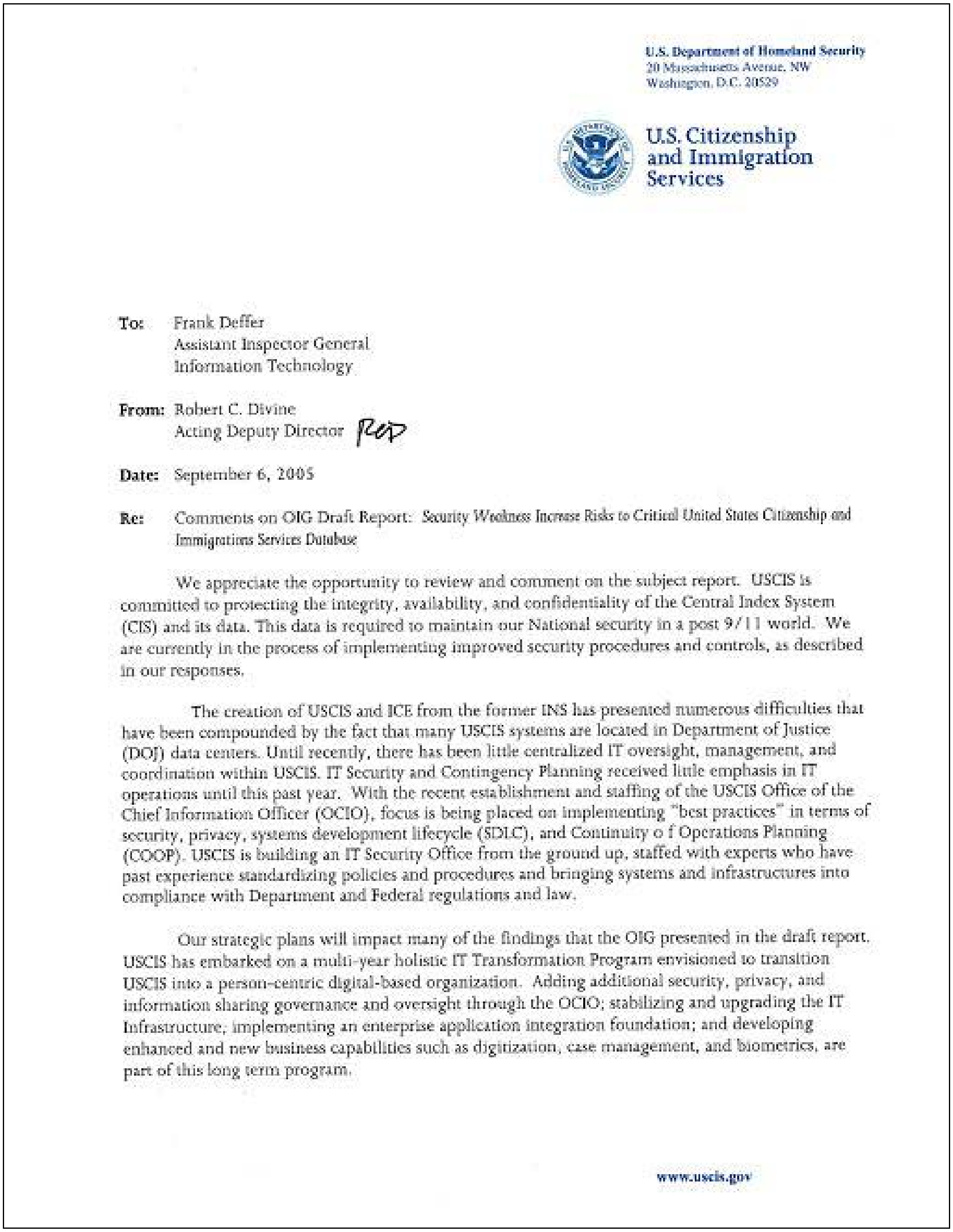
For each of the databases included, we determined whether the component had implemented effective access controls, continuity of operations capabilities, and change management processes. Our focus was to test the implementation of secure configurations on the hosts controlling access to sensitive DHS data. In addition, we obtained FISMA information required for our annual independent evaluation.

