Department of Homeland Security
Office of Inspector General

Examining Insider Threat Risk at the U.S. Citizenship and Immigration Services (Redacted)

OIG-11-33

January 2011

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland Security

JAN 20 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of U.S. Citizenship and Immigration Services' efforts to protect information systems from insider threats. It is based on interviews with employees and officials, direct observations, and a review of applicable documents by the Software Engineering Institute at Carnegie Mellon University.

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. We trust 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.

Frank Deffer
Assistant Inspector General,
Information Technology Audits

Examining Insider Threat Risk at the U.S. Citizenship and Immigration Services

Prepared for Department of Homeland Security

Office of Inspector General

by the Software Engineering Institute at Carnegie Mellon University

Insider Threat Center at CERT

December 2010

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE **MATERIAL IS FURNISHED ON AN "AS-IS" BASIS**. **CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND**, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, **WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL**. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Table of Contents

Executive Summary

The U.S. Department of Homeland Security, Office of Inspector General engaged the Insider Threat Center at CERT, of the Software Engineering Institute at Carnegie Mellon University to conduct an insider threat assessment of U.S. Citizenship and Immigration Services. The objective of the assessment was to determine how U.S. Citizenship and Immigration Services has taken steps to protect its information technology systems and data from the threats posed by employees and contractors. The assessment evaluated U.S. Citizenship and Immigration Services against approximately 400 real insider threat compromises documented in the CERT Insider Threat Case database. These cases, all prosecuted in the United States, include fraud, sabotage, and theft of intellectual property.

The assessment team performed fieldwork in the national capital region, Vermont Service Center, and U.S. Citizenship and Immigration Services Burlington offices. Due to the limited scope of the assessment, systems reviewed, and locations visited, CERT was not able to verify the institutionalization and enforcement of any U.S. Citizenship and Immigration Services' policies or render an overall opinion of the effectiveness of U.S. Citizenship and Immigration Services insider threat posture. The Office of Inspector General did not request CERT to conduct a comprehensive information system's technical security controls review or vulnerability assessment to determine the susceptibility to internal threats. The Office of Inspector General may perform an in-depth follow up review to render an overall opinion of the effectiveness of U.S. Citizenship and Immigration Services insider threat posture.

U.S. Citizenship and Immigration Services has made progress in implementing elements of an effective insider threat program. Specifically, it has established a Conviction Task Force to review former employees convicted of criminal misconduct within the scope of their duties; performs risk management for information technology and financial management; developed exit procedures for employees; improved protection of its facilities and assets; and adheres to formalized processes for some systems. In addition, it is implementing Homeland Security Presidential Directive 12 for physical and electronic account management.

While these efforts have resulted in some improvements, U.S. Citizenship and Immigration Services has opportunities to improve its security posture against threats posed by employees and contractors. For example, it can institute an enterprise risk management plan and incorporate insider threat risk mitigation strategies into its new business processes. It can also centralize records of misconduct and violations; institute a logging strategy to preserve system activities; implement separation of duties for adjudicative decisions; conduct audits of non-U.S. Citizenship and Immigration Services accounts; employ consistent policies for physical security; and consistently enforce employee exit procedures.

The assessment team is making 18 recommendations to the Director of U.S. Citizenship and Immigration Services to strengthen the department's security posture against malicious insider threats. USCIS concurred with all of our recommendations and has already begun to take actions to implement them. The department's response is included, in its entirety, as appendix I.

Background

The U.S. Department of Homeland Security (DHS), Office of Inspector General (DHS OIG) engaged the CERT program in the Software Engineering Institute at Carnegie Mellon University to conduct an insider threat vulnerability assessment of U.S. Citizenship and Immigration Services (USCIS). The project approaches the insider threat problem on two primary fronts:

- The human behavioral component
- The technological solution for automating prevention and detection capabilities to identify, measure, monitor, and control insider threat vectors

Insiders can be current or former employees, contractors, or business partners who have or had authorized access to their organization's system and networks. They are familiar with internal policies, procedures, and technology and can exploit that knowledge to facilitate attacks and even collude with external attackers. CERT's research, conducted since 2001, has focused on gathering data about actual malicious insider acts, including information technology (IT) sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to our Nation's critical infrastructures.

CERT developed an insider threat vulnerability assessment instrument for evaluating vulnerabilities to insider threat based on research to date. Because of the complexity of the insider threat problem—involving security officers, information technology, information security, management, data owners, software engineering, and human resources—organizations need assistance in merging the wealth of available guidance into a single, actionable framework. CERT advises organizations to use this assessment instrument to help safeguard their critical infrastructure.

CERT built the assessment based on research of approximately 400 insider threat cases in the CERT Insider Threat Case database.[1] These cases are a collection of real insider threat compromises—primarily fraud, sabotage, and theft of intellectual property—that have been prosecuted in the United States. Starting in 2002, CERT collaborated with U.S. Secret Service behavioral psychologists to collect approximately 150 actual insider threat cases that occurred in U.S. critical infrastructure sectors between 1996 and 2002, and examined them from both a technical and a behavioral perspective. Since that original study, CERT has continued to add cases, with funding from Carnegie Mellon's CyLab[2], bringing the case library to a total of approximately 400 cases. The instrument encompasses technical, behavioral, process, and policy issues, and is structured around information technology, information security, human resources, physical security, business processes, legal and contracting, management, and organizational issues.

---

[1] Note that the database does not contain national security espionage cases involving classified information.

[2] http://www.cylab.cmu.edu/

Objective

The objective of the insider threat vulnerability assessment was to determine how USCIS has taken steps to protect its IT systems and data from the threat posed by employees and contractors. This assessment was based on behavioral as well as technical experience and it is intended to assist USCIS in safeguarding its critical infrastructure. The assessment will:

- Enable USCIS to gain a better understanding of its vulnerability to insider threat and provide an ability to identify and manage associated risks
- Identify technical, organizational, personnel, business security, and process issues into a single, actionable framework
- Identity short-term countermeasures against insider threats
- Help guide USCIS in its ongoing risk management process for implementing long-term, strategic countermeasures against insider threats

Scope

USCIS employs approximately 18,000 government employees and contractors located at 250 offices throughout the world.[3] The insider threat vulnerability assessment is intended to focus on critical systems and high-risk areas of concern that can be assessed in a 3 to 5 day timeframe. Therefore, at a pre-assessment walkthrough meeting, USCIS staff identified 3 systems of the 96 systems used by the agency as critical to its overall mission:

- Verification Information System (VIS)—this public-facing system is composed of five different applications. The purpose of the system is to provide—
  - Immigration status information to government benefit-granting organizations to help them determine the eligibility of aliens who apply for benefits
  - A means for private employers to perform employment eligibility verification of newly hired employees
- Computer Linked Application Information Management System (CLAIMS)—This system provides the following functions:

[3] http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=2af29c7755cb9010VgnVCM10000045f3d6a1RCRD&vgnextchannel=2af29c7755cb9010VgnVCM10000045f3d6a1RCRD

    - CLAIMS 3-Local Area Network (C3-LAN) was originally developed to track the receipting of applicant or petitioner remittances and to produce notices documenting the remittance. C3-LAN now includes adjudication, archive, card production, case history, case transfer, on-demand reports, electronic file tracking, image capture, production statistics, status update, and electronic ingest of application data captured through the E-Filing web application and the Department of Treasury sponsored lockbox operations.
    - C3 mainframe supports processing of USCIS applications and petitions for various immigrant benefits (e.g., change of status, employment authorization, and extension of stay).
- Fraud Detection and National Security Data System (FDNS DS)—This system was developed to identify threats to national security, combat benefit fraud, and locate and remove vulnerabilities that compromise the integrity of the legal immigration system.

It is important to note that the insider threat vulnerability assessment is limited to areas of concern observed in the hundreds of cases in the CERT Insider Threat database. People, technology, and organizations are constantly changing, and malicious insiders continue to come up with new avenues of attack in order to defeat a previously effective countermeasure. However, many of the countermeasures suggested in this report are applicable to a multitude of attack vectors.

It is also important to note that CERT's insider threat research has only explored *intentional* insider crimes. Accidental data leakage is an area of significant concern for organizations; however, CERT has not yet explored that aspect of insider threat. In addition, the focus of the research to date is to describe how the insider threat problem evolves over time. CERT's long-term research does include measuring the effectiveness of mitigation strategies.

Assessment Process/Methodology

An entrance conference was conducted by the DHS OIG, CERT, and USCIS on February 23, 2010. The entrance conference introduced USCIS to the CERT assessment team. Following the entrance conference, a pre-assessment walkthrough was held at USCIS headquarters on March 10, 2010. At that meeting, the CERT assessment team and the DHS OIG team explained the assessment process to representatives of USCIS. USCIS provided some documentation to the assessment team at that time and more documents throughout the assessment; those documents were reviewed to provide substantiation for findings in this report.

USCIS identified 96 systems it uses. Following the initial meeting, USCIS leadership and the assessment team chose the VIS, CLAIMS, and FDNS DS systems because they were critical to the overall mission of USCIS. These three systems were the focus of the 5 day onsite assessment.

At the pre-assessment walk-through, USCIS indicated that it had created a Convictions Task Force to review the activities of 10 former employees convicted of criminal misconduct within the scope of their official duties. The purpose of the task force is to identify issues these employees exploited to commit their crimes. The task force intended to develop findings and recommendations aimed at preventing similar crimes in the future. It graciously extended an invitation to the CERT and DHS OIG teams to participate. As a result, the teams observed, or reviewed transcripts of, all telephone conferences conducted by the task force. These findings are reflected in this report.

The CERT insider threat team and the DHS OIG liaison were on site at various USCIS locations in the national capital region (NCR) from March 30 through April 1, 2010.

The DHS OIG liaisons were present at all interviews. The DHS OIG attended these interviews as an observer and assisted CERT as needed.

Face-to-face interviews were conducted with approximately 58 representatives in the NCR, followed by 32 representatives in the Vermont Service Center and USCIS Burlington offices. In addition, telephone conferences were held with staff from the Office of Security and Integrity (OSI) Investigations Division and the Security Network Operations Center (SNOC). Interviewees represented the following areas:

- Data Owners (VIS, CLAIMS, and FDNS DS)
- Computer Sciences Corporation (CSC) (software engineering and operational support for VIS, CLAIMS, and FDNS DS)

- OSI (Physical Security, Regional Security, Investigations, Personnel Security, Counter-intelligence)
- Human Capital and Training (Training, Human Resources Operations Center, Labor Employee Relations)
- Office of Information Technology (OIT) (IT Security, Computer Security Incident Response Team, Security and Network Operations Center, Account Management, Enterprise Operations)
- Legal (Procurement Law)
- Vermont Service Center (adjudicators, data entry clerks, supervisor, directors, OIT, software engineering)

All interviews were considered confidential; no record of participating employees is included in this report or in subsequent briefings. Findings are attributed only to a group or department interviewed, a document, the Convictions Task Force telephone conferences, or direct observation.

Results of Assessment

This section summarizes the insider threat assessment findings derived from 3 days of onsite interviews with USCIS employees and contractors in the NCR, followed by 2 days in Burlington and St. Albans, Vermont. This section describes the most prevalent, high-impact, areas of concern. For a complete list of all areas of concern, refer to the appendixes of this report. The information in this report is based on interviews, USCIS Convictions Task Force telephone conferences, and document reviews. The assessment team did not have the opportunity to perform alternate validation methods, including process observation and direct testing. The team relied on the responses provided by employees and contractors during face-to-face and telephone interviews, as well as reviews of the documentation provided. When appropriate, the team attempted to interview multiple individuals to substantiate a response to a given assessment question. Due to the limited scope of the process, the assessment team was not able to verify the institutionalization or enforcement of any USCIS policies.

Organizational

Many organizations that have suffered a loss from an insider threat have done so, at least partially, because there were hindrances to effective communication and risk management across departments and their subcomponents. The following assessment results for organizational issues pertain to risk management and the ongoing Transformation effort. Communication and a common belief and understanding of risks posed to USCIS across departments will be essential to developing an effective insider threat mitigation plan.

Enterprise Risk Management

USCIS is in a difficult position. Part of its mission is to provide customer service to those seeking immigration and citizenship benefits from the U.S. government. It is challenging to optimize business processes for customer service while at the same time implementing protective measures to counter the risk posed by granting those very benefits. Many USCIS employees interviewed for this assessment identified the organization's primary risk as allowing the next terrorist to live and work legally in the United States. They desire help in identifying and implementing internal controls to counter that risk. Some of the interviewees, however—even some of the information system security officers (ISSOs) and data owners—focused on leakage of personally identifiable information (PII) as their primary concern. After delving into the matter with the assessment team, they came to understand the risk posed by exposure or misuse of critical data as the greatest risk faced by USCIS, primarily because such a security breach could result in allowing a terrorist into the country legally.

A critical issue for USCIS is ensuring that the entire organization is risk aware, and implementing a formal risk management process to address risk consistently and continually across the enterprise. There does not appear to be a consistent understanding of the broad spectrum of risks facing USCIS. The assessment team was told there is no enterprise-wide risk management program at USCIS. OIT performs risk management for Information Technology (IT), and Financial Management performs risk management for financial matters, but no one was aware of any enterprise-wide efforts. In addition, each field office and service center appears to operate fairly independently. It is important for those organizations to work together to identify, prioritize, and address risk. Ongoing communication between all components of USCIS will help ensure that new threats, attack vectors, and countermeasures are communicated and handled effectively by all.

In addition, USCIS employees and contractors hold the keys to one of the world's most coveted kingdoms—U.S. citizenship. This makes employees and contractors attractive targets for recruitment. Because of the sensitive nature of USCIS mission, some of its employees and contractors have been targets for recruitment for theft or unauthorized modification of USCIS data. All employees should be aware of the consequences of participating in fraud against USCIS. They should also be instructed on how to report solicitations made to commit fraud.

Transformation

Transformation is a large business process reengineering effort in USCIS primarily focused on improved customer service, workflow automation, fraud detection, and national security issues. USCIS is relying heavily on Transformation to correct many of the problems resulting from legacy systems. This reliance on a single effort makes its effectiveness very important. The team found the Transformation effort to be a massive undertaking that appears to be implementing a very detailed project plan.

Based on the team's review of the requirements for fraud detection and national security issues, it appears there are no requirements to address insider threats. The assessment team reviewed five comprehensive Transformation documents as part of this assessment. The documents describe system requirements in detail. Fraud detection refers to detection of fraud perpetrated by applicants and petitioners; national security issues focus on the handling of investigations within USCIS that involve national security issues.

Again, an enterprise risk management approach should be considered when defining requirements for Transformation. Insiders at USCIS have perpetrated fraud in the past, as evidenced by the Convictions Task Force. In addition, USCIS insiders are capable of granting legal residency or citizenship status to someone who poses a national security risk to the United States.

Training and Awareness

It is essential that security awareness training is consistently provided to all employees to ensure security policies and practices are institutionalized throughout an organization. Many times, co-workers and supervisors are the first people to observe concerning behavior exhibited by malicious insiders. Failure to report concerning behavior by co-workers or others in an organization was a primary reason insiders in the CERT Insider Threat Case database continued to set up or carry out their attacks.

USCIS should continue to provide security awareness training to all employees and contractors across the globe. This training should be consistently applied to each site, with a consistent message of security of USCIS people, systems, and data. It is imperative that all USCIS employees be responsible for achieving the mission of USCIS and protecting the critical assets to the highest extent possible.

Human Resources

An organization's approach to reducing insider threat should focus on proactively managing employee issues and behaviors. This concept begins with effective hiring processes and background investigations to screen potential candidates. Organizations should also train supervisors to monitor and respond to behaviors of concern exhibited by current employees. Some cases from the CERT Insider Threat database revealed that suspicious activity was noticed in the workplace but not acted upon. Organizations must establish a well-organized and professional method for handling negative employment issues and ensuring that human resource policy violations are addressed.

Organizational issues related to functions shared by human resources (HR) and security personnel are at the heart of insider risk management. Employee screening and selection is vital to preventing candidates with known behavioral risk factors from entering the organization; or, if they do, ensuring that these risks are understood and monitored. Clear policy guidelines, addressing both permitted and prohibited employee behavior, are vital to risk detection and monitoring. Clear requirements for ensuring employees' knowledge of these guidelines are also essential to their success. In addition, reports of policy questions and violations need to be systematically recorded so that management, HR, and security personnel can approach case decisions with complete background information.

Analysis of these reports across individuals and departments can supply vital knowledge of problem areas beyond individual cases. Relationships in which HR, security, and management personnel collaborate as educators and consultants are vital to early detection and effective management of employees posing an insider risk. The need for clear policies,

complete personnel risk data, and close management-HR-security collaboration is rarely greater than when handling employee termination issues, whether voluntary or involuntary.

Screening and Hiring Practices

Several personnel screening and hiring practices pose a risk to USCIS systems and data.

USCIS does not have a consistent procedure for deciding whether to conduct a face-to-face interview prior to hiring an applicant being screened for government employment. There was an impression at USCIS headquarters that nearly 100% of those employees hired by managers are interviewed, but representatives in Burlington, Vermont told us otherwise. This gap between perception and reality (there is not a policy stating that this must be done) is a concern. USCIS should require interviews for all positions. The interviews need to be conducted by someone involved in the day-to-day supervision of the position to be filled.

If a personal issue (e.g., substance abuse, relatively large financial indebtedness) arises during Personnel Security's (PERSEC's) screening, PERSEC may issue a letter of advisement to the candidate and clear that person for hire. PERSEC is hesitant to share negative information about applicants with USCIS because of privacy concerns. Because of these concerns, a manager may not know that someone is coming into a position with a history of alcohol and/or drug abuse, financial indebtedness, etc. The privacy wall between PERSEC and field personnel concerned with hiring is troubling. It is difficult for PERSEC representatives to indicate their concerns about potential hires if they have risk factors that do not cross adjudication guidelines for disqualification.

Foreign Service National (FSN) employees, who work at U.S. embassies and consulates abroad, have access to USCIS critical systems and data in some cases. In order to be hired and granted access to any of those systems, FSNs are vetted by the U.S. Department of State. Although the access to USCIS systems must be approved by the chief security officer (CSO) and chief information officer (CIO) for DHS, USCIS has very little visibility into the screening process for FSNs.

Exit Procedures

Exit procedures typically detail the steps that must be taken when an employee retires, resigns or is fired, transferred, or put on a leave of absence. These procedures for USCIS have been recently developed and, in some cases, are still under development. USCIS expects to release more formalized procedures in the next 3 months, but there is not a common understanding of the proper procedures. It appears the responsibility for ensuring that employees and contractors are properly terminated rests solely with the manager or Contracting Officer's Technical Representative (COTR). It also appears different managers follow

different procedures to ensure that access is disabled and equipment is returned as employees and contractors leave USCIS. This gap may manifest itself in the inconsistent collection of badges, laptops, mobile devices, and other USCIS equipment, and improper disabling or termination of access.

Physical Security

Some insiders documented in the CERT Insider Threat Case database exploited physical security vulnerabilities. Some were able to gain access to organization facilities outside of normal working hours to steal controlled information or to exact revenge on the organization by sabotaging critical operations. Physical security can provide another layer of defense against terminated insiders who wish to regain physical access to attack. Just as with electronic security, however, former employees have been successful in working around their organization's physical security measures. It is important for organizations to manage physical security for full-time, part-time, and temporary employees, contractors, and contract laborers.

USCIS Physical Security has made significant progress protecting USCIS facilities and assets in the NCR since January 2008, when it stood up a new physical security program. Although physical security in the NCR is consistently directed and enforced by Physical Security, each field office sets its own policies and access controls. [redacted] Finally, issues concerning the security of applicants' physical case files should be considered as part of a USCIS risk management strategy by USCIS.