To identify USCIS' critical database systems, we analyzed the DHS Enterprise Architecture inventory of the Department's IT assets as of October 2004. We supplemented this information with NIST SP 800-26 Security Self-Assessments, where available. Based on our analysis, we selected the Central Index System for inclusion in our review.

To evaluate the effectiveness of controls implemented for the Central Index System, we performed extensive manual security parameter checks on the Central Index System mainframe computer operating system, security software, and DBMS. Upon completion of the tests, we discussed the results with USCIS.

We conducted fieldwork at the USCIS and ICE facilities in Washington, DC; the DOJ *Justice Data Centers* in --------------------- and - ; and, the OIG's ATL. We conducted our audit from January to May 2005 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix D.

Our principal points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits at (202) 254-4100; and Edward G. Coleman, Director, Information Security Audit Division at (202) 254-5444.



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

U.S. Citizenship
and Immigration
Services

To: Frank Deffer
Assistant Inspector General
Information Technology

From: Robert C. Divine
Acting Deputy Director RCD

Date: September 6, 2005

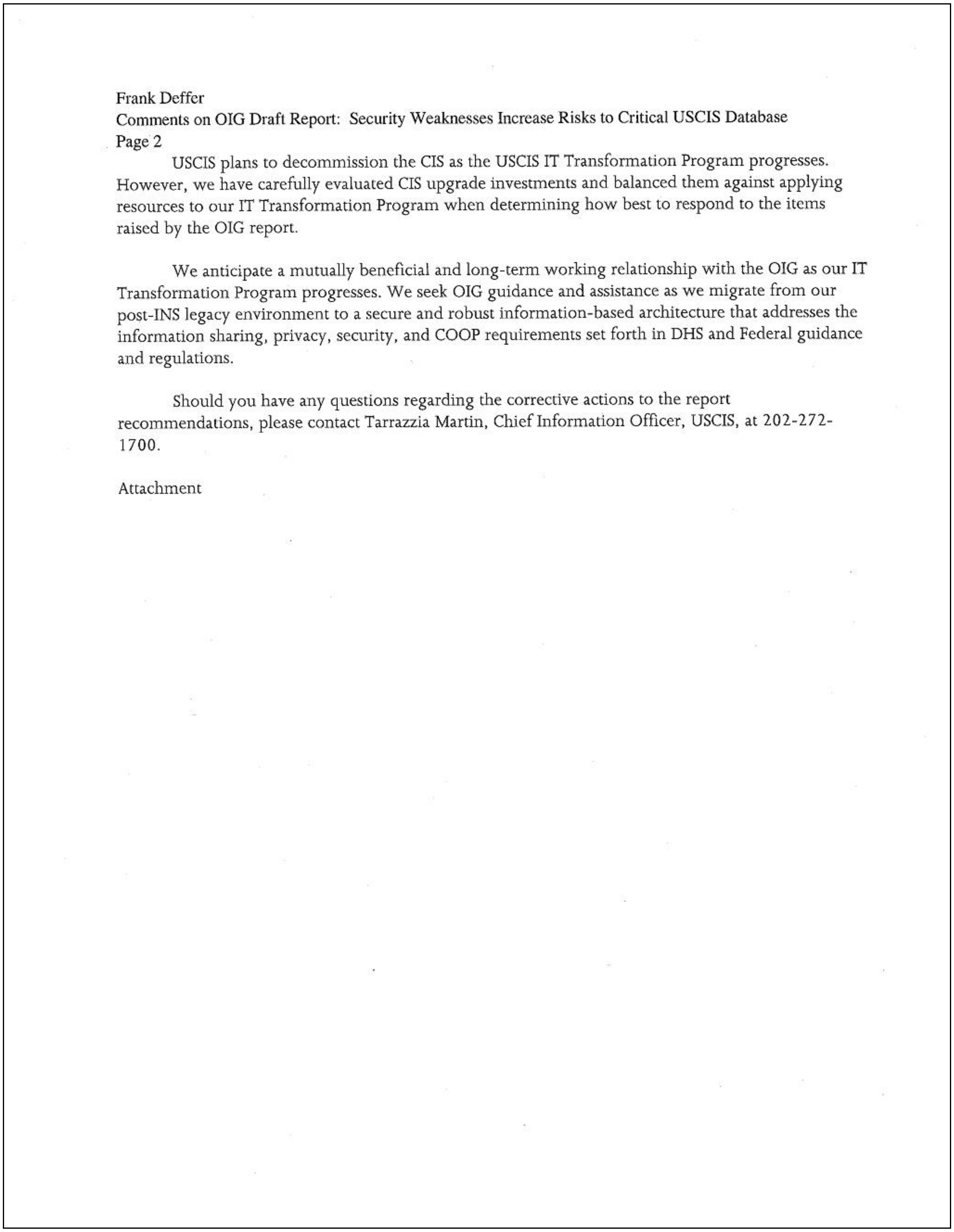
Re: Comments on OIG Draft Report: *Security Weakness Increase Risks to Critical United States Citizenship and Immigrations Services Database*

We appreciate the opportunity to review and comment on the subject report. USCIS is committed to protecting the integrity, availability, and confidentiality of the Central Index System (CIS) and its data. This data is required to maintain our National security in a post 9/11 world. We are currently in the process of implementing improved security procedures and controls, as described in our responses.

The creation of USCIS and ICE from the former INS has presented numerous difficulties that have been compounded by the fact that many USCIS systems are located in Department of Justice (DOJ) data centers. Until recently, there has been little centralized IT oversight, management, and coordination within USCIS. IT Security and Contingency Planning received little emphasis in IT operations until this past year. With the recent establishment and staffing of the USCIS Office of the Chief Information Officer (OCIO), focus is being placed on implementing "best practices" in terms of security, privacy, systems development lifecycle (SDLC), and Continuity o f Operations Planning (COOP). USCIS is building an IT Security Office from the ground up, staffed with experts who have past experience standardizing policies and procedures and bringing systems and infrastructures into compliance with Department and Federal regulations and law.

Our strategic plans will impact many of the findings that the OIG presented in the draft 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.

www.uscis.gov



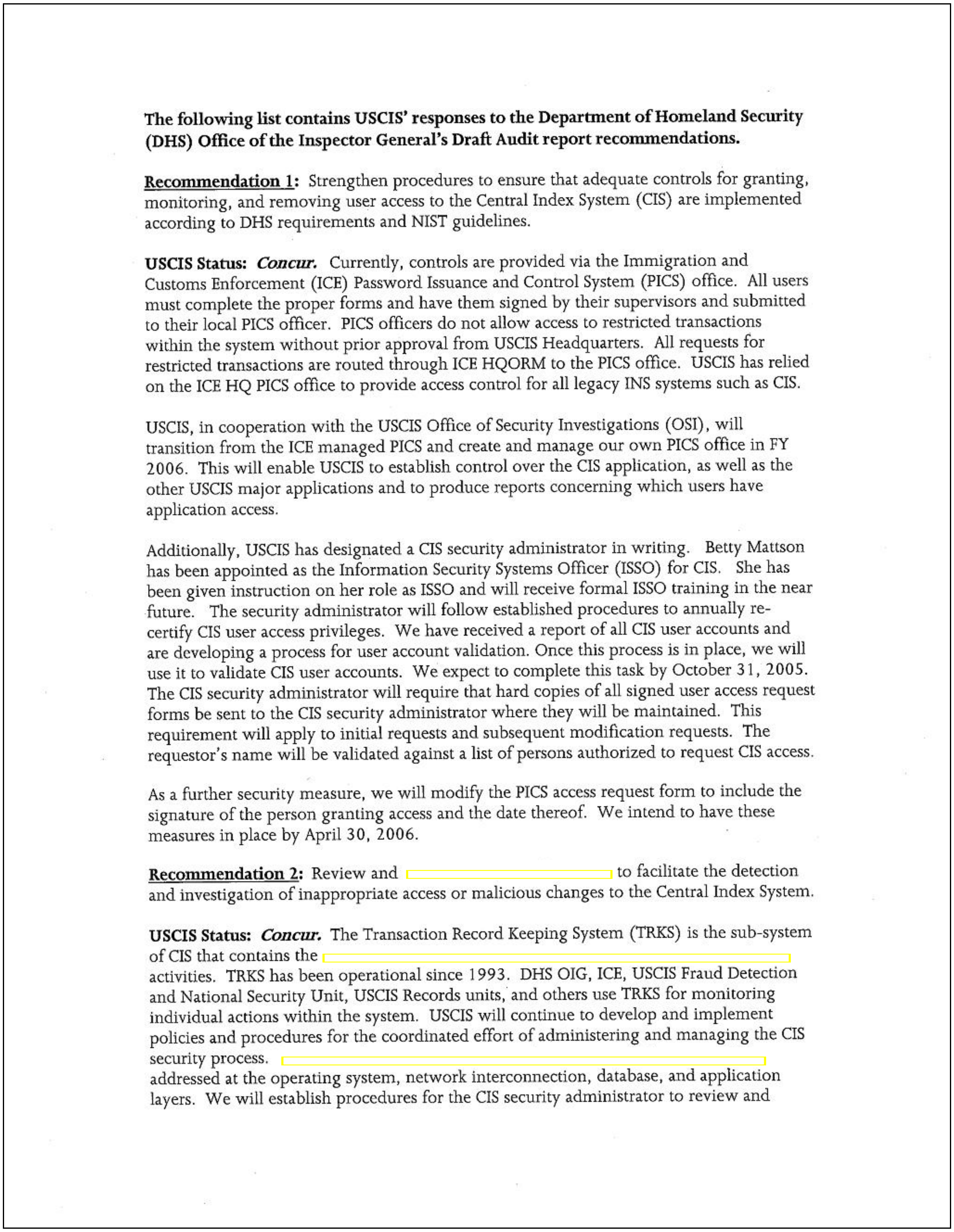
Frank Deffer
Comments on OIG Draft Report: Security Weaknesses Increase Risks to Critical USCIS Database
Page 2

USCIS plans to decommission the CIS as the USCIS IT Transformation Program progresses. However, we have carefully evaluated CIS upgrade investments and balanced them against applying resources to our IT Transformation Program when determining how best to respond to the items raised by the OIG report.

We anticipate a mutually beneficial and long-term working relationship with the OIG as our IT Transformation Program progresses. We seek OIG guidance and assistance as we migrate from our post-INS legacy environment to a secure and robust information-based architecture that addresses the information sharing, privacy, security, and COOP requirements set forth in DHS and Federal guidance and regulations.

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



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

Recommendation 1: Strengthen procedures to ensure that adequate controls for granting, monitoring, and removing user access to the Central Index System (CIS) are implemented according to DHS requirements and NIST guidelines.

USCIS Status: ***Concur.*** Currently, controls are provided via the Immigration and Customs Enforcement (ICE) Password Issuance and Control System (PICS) office. All users must complete the proper forms and have them signed by their supervisors and submitted to their local PICS officer. PICS officers do not allow access to restricted transactions within the system without prior approval from USCIS Headquarters. All requests for restricted transactions are routed through ICE HQORM to the PICS office. USCIS has relied on the ICE HQ PICS office to provide access control for all legacy INS systems such as CIS.