Controlling and Monitoring Proper Access Authorization

USCIS handles the physical security and access authorization of facilities differently depending on where the facility is located. The physical security of NCR facilities is handled by one group of USCIS personnel, but the physical security of field offices falls under the Field Security Division (FSD). In some cases, a physical security representative is not located in a field office at all. When this is the case, the responsibility falls on other management personnel who may not be equipped to handle these issues properly and report them in a timely manner. [redacted]

[redacted] In 10 cases documented in

the CERT Insider Threat Case database, the insider was able to commit a crime following termination because of failure to notify security, employees, and business partners of the termination. To control access to USCIS facilities, it is important for USCIS to compare current employees and contractors to the authorized access list in each facility's access control system. Disabling physical access to facilities when employees and contractors terminate is essential to protecting USCIS employees and facilities.

Security of Physical Case Files

At the Vermont Service Center, the assessment team observed physical case files of benefit applicants stacked in crates in the hallways. Case files are assumed to be secure once they are contained within a Service Center, but they could be physically altered or stolen by anyone with physical access to the facility. One interviewee stated that adjudicators typically have 50 to 100 files scattered around their offices or desks. Some are tracked and some may not be. Adjudicators conduct interviews with applicants in their offices and they may leave applicants unescorted in their offices with the case files when, for instance, making copies or attending to other USCIS business. According to the same interviewee, in one field office, naturalization certificates, passports, and credit card information have been found in garbage cans in the hallway. Thirteen insiders documented in the CERT database stole physical property belonging to their organization.

Business Processes

A variety of cases from the CERT Insider Threat Case database document insider attacks in which gaps in business processes provided a pathway for attack. Enforcing separation of duties and the principle of least privilege are proven methods for limiting authorized access by insiders. Ideally, organizations should include separation of duties in the design of key business processes and functions and enforce them via technical and non-technical means. Access control based on separation of duties and least privilege, in both the physical and virtual environment, is crucial to mitigating the risk of insider attack. These concepts alone will not eliminate the threat posed by insiders; they are, however, another layer in the defensive posture of an organization.

Because of the sensitive nature of the USCIS mission, some of its employees and contractors have been targets for recruitment for theft or unauthorized modification of USCIS data. Twenty-nine percent of the insiders documented in the CERT database were recruited by outsiders to commit their crimes. Most of these insiders committed their crimes for financial gain. Critical USCIS business processes should include technical controls to enforce separation of duties and dual control to reduce the risk of insider fraud. In addition, potential vulnerabilities surround the use of the ICE Password Issuance and Control System (PICS) for authorization for critical USCIS systems. Although PICS is outside the control of USCIS,

CERT recommends that USCIS explore the possibility of auditing and controlling authorizations in PICS for critical USCIS systems. Finally, account management issues related to critical systems should be considered.

Verification Information System

The Verification Information System (VIS) provides immigrant status information to both government agencies and private employers in order to verify benefit and employment eligibility. Because these functions require granting VIS access to parties external to USCIS, USCIS must issue accounts and require that those accounts be used properly. Twenty-four (6%) of the insiders documented in the CERT database were able to carry out their crimes because insiders shared account and password information, often to make their jobs easier and to increase productivity.

Modifications by VIS users to critical data are logged, [redacted]

CLAIMS 3-LAN

Currently, all denied benefits applications are reviewed by a supervisor; only a subset of approved applications are reviewed. A discrepancy arose during interviews: adjudicators said that supervisors stopped looking at all denials because they are too busy. Supervisors also receive a report of all adjudication decisions entered by an adjudicator for a form type that the adjudicator does not normally approve. When adjudicators are in training, which takes place for at least 6 months on a specific type of case, they are under 100% review. A quality assurance (QA) process is also in place. One part of QA involves a supervisor pulling 10 cases per month per adjudicator to review. The supervisor examines adjudicative decision, security, and procedural issues. In another aspect of the QA, other "sister" USCIS Service Centers review a random selection of cases. The primary purpose of QA is to identify the need for remedial training rather than deliberate fraud. Auditing every denied request indicates that the biggest risk to USCIS is to incorrectly deny a benefit to an applicant rather than to grant a benefit to someone who does not deserve it.

FDNS DS

[redacted]

[redacted]

[redacted]

Incident Response

Through case analysis, CERT has noted that procedures for responding to potential insider incidents present unique challenges; an incident response plan for insider incidents differs from a response plan for incidents caused by an external attacker. In addition, inadequate detection and response to security violations could embolden the insider, making the organization even more vulnerable to an insider crime. In fact, in 18 of the cases documented in the CERT Insider Threat Case database, the organization experienced repeat insider incidents of a similar nature. Insider incident management should leverage existing security policies and formal procedures for handling policy violations. Some of the cases from the CERT Insider Threat Case database illustrate insider attacks in which an organization's lack of incident response procedures limited its ability to manage its response effort, sometimes even resulting in multiple criminal acts by the same insider.

Furthermore, 81 of the insiders documented in the CERT Insider Threat Case database displayed concerning behaviors in the workplace prior to, or while carrying out, their criminal activities online. Supervisors and employees should be trained to recognize and respond to indicators of risk for violence, sabotage, fraud, theft and other malicious insider acts. Even if it is not possible to require nonsupervisors to report concerns, this training may increase the frequency of reporting and the deterrence of insider actions.

Incident Management

USCIS is a complex organization with many different components involved in detecting, tracking, investigating, and following up on employee misconduct. Organizations involved include the Office of Investigations within the OSI, Labor and Employee Relations (LER), HR, Computer Security Incident Response Team (CSIRT), PERSEC, Counterintelligence (CI), COTRs, OIT, DHS OIG, Physical Security, supervisors, and possibly data owners and ISSOs. Many different parties explained how they might be involved in one aspect of an incident, but no single department coordinates these activities or conducts a holistic risk analysis of individuals who have committed violations. This complex and widely distributed business process has resulted in a situation in which it is very difficult to obtain a complete picture of an individual's insider threat risk level. Consequently, any effort to coordinate a proactive

program for insider threat mitigation would have to cross significant bureaucratic boundaries within these myriad departments of USCIS.

Software Engineering

[redacted]

[redacted]

[redacted] Code Reviews

Some USCIS systems adhere to a formalized process of software engineering, using contractors with a specified level of process maturity (i.e., capability maturity model integration (CMMI) level 3), [redacted] There was even a documented case in which source code contained something inappropriate and was only discovered only after the code was turned over from one contractor to another.

Insiders inserted malicious code into an operational system in 33 cases documented in the CERT Insider Threat Case database, and into source code in 10 cases. These types of crimes can have serious results, enabling insiders to conceal their actions over an extended period of time. These actions have been used to create mechanisms for committing fraud without detection and to set up future IT sabotage attacks.

Code reviews can be very time-consuming, but most malicious insiders insert malicious code into production systems once they are stable and in the maintenance phase, when changes are less frequent and less substantial.

Information Technology

Account Management

Research has demonstrated that if an organization's computer accounts can be compromised, insiders have an opportunity to circumvent manual and automated control mechanisms intended to prevent insider attacks. Effective computer account and password management policies and practices are critical to impede an insider's ability to use the organization's systems for illicit purposes. In a variety of cases documented in the CERT Insider Threat Case database, insiders exploited password vulnerabilities, shared accounts, and backdoor accounts to carry out attacks. It is important for organizations to limit computer accounts to those that are absolutely necessary, using strict procedures and technical controls that facilitate attribution of all online activity associated with each account to an individual user. Furthermore, an organization's account and password management policies must be applied consistently across the enterprise to include contractors, subcontractors, and vendors who have access to the organization's information systems and/or networks.

In some areas, computer accounts are managed fairly well at USCIS. It is implementing Homeland Security Presidential Directive 12 (HSPD-12) for physical and electronic account management. In addition, most shared accounts are controlled and all actions performed using those accounts can be attributed to a single user. However, some account management lies outside the control of USCIS. This presents a high degree of risk. First of all, accounts and access for FSNs should be considered carefully by USCIS. Although FSNs must submit paperwork through proper channels, which requires authorization by the CSO and CIO of DHS, such paperwork was not submitted consistently prior to 2007. As a result, there may be active accounts for which there is little to no accounting for the creation of the account. [redacted] Although account naming conventions are dictated by DHS and the U.S. Department of State, USCIS could request a naming convention to differentiate between FSN and U.S. citizen federal employee accounts. In addition, USCIS should consistently track the authorization and creation of all USCIS accounts. To determine if un-

authorized or legacy accounts exist, USCIS should consider conducting an account audit with the assistance of U.S. Department of State personnel to validate all existing FSN accounts.

Second, access to some critical USCIS systems is controlled by the Password Issuance and Control System (PICS). The purpose of PICS is to facilitate the administration of usernames and passwords to certain ICE and USCIS information systems. One area of concern regarding PICS is that it is administered by ICE, and there are more than 2,000 Local PICS Officers (LPOs) across various components of DHS. These LPOs use PICS to grant authorized access to ICE and USCIS systems for the personnel at their respective site or agency, such as local sheriffs, petitioners, Customs and Border Patrol (CBP), Department of Justice (DOJ), Transportation Security Administration (TSA), Terrorism Task Force, and DHS OIG. Each LPO can grant access to any system controlled by PICS. In other words, LPOs throughout USCIS and ICE can grant access for *any* of their staff to *any* USCIS system. Furthermore, [redacted] Given the distributed nature of account administration, it is very difficult for USCIS data owners and OIT staff to manage authorization of user accounts to USCIS critical systems. Finally, the process for communicating changes in employee status and disabling accounts varies widely among individual field offices, Service Centers, and offices in the NCR. [redacted]

The application of account management practices under the control of USCIS is inconsistent. For example, disabling or terminating accounts for employees is not always completed in a timely manner upon the employee's change in status. This lack of consistency is made worse when decentralized LPOs across USCIS do not follow the same procedures. In other cases, employees are retaining access after a transfer when they should not, which requires the losing and gaining supervisors to notify proper account management personnel.

Access Control

An organization's lack of sufficient access control mechanisms was a common theme in many of the insider threat cases examined by CERT. Insiders have been able to exploit excessive privileges to gain access to systems and information they otherwise would not have been authorized to access. Additionally, insiders have been known to use remote access after termination to attack an organization's internal network. Organizations should ensure network monitoring and logging is enabled for external access. Monitoring of network activity is extremely important, especially in the period between employee resignation and termination.

Given the distributed nature of access authorization via PICS, ICE, and the U.S. Department of State, non-USCIS employees and contractors could be granted access to USCIS critical systems. It is possible that the non-USCIS employees and contractors, particularly those

granted access through the U.S. Department of State for access from embassies overseas, have not been through the rigorous pre-employment screening required of USCIS employees and contractors. USCIS should consider the risk these insiders pose to the protection of the critical USCIS data and systems, and implement protection mechanisms to limit the damage that these insiders might cause.

Other access control issues that should be considered by USCIS include unrestricted access to some critical systems by OIT staff, lack of consistent processes for managing employee access as they move from one department to the next within USCIS, ability to use personal computers for USCIS work, and lack of monitoring and controls for some critical system administration functions.

Protection of Controlled Information

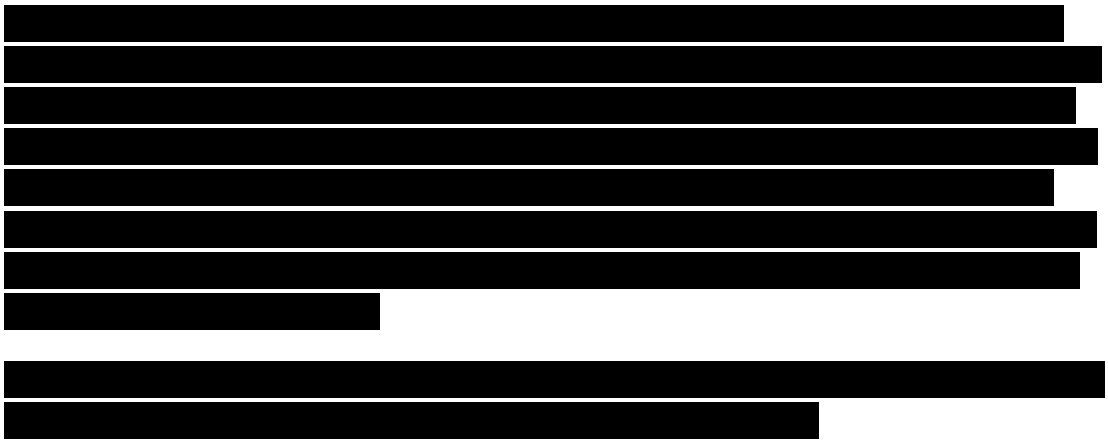
Protecting controlled information (i.e., information that is classified, sensitive but unclassified, or proprietary) is critical to mitigating the insider threat risk to organizations. A variety of insider threat cases studied by CERT revealed circumstances in which insiders carried out an attack through the unauthorized download of information to portable media or external storage devices. In some instances, malicious insiders used email to plan their attacks or to communicate sensitive information to competitors or conspirators. Organizations must ensure that employees understand policies regarding what constitutes acceptable use of company resources, including information assets, and enforce compliance through technical means. The unauthorized exfiltration of controlled information by malicious insiders can have devastating effects on an organization. Protecting controlled information (i.e., information that is classified, sensitive but unclassified, or proprietary) is critical to mitigating the insider threat risk to organizations.

USCIS has implemented network monitoring strategies that would detect large amounts of data downloaded or an anomalous increase in network traffic, either by total volume or type of traffic (e.g., by port or protocol). Though monitoring network traffic may help protect controlled information, [redacted]

Logging / Auditing / Monitoring

Insider threat research conducted by CERT has shown that logging, monitoring, and auditing employee online actions can provide an organization the opportunity to discover and investigate suspicious insider activity before more serious consequences ensue. Organizations should leverage automated processes and tools whenever possible. Moreover, network auditing should be ongoing and conducted randomly, and employees should be aware that certain activities are regularly monitored. This employee awareness can potentially serve as a deterrent to insider threats.

The prevention of insider attacks is the first line of defense. Nonetheless, effective backup and recovery processes need to be in place and operationally effective so that if a compromise occurs, business operations can be sustained with minimal interruption. In one case documented in the CERT Insider Threat Case database, an insider was able to magnify the impact of his attack by accessing and destroying backup media. Organizations need to consider the importance of backup and recovery processes and care must be taken that backups are performed regularly, protected, and tested to ensure business continuity in the event of damage to or loss of centralized data.



Technical Security Vulnerabilities

Proactively addressing known security vulnerabilities should be a priority for any organization seeking to mitigate the risk of insider threats as well as external threats. Case studies have shown that malicious insiders, following termination, will sometimes exploit known technical security vulnerabilities that they know have not been patched to obtain system access and carry out an attack. Organizations should have a process to ensure that operating systems and other software have been hardened or patched in a timely manner when possible. Failure to address known vulnerabilities provides an insider ample opportunity and pathways for attack, making it more difficult for an organization to protect itself.

There is a primary concern in this area at USCIS. USCIS should consider the frequency with which it scans its systems for technical security vulnerabilities. [redacted]

There is also another concern in this area at USCIS. [redacted]

Configuration Management

Effective configuration management helps ensure the accuracy, integrity, and documentation of all computer and network system configurations. A wide variety of cases in the CERT Insider Threat Case database document insiders who relied heavily on the misconfiguration of systems. They highlight the need for stronger, more effective implementation of automated configuration management controls. Organizations should also consider consistent definition and enforcement of approved configurations. Changes or deviations from the approved configuration baseline should be logged so they can be investigated for potential malicious intent. Configuration management also applies to software, source code, and application files. Organizations that do not enforce configuration management across the enterprise are opening vulnerabilities for exploit by technical insiders with sufficient motivation and a lack of ethics.

The OIT has a configuration management policy that provides baseline software configurations for USCIS desktops and laptops. The OIT scans for incorrect, outdated, or un-patched versions of software on the approved software list. The OIT keeps track of different baselines for different contracts. Despite tracking and a rigorous configuration management policy, [redacted] Rogue software or malware is often discovered through a deliberate manual scan, rather than through an automated process. To make this task more difficult, USCIS employees with seniority or influence have been able to use local administrator privileges to install software for the sake of convenience. Concerns regarding configuration management surround the difficulty for the OIT to adequately prevent, detect, and respond to rogue software or malware using its current procedures. We suggest some considerations for lev-

eraging existing deployments and modifying incident response practices to increase effectiveness.

Recommendations

The following 18 recommendations present actionable steps that will enable USCIS to improve its posture against malicious insider threats. These high-level strategies should be planned and implemented with the assistance of the many diverse departments within USCIS. Appendixes contain more specific recommendations that pertain to a particular department (e.g., OIT and HR). The appendixes also list the relevant parties to assist USCIS in reviewing each issue more granularly and to decide whether USCIS has resources to implement a particular recommendation.

Recommendation #1: Institute an enterprise risk management plan

USCIS must ensure that the entire organization is risk aware and implement a formal risk management process to address risk consistently and continually across the enterprise. There does not appear to be a consistent understanding of the broad spectrum of risks facing USCIS. The OIT performs risk management for IT, and Financial Management performs risk management for financial matters, but no one was aware of any enterprise-wide efforts. In addition, each field office and service center appears to operate fairly independently. It is important for those organizations to work together to identify, prioritize, and address risk. Ongoing communication between all components of USCIS will help ensure that new threats, attack vectors, and countermeasures are communicated and handled effectively by all.

Recommendation #2: Incorporate insider threat risk mitigation strategies into the Transformation effort

Transformation is a large business process reengineering effort in USCIS primarily focused on improved customer service, workflow automation, fraud detection, and national security issues. Risk management is within the scope of Transformation, but only as it pertains to automated risk scoring of applicants and to workflow management to optimize adjudicator workload. USCIS should incorporate comprehensive insider threat risk mitigation requirements into the Transformation effort.

Recommendation #3: Centralize records of misconduct and violations to better enable a coordinated response to insider threats

USCIS is a complex organization with many different components involved in detecting, tracking, investigating, and following up on employee misconduct. This complex and widely distributed business process has resulted in a situation in which it is very difficult to obtain a complete picture of an individual's insider threat risk level. USCIS should create a central repository of employee and contractor misconduct, security violations, Significant Incident Reports (SIRs), and other suspicious activity reports so repeat offenders can be easily identi-

fied, because repeat offenses could indicate an insider of higher risk. Given the difficulty of creating such a repository, the assessment team recommends that, at the very least, USCIS establish a mechanism by which disparate databases or departments (e.g., HR, IT, and Legal) can communicate with each other to identify any insider risks.

Recommendation #4: [redacted]

Recommendation #5: Consider separation of duties for critical business processes and their related information systems

USCIS currently reviews every denied request for benefits, but reviews only a subset of the approved requests. These quality assurance processes indicate that USCIS emphasizes customer service and adjudication process improvement over the possible detection of an improper granting of a benefit, which several employees identified as the greatest risk to USCIS. If USCIS enforced a separation of duties, where an adjudicator's decision is not final until it is reviewed by a supervisor, it would at least partially mitigate the risk of an adjudicator granting benefits illegally. Critical USCIS business processes must include technical controls to enforce separation of duties and dual control to reduce the risk of insider fraud.

Recommendation #6: Conduct audit of PICS and FSN accounts for USCIS systems

The systems and processes used to grant USCIS employees and contractors access to USCIS systems are clear. PICS, on the other hand, is administered by ICE, which delegates the authority to create accounts to LPOs, who may be in an agency altogether outside of USCIS. FSNs are vetted by and granted access to the networks of the U.S. Department of State, which has access to USCIS systems. USCIS should conduct an audit or review on how non-USCIS employees are granted access to USCIS systems.

Recommendation #7: Employ consistent physical security policies for field offices and service centers, including the physical case files

USCIS handles the physical security and access authorization of facilities differently depending on where the facility is located. In some cases, a physical security representative is not located in a field office at all. When this is the case, the responsibility falls on other management personnel who may not handle these issues in a consistent manner. Also, USCIS

stores physical files for benefit applicants in the Vermont Service Center with no physical protection beyond the exterior building and guard controls. USCIS should evaluate current physical access procedures to determine if they adequately address risk and if they are enforced consistently across the enterprise.