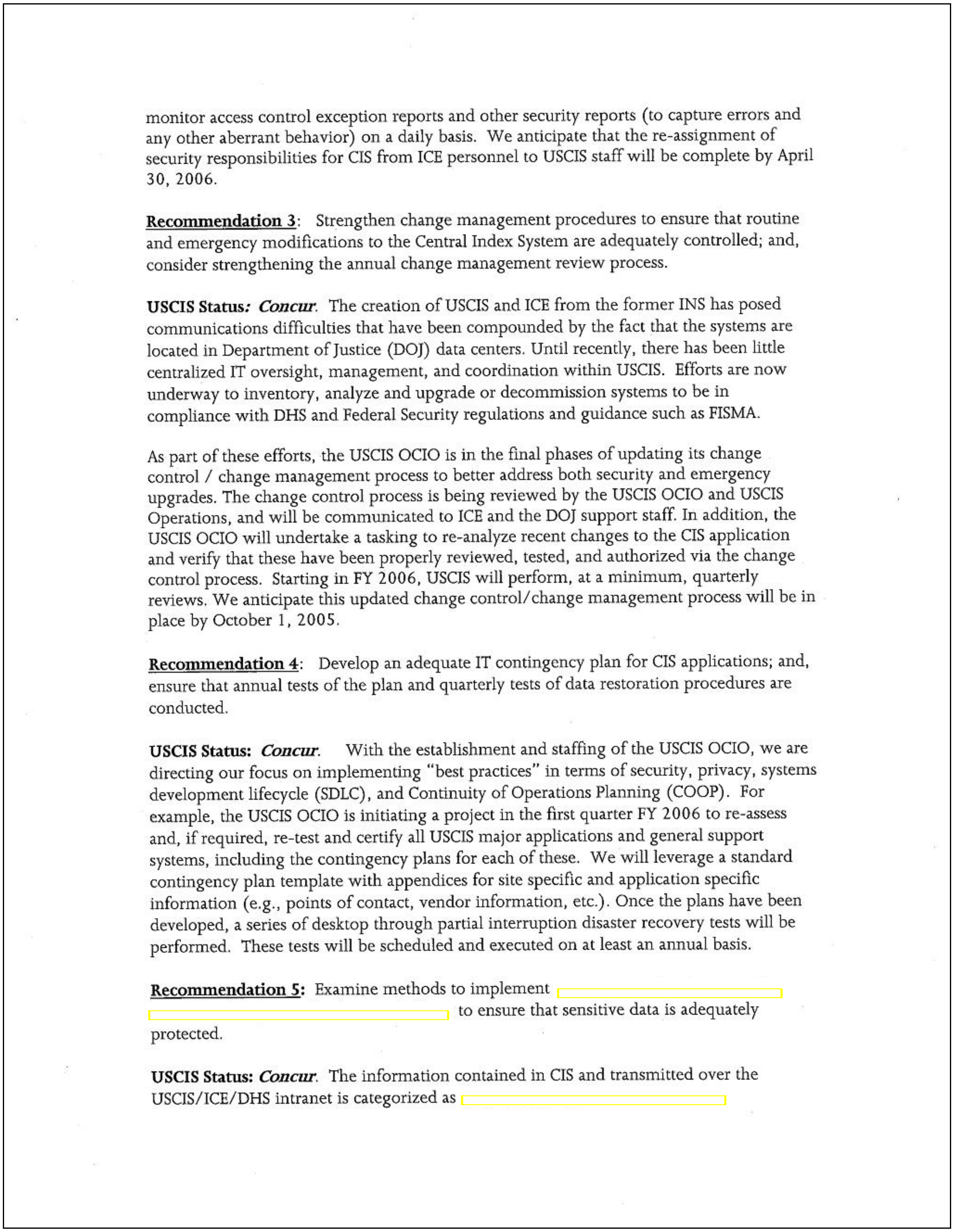
USCIS, in cooperation with the USCIS Office of Security Investigations (OSI), will transition from the ICE managed PICS and create and manage our own PICS office in FY 2006. This will enable USCIS to establish control over the CIS application, as well as the other USCIS major applications and to produce reports concerning which users have application access.

Additionally, USCIS has designated a CIS security administrator in writing. Betty Mattson has been appointed as the Information Security Systems Officer (ISSO) for CIS. She has been given instruction on her role as ISSO and will receive formal ISSO training in the near future. The security administrator will follow established procedures to annually re-certify CIS user access privileges. We have received a report of all CIS user accounts and are developing a process for user account validation. Once this process is in place, we will use it to validate CIS user accounts. We expect to complete this task by October 31, 2005. The CIS security administrator will require that hard copies of all signed user access request forms be sent to the CIS security administrator where they will be maintained. This requirement will apply to initial requests and subsequent modification requests. The requestor's name will be validated against a list of persons authorized to request CIS access.