Recommendation #8: Consistently enforce exit procedures

Exit procedures typically detail the steps that must be taken when an employee retires, resigns or is fired, transferred, or put on a leave of absence. These procedures for USCIS have been recently developed and, in some cases, are still under development. USCIS expects to release more formalized procedures in the next 3 months, but there is not a common understanding of the proper procedures. It appears the responsibility for ensuring that employees and contractors are properly terminated rests solely with the manager and COTR. It also appears that different managers follow different procedures to ensure that access is disabled and equipment is returned as employees and contractors leave USCIS. This gap may manifest itself in the inconsistent collection of badges, laptops, mobile devices, and other USCIS equipment, and improper disabling or termination of access. USCIS should adopt an enterprise-wide exit procedure to ensure consistent termination of all employees and contractors.

Recommendation #9: Examine HR screening procedures for high-risk positions and FSNs

Changes should be made to the USCIS hiring processes for select, high-risk positions. For example, USCIS should consider additional screening for adjudicators. USCIS should be more involved in deciding who is granted authorized access because of the sensitive nature of the systems and data that USCIS manages.

Recommendation #10: Ensure that physical and computer access is terminated in a timely fashion

USCIS should automate the revocation of employee and contractor physical access when a termination occurs. The termination checklist should include a notification to Physical Security so physical access can be disabled in a timely manner. USCIS should also review account management procedures to ensure that the steps taken to remove or alter account access are complete, understood by all relevant parties, and consistently followed.

Recommendation #11: Enforce a requirement for individual accounts on critical systems

In some cases, USCIS is aware of account sharing taking place at third party employers who use USCIS systems to verify immigration status. To consistently identify malicious insider activity, all actions must be attributable to one and only one individual. USCIS should consider increasing the consequences for infractions, and possibly implement stronger authentication to make sharing of accounts more difficult.

Recommendation #12: [redacted]

Recommendation #13: Reduce the number of privileged accounts for critical data systems

Some data systems, including FDNS DS, have a high number of privileged users. Many of these users do not need the escalated access to complete their job responsibilities. USCIS should audit the privileged user accounts and reduce those accounts commensurate with job responsibilities.

Recommendation #14: [redacted]

Recommendation #15: Implement procedural and technical controls to prevent source code under development from being released without appropriate review

USCIS should consider implementing procedural and technical controls to enforce separation of duties between software engineers and the system administrators responsible for

releasing changes into production systems. USCIS should consider identifying high-risk, critical software modules that could be used to carry out illicit activity. In addition, formal software development practices should be followed, [redacted]

Recommendation #16: [redacted]

Recommendation #17: [redacted]

Recommendation #18: Periodic security refresher training should be regularly conducted and required for all employees

USCIS should reinforce security practices and procedures for all employees, especially those assigned to security roles, through Information Assurance refresher training. Though annual refresher training is mandated, it has not been completed in a timely manner for all roles. USCIS should ensure that this training is adapted to specific roles, regularly conducted and tracked, and consequences imposed for those who have not completed the training.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the USCIS Deputy Director. We have included a copy of the comments, in its entirety, in appendix I.

USCIS concurred with our findings and recommendations and indicated that the report will be of great assistance as they seek to further strengthen internal controls in this area. In the written comments, USCIS did not provide information on how it intends to address our recommendations. Therefore, we consider our recommendations unresolved and open pending our review of USCIS' corrective action plans.

Appendixes

The following pages contain appendixes A through G that contain a complete, detailed list of findings from the assessment.

The appendixes are organized into the following sections:

- Appendix A: Organizational
- Appendix B: Human Resources
- Appendix C: Physical Security
- Appendix D: Business Process
- Appendix E: Incident Response
- Appendix F: Software Engineering
- Appendix G: Information Technology
- Appendix H: Acronyms
- Appendix I: Management Comments to the Draft Report
- Appendix J: Contributors to this Report
- Appendix K: Report Distribution

Each section in appendixes A – G contains a brief introduction, summary of the findings for that area, and a table listing detailed findings. The tables are structured as follows:

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures

Each row represents a unique area of concern. **Responsible Personnel** lists the groups within USCIS that would be responsible for implementing suggested countermeasures for that area. **Policy and/or Security Measure** lists information related to that area of concern specific to USCIS obtained in interviews. If that column was intentionally left blank, it indicates that no evidence was provided for the existence of a policy and/or security measure. **Policy or Practice Gaps** describes gaps identified by interviewees or gaps noted by CERT staff. Finally, **Suggested Countermeasures** describes countermeasures that USCIS could implement to address a particular vulnerability.

It is important to note that all suggested countermeasures must be considered in the context of a broader risk analysis. It is not practical for most organizations to implement 100% protection against every threat to every organizational resource. Therefore, it is important to adequately protect critical information and other resources and not direct significant effort toward protecting relatively unimportant data and resources. A realistic and achievable

security goal is to protect those assets deemed critical to the organization's mission from both external and internal threats.

Risk is the combination of threat, vulnerability, and mission impact. Some countermeasures in this report are intended to help USCIS recognize and understand the insider threat. Others focus on closing gaps that leave USCIS more vulnerable to insider attack. Mission impact cannot be adequately assessed by CERT through this exercise because it will vary depending on the criticality of systems and information.

The results of this insider threat vulnerability assessment should be used to develop or refine the organization's overall strategy for securing its networked systems, striking the proper balance between countering the threat and accomplishing the organizational mission.

Many of the findings in this report include the relative frequency of the issue raised in the CERT Insider Threat Case database. At the time this report was written, there were 386 cases of malicious insider activity against which the suggested countermeasure percentage is calculated. So, if a particular activity was seen in 38 of our cases, we may indicate that it was seen in 10% of the cases in the Insider Threat Case database.

Appendix A: Organizational

Risk Management / Communication / Security Process Improvement

USCIS is in a difficult position. Part of its mission is to provide customer service to those seeking immigration and citizenship benefits from the U.S. Government. However, it is challenging to optimize business processes for customer service while at the same time implementing protective measures to counter the risk posed by granting those very benefits. Many USCIS employees interviewed for this assessment identified the organization's primary risk as allowing the next terrorist to live and work legally in the United States. They desire help in identifying and implementing internal controls to counter that risk. Some of the interviewees, however—even some of the ISSOs and data owners—focused on leakage of PII as their primary concern. After delving into the matter with the assessment team, they came to understand the risk posed by exposure or misuse of critical data as the greatest risk faced by USCIS, primarily because such a security breach could result in allowing a terrorist into the country.

A critical issue for USCIS is ensuring the entire organization is risk aware, and implementing a formal risk management process to address risk consistently and continually across the enterprise. There does not appear to be a consistent understanding of the broad spectrum of risks facing USCIS. The assessment team was told there is no enterprise-wide risk management program at USCIS. OIT performs risk management for IT and Financial Management performs risk management for financial matters, but no one was aware of any enterprise-wide efforts. In addition, each field office and service center appears to operate fairly independently. It is important for those organizations to work together to identify, prioritize, and address risk. Ongoing communication between all components of USCIS will help ensure that new threats, attack vectors, and countermeasures are communicated and handled effectively by all.

In addition, USCIS employees and contractors hold the keys to one of the world's most coveted kingdoms—U.S. citizenship. This makes employees and contractors attractive targets for recruitment. Because of the sensitive nature of USCIS mission, some of its employees and contractors

have been targets for recruitment for theft or unauthorized modification of USCIS data. All employees should be aware of the consequences of participating in fraud against USCIS. They should also be instructed on how to report solicitations made to commit fraud.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Enterprise Risk Management	**USCIS Leadership** **ISSOs** **Data Owners** **Information Technology**	Individual organizations within USCIS do risk management related to their particular domain. For instance, IT does risk management from an IT perspective, and the Financial Management does financial risk management.	USCIS personnel stated there is no enterprise risk management process for analyzing the organization's overall risk.	We suggest that USCIS institute an enterprise risk management program. Without a common vision for risk management, the ISSOs and all organizations within USCIS cannot effectively understand the risk environment and work together to effectively mitigate risk.
		In interviews, some USCIS staff, including some ISSOs, data owners, and OIT staff, seemed to view loss of PII as the most important insider threat risk. All of the assessment questions were answered in the context of loss of PII.	When we asked specifically what they see as the biggest insider threat risk, everyone seemed to agree it is creation of real citizenship documents for people who should not have them. In fact, interviewees at the Vermont Service Center categorized the functions characterized by the highest risk as follows: 1) Unlawful alien in the United States granted non-immigrant status 2) Someone with non-immigrant status granted permanent residency, which means he or she can live and work indefinitely in the United States	Again, an enterprise risk management program will ensure that everyone across USCIS is working together to mitigate the highest priority risks. There are regulations and laws surrounding protection of PII, but focusing primarily on that issue can lead to a false sense of security if other more important risk areas are given less attention.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			and also can petition for relatives	
		The Vermont Service Center is implementing separation of duties for performing functions #1 and #2 above (granting non-immigrant status and moving someone from non-immigrant status to permanent residency) so that one USCIS adjudicator alone cannot take an applicant from unlawful to permanent resident. These two functions will be performed at different physical locations 29 miles apart.	The Vermont Service Center has not had an adjudicator who performed both functions #1 and #2 for the same applicant.	This decision demonstrates that leadership at the Vermont Service Center recognizes the significant risk of creating legal citizenship documents for illegal aliens and is taking steps to mitigate that risk. However, our insider threat assessment has uncovered other issues that could be addressed to mitigate that risk. Again, a formal risk analysis would enable USCIS to thoroughly examine the issues and prioritize countermeasures using a formal process. For example, an alternative to the physical move could be to implement an audit mechanism to look for adjudicators who performed both functions #1 and #2 for the same applicant.
Enterprise-Wide Communication	**USCIS Leadership**	No evidence provided	There is no consistency of controls from one service center to the next. We were told they each operate fairly independently.	USCIS would benefit from ongoing communications about risk-based issues between the service centers. For instance, communications concerning problems, effective countermeasures, modifications to

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				business processes, or ideas for countering increased risk could lead to an improved risk posture for the entire USCIS enterprise.
Continual Security Process Improvement	**USCIS Leadership** **ISSOs** **Data Owners** **Information Technology**	The USCIS Convictions Task Force is an excellent forum for analyzing past criminal cases and determining measures that should be instituted to prevent similar crimes in the future.	There is no process for following up on a case after the Office of Special Investigation (OSI) finishes an investigation. The Convictions Task Force is the only process we found for formal tracking, analysis, and process improvement based on actual incidents. The assessment team asked various groups if there is any follow up to incidents, for instance implementing automated scripts or controls to detect the same incident in the future. The team could not find a single person who knows of such an activity. Many examples of employee misconduct cited to the assessment team could easily have been detected or even prevented via automated controls. In addition, there is no mechanism for communicating issues outside of a	In nearly 25%(91) of the cases in the CERT Insider Threat Case database, the insider was able to carry out the crime because of inadequate auditing of critical processes; in 28 of these cases, it was because of inadequate auditing of irregular processes. In 29 of the cases, the organization had repeated incidents of a similar nature. Automated scripts are an excellent mechanism for detecting suspicious transactions as well as honest mistakes. USCIS should consider a formal process for analysis of the OSI's findings and the development of automated checks implemented nationally.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			given service center.	
USCIS Employees are Potential Targets for Recruitment	**Human Resources** **Physical Security**	No evidence provided	Some USCIS employees interviewed have received a request for assistance from a friend, relative, or stranger seeking to promote a case for some form of applicant. One adjudicator said he does not tell others who he works for. However, the distinctive green parking sticker on his car could, in a small town like Burlington, VT, reveal the identity of his employer. USCIS personnel are therefore unusually vulnerable to solicitation by outsiders.	Twenty-nine percent of the insiders in the CERT Insider Threat Case database were recruited by outsiders to commit their crimes. USCIS should consider increasing the security awareness training provided to USCIS employees and contractors. The training should be continuous, including portions intended to raise awareness of the potential target that USCIS employees present. All employees should be aware of the consequences of participating in fraud against USCIS as well as how to report solicitations made to commit fraud.
Transformation	**USCIS Leadership** **Data Owners** **Information Technology** **Human Resources**	Transformation is a large business process reengineering effort in USCIS that is primarily focused on improved customer service and fraud detection. For example, the assessment team was told that Transformation will automatically validate data in CLAIMS against other external systems (e.g., ICE and FBI), and that security requirements and controls	Transformation was mentioned in most interviews for this assessment. It appears that USCIS is relying heavily upon Transformation to correct many of the problems resulting from legacy systems. However, it is unclear whether internal personnel security and information security concerns will be included in this program.	This reliance on a single effort makes the effectiveness of this effort very important. USCIS should consider the Transformation project from an enterprise-wide perspective. It is important for it to use a formal requirements gathering process in order to effectively mitigate both internal and external threats.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		have been identified by current C3LAN data owners.	Reading the Transformation requirements documentation, it is not clear that insiders are considered in the security requirements for prevention and detection of fraud or national security in USCIS systems.	Personnel security should be included, as well as information security, to ensure that the appropriate internal controls are in place to reduce the risk posed by malicious insiders.

Training and Awareness

It is essential that security awareness training be consistently provided to all employees to ensure that security policies and practices are institutionalized throughout an organization. Many times, coworkers and supervisors are the first people to observe concerning behavior exhibited by malicious insiders. Failure by coworkers or others in an organization to report concerning behavior was a primary reason insiders in the CERT Insider Threat Case database were able to set up or carry out their attacks.

USCIS should continue to provide security awareness training to all employees and contractors across the globe. This training should be consistently applied to each site, with a consistent message of security of USCIS people, systems, and data. It is imperative that all USCIS employees be responsible for achieving the mission of USCIS and protecting the critical assets to the highest extent possible.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Training or Skills Required of Those in Appointed Security Roles	**USCIS Leadership**	USCIS has a training process through an information systems security manager (ISSM). USCIS relies heavily on contractors to provide adequately trained staff.	Many ISSOs are not well versed in security. ISSOs are currently in an education process, but ISSOs are typically not security watchdogs.	ISSOs must have proper training in order to keep up with the ever-changing information security environment and to be able to deal with the myriad technologies and tools available to them. Appropriate budget should be allocated for ISSO training, including vendor-specific training (e.g., McAfee and Cisco) and industry-specific training (e.g., SANS).

Appendix B: Human Resources

Employee Issues

An organization's approach to reducing insider threat should focus on proactively managing employee issues and behaviors. This concept begins with effective hiring processes and background investigations to screen potential candidates. Organizations should also train supervisors to monitor and respond to behaviors of concern by current employees. Some cases from the CERT Insider Threat Case database revealed that suspicious activity was noticed in the workplace but not acted upon. Organizations should establish a well-organized and professional method for handling negative employment issues and ensuring that human resource policy violations are addressed.

Organizational issues related to functions shared by HR and security personnel are at the heart of insider risk management. Employee screening and selection is vital to preventing candidates with known behavioral risk factors from entering the organization; or, if they do, ensuring that these risks are understood and monitored. Clear policy guidelines addressing both permitted and prohibited employee behavior are vital to risk detection and monitoring, and clear requirements for ensuring employees' knowledge of these guidelines are essential to their success. In addition, reports of policy questions and violations need to be systematically recorded so that management, HR, and security personnel can approach case decisions with complete background information.

Analysis of these reports across individuals and departments can supply vital knowledge of problem areas beyond individual cases. Relationships in which HR, security, and management personnel collaborate as educators and consultants are vital to early detection and effective management of employees posing an insider risk. The need for clear policies, complete personnel risk data, and close management-HR-security collaboration is rarely greater than when handling employee termination issues, whether voluntary or involuntary.

CERT suggests enhancements to the USCIS hiring and termination processes. For example, USCIS should consider additional screening for high-risk positions, such as adjudicators. USCIS should also consider becoming more involved in vetting Foreign Service Nationals (FSN) prior to grant-

ing them access to USCIS critical systems and data. Finally, USCIS should consider adopting an enterprise-wide exit procedure to ensure consistent termination of all employees and contractors.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Pre-Employment Screening	**USCIS Leadership** **Human Resources**	No evidence provided	The employee screening process lacks any form of psychological screening for a range of positions, including adjudicators.	Five percent (18) of the insiders in the CERT database had possible psychological issues. USCIS should consider including psychological testing as part of the new hire process for select positions, including adjudicators. Given the significant social pressures on adjudicators and the relative lack of monitoring for insider risk, it seems important to improve this aspect of screening.
	Human Resources	Applicants are assigned a rating by HR; the rating is used to rank applicants.	There is currently no audit log that would capture instances in which someone in HR changed a rating to enable someone to get hired more easily.	USCIS should consider implementing an audit log to track the candidate ratings and alert when candidate ratings are changed by someone in HR.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
	USCIS Leadership **Human Resources**	If a personal issue (e.g., substance abuse, relatively large financial indebtedness) arises during Personnel Security's (PERSEC's) screening, PERSEC may issue a letter of advisement to the candidate and clear that person for hire. PERSERC is hesitant to share negative information about applicants with USCIS because of privacy concerns. Because of these concerns, a manager may not know that someone is coming into a position with a history of alcohol and/or drug abuse, financial indebtedness, etc.	The privacy wall between PERSEC and field personnel concerned with hiring is troubling. It is difficult for PERSEC representatives to indicate their concerns about potential hires who have risk factors that do not cross adjudication guidelines for disqualification.	USCIS should consider additional screening for adjudicators. USCIS should be more involved in deciding who is granted authorized access because of the sensitive nature of the systems and data that USCIS manages.
	USCIS Leadership **Human Resources**	Each field office determines whether or not to meet an applicant face-to-face before hiring.	There was an impression at headquarters that nearly 100% of those hired by managers are interviewed, but representatives in Burlington, Vermont told us otherwise. This gap between perception (there is not a policy stating this must be done) and reality is of concern. There have been known instances in which applicants were only screened	USCIS should require interviews for all positions. The interviews need to be conducted by someone involved in the day-to-day supervision of the position to be filled.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			on paper or over the phone before being hired. Standard operating procedures are not followed at all field offices.	
	USCIS Leadership **Human Resources**	PERSEC vets federal employees and contractors (with a minimum background investigation).	USCIS relies on the U.S. Department of State to vet foreign national employees who work at embassies or consulates abroad. FSNs, in some instances, are granted accounts on USCIS information systems. If FSNs need access to DHS systems (including USCIS) currently, this access must be approved by the CSO and CIO for DHS. This practice was not always followed consistently in the past, so there may be FSNs who were granted access without all the current vetting and approvals.	USCIS should consider becoming more involved in vetting of FSNs prior to granting them access to USCIS systems. In addition, USCIS should audit current FSNs with access to USCIS systems and ensure that appropriate vetting was performed.
Candidate Certification Verification	**Human Resources**	No evidence provided	USCIS does not have a standard procedure for verifying the certifications of job applicants.	USCIS should consider implementing a step in the new-hire process to verify certifications of all candidates. A few insiders documented in the CERT Insider Threat Case database were able

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				to obtain positions in organizations by providing falsified certifications.
Employee and Contractor Termination	**USCIS Leadership** **Human Resources**	Exit procedures are recently developed and, in some cases, still under development (i.e., formal exit procedures are expected to be released in 3 months).	This gap may manifest itself in the inconsistent collection of badges, laptops, mobile devices, and other USCIS equipment.	USCIS should consider adopting an enterprise-wide exit procedure to ensure consistent termination of all employees and contractors. It appears the responsibility for ensuring that employees and contractors are terminated rests solely with the manager. It also appears different managers follow different procedures to ensure that access is disabled and equipment is returned as employees and contractors leave USCIS.
Employee and Contractor Mandatory Drug Testing	**Human Resources**	All federal positions are subject to drug testing, but only for new hires.	According to a USCIS Convictions Task Force investigation case call, contractor positions do not require drug testing.	Fifteen insiders documented in the CERT Insider Threat Case database exhibited substance abuse. USCIS should consider implementing mandatory post-hire drug testing for all employees and contractors.