As a further security measure, we will modify the PICS access request form to include the signature of the person granting access and the date thereof. We intend to have these measures in place by April 30, 2006.

Recommendation 2: Review and [redacted] to facilitate the detection and investigation of inappropriate access or malicious changes to the Central Index System.

USCIS Status: ***Concur.*** The Transaction Record Keeping System (TRKS) is the sub-system of CIS that contains the [redacted] activities. TRKS has been operational since 1993. DHS OIG, ICE, USCIS Fraud Detection and National Security Unit, USCIS Records units, and others use TRKS for monitoring individual actions within the system. USCIS will continue to develop and implement policies and procedures for the coordinated effort of administering and managing the CIS security process. [redacted] addressed at the operating system, network interconnection, database, and application layers. We will establish procedures for the CIS 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. We anticipate that the re-assignment of security responsibilities for CIS from ICE personnel to USCIS staff will be complete by April 30, 2006.

Recommendation 3: Strengthen change management procedures to ensure that routine and emergency modifications to the Central Index System are adequately controlled; and, consider strengthening the annual change management review process.

USCIS Status*: Concur*. The creation of USCIS and ICE from the former INS has posed communications difficulties that have been compounded by the fact that the systems are located in Department of Justice (DOJ) data centers. Until recently, there has been little centralized IT oversight, management, and coordination within USCIS. Efforts are now underway to inventory, analyze and upgrade or decommission systems to be in compliance with DHS and Federal Security regulations and guidance such as FISMA.

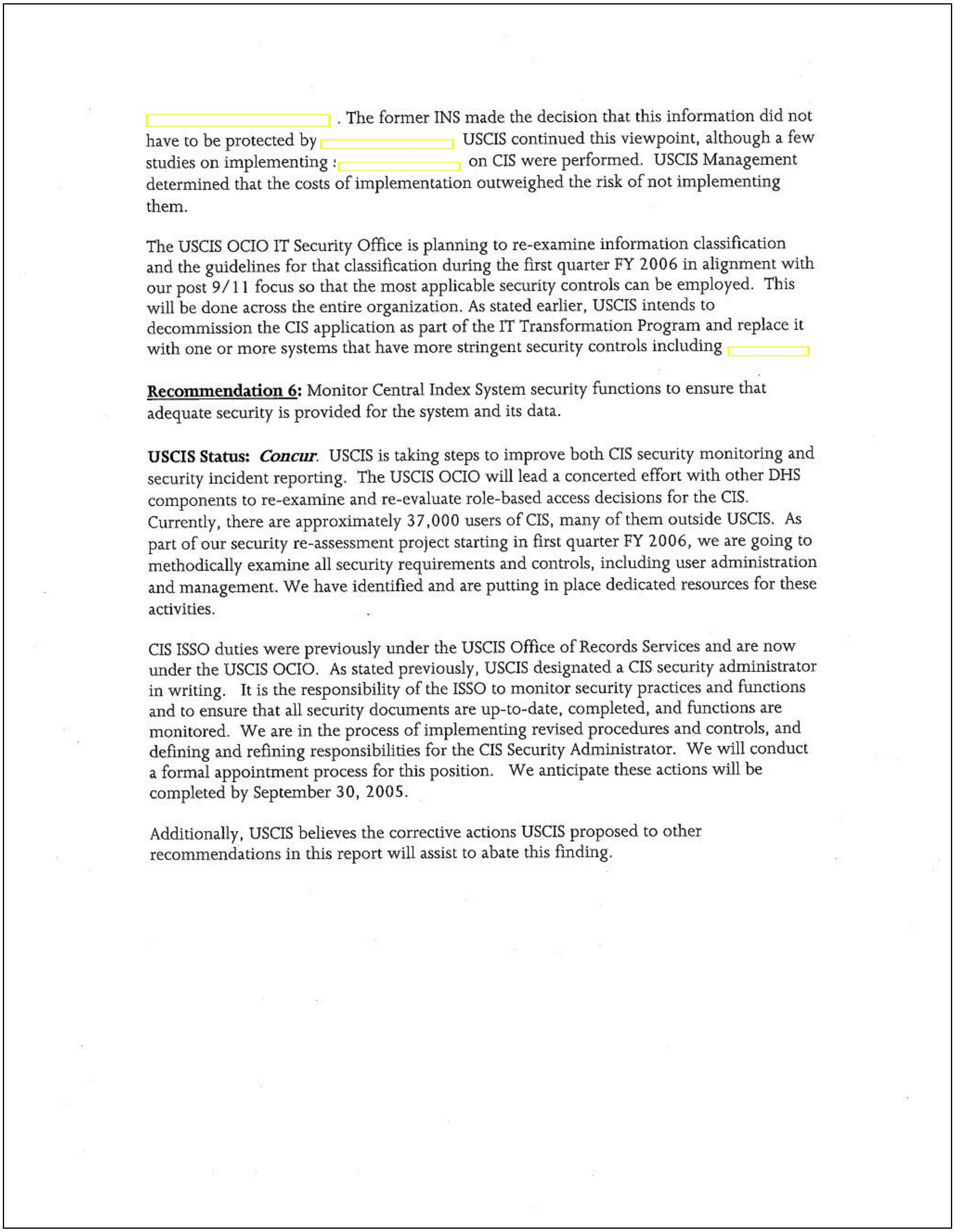
As part of these efforts, the USCIS OCIO is in the final phases of updating its change control / change management process to better address both security and emergency upgrades. The change control process is being reviewed by the USCIS OCIO and USCIS Operations, and will be communicated to ICE and the DOJ support staff. In addition, the USCIS OCIO will undertake a tasking to re-analyze recent changes to the CIS application and verify that these have been properly reviewed, tested, and authorized via the change control process. Starting in FY 2006, USCIS will perform, at a minimum, quarterly reviews. We anticipate this updated change control/change management process will be in place by October 1, 2005.

Recommendation 4: Develop an adequate IT contingency plan for CIS applications; and, ensure that annual tests of the plan and quarterly tests of data restoration procedures are conducted.

USCIS Status: *Concur*. With the establishment and staffing of the USCIS OCIO, we are directing our focus on implementing "best practices" in terms of security, privacy, systems development lifecycle (SDLC), and Continuity of Operations Planning (COOP). For example, the USCIS OCIO is initiating a project in the first quarter FY 2006 to re-assess and, if required, re-test and certify all USCIS major applications and general support systems, including the contingency plans for each of these. We will leverage a standard contingency plan template with appendices for site specific and application specific information (e.g., points of contact, vendor information, etc.). Once the plans have been developed, a series of desktop through partial interruption disaster recovery tests will be performed. These tests will be scheduled and executed on at least an annual basis.

Recommendation 5: Examine methods to implement [redacted] [redacted] to ensure that sensitive data is adequately protected.

USCIS Status: *Concur*. The information contained in CIS and transmitted over the USCIS/ICE/DHS intranet is categorized as [redacted]



[redacted]. The former INS made the decision that this information did not have to be protected by [redacted] USCIS continued this viewpoint, although a few studies on implementing [redacted] on CIS were performed. USCIS Management determined that the costs of implementation outweighed the risk of not implementing them.

The USCIS OCIO IT Security Office is planning to re-examine information classification and the guidelines for that classification during the first quarter FY 2006 in alignment with our post 9/11 focus so that the most applicable security controls can be employed. This will be done across the entire organization. As stated earlier, USCIS intends to decommission the CIS application as part of the IT Transformation Program and replace it with one or more systems that have more stringent security controls including [redacted]

Recommendation 6: Monitor Central Index System security functions to ensure that adequate security is provided for the system and its data.

USCIS Status: ***Concur***. USCIS is taking steps to improve both CIS security monitoring and security incident reporting. The USCIS OCIO will lead a concerted effort with other DHS components to re-examine and re-evaluate role-based access decisions for the CIS. Currently, there are approximately 37,000 users of CIS, many of them outside USCIS. As part of our security re-assessment project starting in first quarter FY 2006, we are going to methodically examine all security requirements and controls, including user administration and management. We have identified and are putting in place dedicated resources for these activities.