Appendix C: Physical Security

Field offices / Access Following Termination / Security of Physical Case Files

Some insiders documented in the CERT Insider Threat Case database exploited physical security vulnerabilities. Some were able to gain access to organization facilities outside of normal working hours to steal controlled information or to exact revenge on the organization by sabotaging critical operations. Physical security can also provide another layer of defense against terminated insiders who wish to regain physical access to attack. Just as with electronic security, however, former employees have been successful in working around their organization's physical security measures. It is important for organizations to manage physical security for full-time, part-time, and temporary employees, contractors, and contract laborers.

USCIS Physical Security has made significant progress protecting USCIS facilities and assets in the national capital region (NCR) since January 2008, when it stood up a new physical security program. Although physical security in the NCR is consistently directed and enforced by Physical Security, each field office sets its own policies and access controls. In addition, gaps in termination procedures have resulted in ongoing physical access following termination. Finally, issues concerning the security of physical case files should be considered as part of a USCIS risk management strategy.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Physical Security of Field Offices	**USCIS Leadership** **Physical Security**	USCIS is in the process of putting a new access control system in place for the NCR. Before it does, it will disable access for anyone who has not used physical access in more	Each USCIS facility has its own policies and access controls systems. Some field offices within USCIS have access control systems; others do not. Not all offices in the field have electronic	Forty of the insiders documented in the CERT database took advantage of inadequate physical security to carry out their crimes. Electronic access controls provide

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		than 12 months, as well as anyone no longer employed by USCIS. It also plans on examining all accounts that have not used physical access in more than 30 days. Security of field offices falls under the Field Security Division (FSD). The Office of Security and Integrity (OSI) recently developed an inspection workbook and is field testing it with FSD. USCIS Field Security Division is planning to put a security representative in every field office. It expects two to three times more reports of violations once it has a representative in every location.	access controls – some only have locks and keys. Not every USCIS site has a physical security representative. Where no representative is present, this responsibility falls on other management personnel who may not be equipped to handle these issues properly and report them in a timely manner. Some managers track who accesses what when and others do not. According to Physical Security in Vermont, only 20% of violations are being reported to security.	logs that could be useful in investigations of illicit activity outside of normal working hours. USCIS should consider developing enterprise-wide physical security procedures, roll those out to each field office, and require a physical security representative at each site to ensure consistent enforcement of the policies. USCIS should consider prohibiting each field office from developing site-specific policies and removing enforcement control from each site.
Physical Access Following Termination	**Human Resources** **Physical Security**	No evidence provided	[redacted]	In 10 cases documented in the CERT Insider Threat Case database, the insider was able to attack following termination due to failure to notify security, employees and business partners of the termination. To control access to USCIS facilities, it is important for USCIS to compare current employees and contractors to the authorized access list

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			[redacted]	in each facility's access control system. Disabling physical access to facilities when employees and contractors terminate is essential to protecting USCIS employees and facilities. USCIS should consider automating the revocation of employee and contractor physical access when a termination occurs. The termination checklist should include a notification to physical security so physical access can be disabled.
No Two-Person Control	**USCIS Leadership** **Physical Security**	No evidence provided	[redacted]	[redacted]
		No evidence provided	Security guards at site locations have, on occasion, ignored door-propped-open alarms because theft has traditionally been a very small problem at	Consider consistent enforcement and investigation of USCIS physical security incidents. All alerts should be investigated and

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			USCIS.	documented; if the alert is deemed unnecessary then it should be discontinued. All security violations should be tracked in a central repository so a complete history for each individual is available.
After-Hours Access	**Physical Security**	Authorized Access	Most access is 24 hours a day, 7days a week – [redacted]	Twenty-nine of the insiders documented in the CERT database used physical access outside of normal working hours to attack. USCIS should consider implementing an access control system that grants access commensurate with the position an employee or contractor fills. If a position does not require access outside of normal working hours, the access control system should prohibit such access and log unsuccessful access attempts.
Security of Physical Case Files	**Physical Security**	Protection of USCIS Case File Data	Physical files were observed in crates stacked in the hallways in the Vermont Service Center. According to an interview at the Service Center, anyone could walk out with a "crate full" of files after hours, especially if you are a teleworker.	USCIS assumes its case file data is secure because its employees and contractors have a clearance or have had a background check. It is important to note that 49 insiders documented in the CERT database violated need-to-know

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			Case files are assumed to be secure once they are contained within a Service Center, but they could be physically altered or stolen by anyone with physical access to the facility. One interviewee stated that adjudicators typically have 50 to 100 files scattered around their office or desk. Some are tracked and some may not be. Adjudicators conduct interviews with applicants in their offices and they might leave applicants unescorted in their offices with the case files when, for instance, making copies or attending to other USCIS business. According to the same interviewee, in one field office, naturalization certificates, passports, and credit card information has been found in garbage cans in the hallway. Adjudicators pick up their cases in an envelope in their mailbox. During the site visit, the assessment team observed the mailroom at the Vermont Service Center unattended between	policies in the commission of their crimes. Therefore, relying on clearances alone can be very dangerous. Thirteen insiders documented in the CERT database stole physical property belonging to the organization. CERT suggests USCIS consider the consequences of theft or unauthorized access to physical case files and make a risk-based decision regarding potential policy and procedure changes. There are standard policies and procedures for handling sensitive information, but a strong educational campaign is needed to ensure the protection of data.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			shifts (approximately 3 p.m.). When adjudicators finish with a file, they return it to a drop-off spot. The assessment team observed those spots, which are in the open and unattended. Adjudicators may keep cases overnight and usually return them within 1 week.	
Teleworkers at Service Centers	**USCIS Leadership** **Physical Security**	One hundred eighty-nine people at the Vermont Service Center are authorized to work from home. These employees pick up files at the Vermont Service Center and take them home. They work 2 days per week in the Service Center and 3 days per week at home. USCIS pays an unannounced visit to all homes to inventory the employees' files at least quarterly. These employees must have a locked facility in their home and must always have the ability to return the files to the Service Center within 4 hours.	The control of USCIS data when it leaves the Vermont Service Center is difficult to enforce. Employees must have appropriate storage facilities, but they could easily copy USCIS data and share it with unauthorized individuals.	Twenty-nine percent of the insiders documented in the CERT database were recruited by outsiders to commit their crime. Most of these insiders committed the crime for financial gain. It is important that USCIS recognize the potential for recruitment, and the lack of control exercised over sensitive data at adjudicators' residences.

Appendix D: Business Processes

Technical Controls / Authorization via PICS / Account Management

A variety of cases from the CERT Insider Threat Case database document insider attacks where gaps in business processes provided a pathway for attack. Enforcing separation of duties and the principle of least privilege are proven methods for limiting authorized access by insiders. Ideally, organizations should include separation of duties in the design of key business processes and functions and enforce them via technical and nontechnical means. Access control based on separation of duties and least privilege, in both the physical and virtual environments, is crucial to mitigating the risk of insider attack. These concepts alone will not eliminate the threat posed by insiders; they are, however, another layer in the defensive posture of an organization.

Because of the sensitive nature of the USCIS mission, some of its employees and contractors are targets for recruitment for theft or unauthorized modification of USCIS data. Twenty-nine percent of the insiders documented in the CERT database were recruited by outsiders to commit their crime. Most of these insiders committed the crime for financial gain. Critical USCIS business processes should include technical controls to enforce separation of duties and dual control to reduce the risk of insider fraud. In addition, potential vulnerabilities surround the use of the ICE PICS system for authorization for critical USCIS systems. Although PICS is outside the control of USCIS, CERT recommends that USCIS explore the possibility of auditing and controlling authorizations in PICS for critical USCIS systems. Finally, account management issues related to critical systems should be considered.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Authorization for USCIS Critical Systems through PICS	**Data Owners** **Information Technology**	Several critical USCIS systems are tied to PICS for authentication, which is administrated by the ICE. PICS logs account creations, when the accounts were created, what roles applied to the accounts, etc.	PICS permits users outside of USCIS to authorize users for any USCIS application tied to PICS. Two thousand local PICS officers (LPOs) in the ICE and USCIS can create new accounts in PICS for employees located at their sites.	USCIS should consider implementing an authorization process and system that enables it to control who is granted access to USCIS systems and data.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			LPOs control access for sheriffs, petitioners, CBP, DOJ, TSA, DHS OIG, Terrorism Task Force, and others. Accounts are based on personnel record, so LPOs cannot create accounts for anyone who is not an employee at their site. However, PICS administrators can create accounts for anyone working at their site for any system tied to PICS. [redacted]	CERT suggests that USCIS validate current PICS accounts and roles against current employee lists. Ten percent (37) of the insiders documented in the CERT database had excessive privileges which enabled them to attack. In addition, [redacted] because "privilege creep" enabled a few (six) of the insiders documented in the CERT database to carry out their crimes.