CIS ISSO duties were previously under the USCIS Office of Records Services and are now under the USCIS OCIO. As stated previously, USCIS designated a CIS security administrator in writing. It is the responsibility of the ISSO to monitor security practices and functions and to ensure that all security documents are up-to-date, completed, and functions are monitored. We are in the process of implementing revised procedures and controls, and defining and refining responsibilities for the CIS Security Administrator. We will conduct a formal appointment process for this position. We anticipate these actions will be completed by September 30, 2005.

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

FISMA Requirements

Title III of the E-Government Act, entitled FISMA, provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support federal operations and assets.[8] The agency's security program should provide security for the information as well as the systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

To comply with OMB's FISMA reporting requirements, we evaluated the major applications selected for this audit to determine whether DHS continues to make progress in implementing its agency-wide information security program. We collected information relative to certification and accreditation (C&A), system impact level determination, NIST SP 800-26 annual assessment, security control costs integrated into the life cycle of the system, assessment of E-authentication risks, specialized security training, and plan of action and milestones (POA&M).[9]

Our evaluation of the Central Index System shows that the USCIS has not implemented certain security management practices into its information security program, as required by FISMA.

[8] The E-Government Act of 2002 (Public Law 107-347), signed into law on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States.
[9] As required by: OMB M-04-04, *E-Authentication Guidance for Federal Agencies* and NIST 800-63, *Electronic Authentication Guideline.*

Table 1: FISMA Compliance Metrics

FISMA Reporting Requirements	USCIS	Notes
Does the major application have a complete and current C&A, including a risk assessment and security plan?	Yes	The DOJ mainframe that the Central Index System resides on and the Central Index System applications were certified and accredited separately. The mainframe was issued authority to operate (ATO) on December 29, 2004, and the Central Index System applications were issued ATO on December 29, 2003. Both C&A packages include a security plan and a risk assessment.
Has the major application's impact level been determined according to Federal Information Processing Standard 199 criteria?	Yes	The loss of confidentiality, availability or integrity of the Central Index System would have a high impact on USCIS' mission.
Does the major application have a complete and current NIST SP 800-26 annual assessment?	Yes	An assessment of the Central Index System was completed on October 11, 2004.
Does the assessment indicate that security controls have been tested and evaluated in the last year?	**No**	The assessment indicates that controls are routinely tested. However, we found that periodic vulnerability assessments or configuration reviews are not performed.
Does the assessment indicate that a contingency plan has been established and tested?	**No**	The assessment indicates that an IT contingency plan has been developed but not tested. However, we found that the IT contingency plan for Central Index System applications is not complete or current.
Have security control costs been integrated into the life cycle of the system?	Yes	Security control costs are incorporated and reported to OMB as 10 percent of the system's operations and maintenance funding.
Has an assessment of E-Authentication risk been performed for the major application?	Not Applicable	The Central Index System does not provide direct services to the public.
Have the system and database administrators obtained specialized security training?	**No**	System and database administrators receive the same annual security awareness training that all component personnel receive. Specialized security training is not provided.
Does the major application have any existing POA&Ms?	Yes	Although the POA&Ms for the Central Index System were not complete or current at the beginning of our review, they were updated prior to the completion of our audit. As of May 12, 2005, POA&Ms were entered for 16 Central Index System weaknesses.

Source: OIG table based on interviews with USCIS personnel and analysis of database documentation.

Information Security Audits Division
Edward G. Coleman, Director
Patrick Nadon, Audit Manager
Jason Bakelar, Audit Team Leader
Chris Udoji, Auditor
Meghan Sanborn, Referencer

Advanced Technology Division
Jim Lantzy, Director
Michael Goodman, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
USCIS, Director
Executive Secretary
General Counsel
Chief Information Officer
Chief Information Security Officer
Public Affairs
USCIS, Chief Information Officer
USCIS, Audit Liaison
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program
Chief Information Officer Audit Liaison
Office of Security

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Appropriate Congressional Oversight and Appropriations Committees

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.

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 DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or e-mail DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.