Verification Information System (VIS)

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Sharing VIS Accounts	**Data Owners** **Information Technology**	No evidence provided	VIS administrators in external companies or agencies have been caught letting multiple employees use the same VIS account, but USCIS has no ability to take any action. The accounts enable employees to validate PII and citizenship information.	Twenty four (6 percent) of the insiders documented in the CERT database were able to carry out their crimes because insiders shared account and password information, often to make their jobs easier and to increase productivity. USCIS should consider increasing the consequences for infractions, and possibly implement stronger authentication to make sharing accounts more difficult.
Logging, Auditing, and Alerting in VIS	**Data Owners** **Information Technology**	Modifications by VIS users to critical data are logged.	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]

Computer Linked Application Information Management System (CLAIMS) 3-LAN

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Self Selection of Adjudication Cases	**ISSOs** **Data Owners**	Adjudicators can self-select cases (according to an interview concerning an internal incident that occurred at the USCIS and interviews with data owners at the Vermont Service Center).	Within the Service Centers, adjudicators have virtually unlimited access to applicant files—there are no need-to-know limitations or controls to prevent an adjudicator from accessing sensitive information and reporting it to outsiders or modifying a file (entering an invalid decision). Adjudicators can also approve a case that is not assigned to them. There is no tie between the case management system (i.e., National File Tracking System, or NFTS) and the case adjudication system (i.e., CLAIMS). In the internal case that occurred at USCIS, the perpetrator circumvented the interview process for 14 months –	USCIS should consider implementing technical controls to prohibit adjudicators from self selecting cases to adjudicate.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			he approved "no-show" cases. There were no controls to detect this. In addition, adjudicators can adjudicate any type of case, even though they are each assigned certain types of benefits cases for adjudication.	
Emphasis on Customer Service Over Risk	**Data Owners**	No evidence provided	One interviewee at the Vermont Data Center said that "stats" can be a strain, especially for new hires, although they do get a 90-day grace period.	USCIS should use caution in emphasizing customer service as the only performance metric because this could encourage lack of attention to risk-related activities (such as accurate adjudication decisions).
Lack of Separation of Duties in CLAIMS	**ISSOs** **Data Owners** **Information Technology**	Currently, all declined requests for benefits are reviewed by a supervisor. However, there was a discrepancy during interviews: adjudicators said that supervisors stopped looking at all denials because they are too busy. Supervisors also receive a report of all adjudication decisions entered by an adjudicator for a form type that the adjudicator does not normally approve.	Only a random sample of approved adjudication decisions is reviewed. For some cases (for instance, victims cases), a senior adjudicator has to review the decision after the adjudicator enters it, then the supervisor reviews it. This is a manually enforced process. There was another discrepancy: in interviews, the adjudicators said that	USCIS should consider implementing automated processes to prevent and detect fraud. Management indicated it would like to see automated technical enforcement of the review and approval process. In nearly ten percent (39) of the cases documented in the CERT database, insiders took advan-

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		When adjudicators are in training, they are under 100% review. They are in training on a specific type of case for at least 6 months. Auditing for improperly granted benefits is based on sampling and/or blind quality assurance (QA) according "to Army standards" after the fact. A randomly selected 30 cases per quarter are also reviewed by "sister centers." QA process varies office by office (no national process). This QA has been done for the past year and a half. In the Vermont field office, each supervisor pulls at least 10 cases per adjudicator per month. They review decision-related issues, security-related issues, and procedural issues (did they follow the right steps?). They also look for lessons learned. The primary purpose of QA is to identify the need for remedial training rather than deliberate fraud. Some cases are more than 1,000 pages, so every detail cannot be practically reviewed for every case.	clerks pull cases a couple of times per month – a certain number of cases per employee. Those cases are passed to QA, who reviews the cases. QA then sends feedback to the supervisor and adjudicator if they find something that does not look right.	tage of insufficient separation of duties to carry out their crimes. USCIS should carefully consider the biggest risk to the organization. Many of the USCIS employees interviewed for this assessment identified the primary risk for the organization as allowing the next terrorist to live and work legally in the United States. They desire assistance in identifying and implementing internal controls to counter that risk. Auditing every denied request indicates that the biggest risk to USCIS is to incorrectly deny a benefit to an applicant rather than to grant a benefit to someone who does not deserve it. If USCIS agrees that granting legal documents to illegal applicants is one of the biggest risks to the organization, then it should consider requiring dual

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				authorization for these adjudication decisions.
Lack of Automated Checks	**Data Owners** **Information Technology**	Vermont IT has done data sweeps after it found something suspicious. When it has done so, it has found more of the same activity.	There are no automated checks (there will be in Transformation). Checks that do exist are managed at the local level rather than alerting to the headquarters level.	In nearly twenty-five percent (91) of cases documented in the CERT Insider Threat Case database, the insider was able to carry out the crime because of inadequate auditing of critical processes; in 28 cases it was because of inadequate auditing of irregular processes. In 29 of the cases, the organization had repeated incidents of a similar nature. Automated scripts are an excellent mechanism for detecting suspicious transactions as well as honest mistakes. USCIS should consider a formal process for analyzing the OSI's findings and developing automated checks that are rolled out nationally.
Physical Security of Case Files	**Data Owners** **Adjudicators**	No evidence provided	The NFTS tracks millions of files. It was described, however, as a very large warehouse where files do occa-	Ten percent (40) of the insiders documented in the CERT database carried out their crimes by

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			sionally get lost. Adjudicators are supposed to "wand" the case files but sometimes they miss.	exploiting the physical security of the organization's facilities. USCIS should consider more strict physical controls as part of a risk assessment for the CLAIMS case files.
Prioritization of Process Improvements		The Vermont Service Center will be enforcing a revised adjudication practice that implements separation of duties so that the same adjudicator cannot 1) change an unlawful alien to non-immigrant status, and 2) change the non-immigrant to permanent residency status. The same officer will not be able to favorably adjudicate both steps. These two functions will be performed at different physical locations l29 miles apart.	This is a proactive approach to mitigating a serious insider threat risk. However, the assessment team was told that the Vermont Service Center has never had an adjudicator who illegally performed both steps. In addition, this new process will not be carried out at other Service Centers in the rest of the country.	This decision demonstrates that leadership at the Vermont Service Center and the CLAIMS data owners recognize the significant risk of creating legal citizenship documents for illegal aliens and are taking steps to mitigate that risk. However, our insider threat assessment has uncovered other issues that could be addressed to mitigate that risk. A formal risk analysis would enable USCIS to thoroughly examine the issues and prioritize countermeasures using a formal process. For example, an alternative to the physical move could be to implement an audit mechanism to look for adjudicators who performed both #1 and #2 for

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				the same applicant. C3LAN will be retired as part of Transformation; C4 will also be retired. A copy of security controls and requirements has been provided by C3LAN data owners to Transformation. It is important for the Transformation team to make risk-based decisions in Transformation design and development.
Disabling Access to CLAIMS	**Data Owners** **Information Technology**	Currently, every month USCIS compares the Human Resources attrition list against the C3-LAN account list and disables inactive employee accounts.	[redacted] The new HR form has not been socialized or widely advertised. It is up to the COTRs and supervisors to consistently request that access be disabled when an employee or contractor no longer needs access.	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]
Non-Attribution for DBA Accounts	**Information Technology**	[redacted]	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]
Pending Reduction in Force for Data Entry Clerks	**Data Owners** **Human Resources**	No evidence provided	Data entry clerks will be losing their jobs when they move to LockBox, which will take over the functionality of accepting remittances for benefit applicants. It was stated that the data entry clerks might be hired away to work at the organization which performs that function.	USCIS should be aware of the increased insider risk in the face of negative organizational events like this. It should consider proactive steps to decrease stress in the workplace and to ease potential financial burdens that could make employees more susceptible to recruitment by outsiders.
Sharing Accounts in CLAIMS	**Data Owners** **Information Technology** **Data Entry Clerks**	The NFTS will not let clerks log in if they have not used the system for a certain number of days.	A clerk's cube mate will log in for their cube mate if it is the end of the day and IT has gone home for the day.	Twenty-four (6%) of the insiders documented in the CERT database were able to carry out their crimes because insiders shared account and password information, often to make their jobs easier and to increase productivity. USCIS should consider increasing the consequences for infractions and possibly implement stronger authentication to make account sharing more difficult.

Fraud Detection and Naturalization System – Data System (FDNS DS)

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Logging of Transactions	**Data Owners** **Information Technology**	The FDNS DS is a central repository of fraud and national security investigations. This system holds applicants and petitioners, as well as PII. There is also a national security tab.	[redacted] but there are national controls to ensure that celebrities' files are not being accessed.	[redacted]
Elevated Privileges to FDNS DS	**Data Owners** **Information Technology**	No evidence provided	There is a large superuser community, more than thirty percent of all FDNS DS users, with access to the FDNS DS. These accounts have extensive power; a malicious superuser can completely delete a record or modify the summary of findings.	Ten percent (39) of the insiders documented in the CERT database took advantage of insufficient access controls. USCIS should consider reducing the number of privileged accounts with access to the FDNS DS. If the number of superuser accounts were reduced, then enhanced auditing could be employed on transactions conducted using those accounts.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Unknown [redacted] Connections to [redacted]	**Data Owners** **Information Technology**	No evidence provided	[redacted]	[redacted]
Failure to Address Known Security Vulnerabilities	**Data Owners** **Information Technology**	No evidence provided	There is no automated patching because of the age of the servers and the application. Only critical patches are applied for fear of crashing the servers.	Thirteen insiders in the CERT database exploited known security vulnerabilities that were not addressed by the organization. USCIS should consider upgrading the FDNS DS since these vulnerabilities increase risk of attack from outside and inside.
Production Data Available to Contractors in Development	**Data Owners** **Information Technology**	No evidence provided	CSC has production data in the development environment, even though it should not have access to production data.	Only one insider documented in the CERT Insider Threat Case database stole production data that should not have been available to developers in the development environment. However, it was extremely sensitive data with very strict controls in the production environment, and was not subject to those same controls in the development

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				environment. This is very similar to the situation at USCIS. USCIS should examine data being used in the remote, contractor-owned development environment and either sanitize or anonymize the data or enforce the same level of security controls exercised for the production data.
Configuration Management and/or Change Control Process Not Enforced	**ISSOs** **Data Owners** **Information Technology**	Developers cannot release new executables; a separate system administrator has to push them out.	Contractors sometimes release code to fix problems without following the change management process.	In 17 cases documented in the CERT Insider Threat Case database, the insider was able to attack because of lack of adequate configuration management. USCIS has a formal configuration management process. It is important to enforce its use for all employees and contractors. Otherwise, it will be extremely difficult to investigate a crime committed using flaws intentionally injected into source code by a contractor.

Appendix E: Incident Response

Incident Management / Security Awareness / Concerning Behaviors

Through case analysis, CERT has noted that procedures for responding to potential insider incidents present unique challenges; an incident response plan for insider incidents differs from a response plan for incidents caused by an external attacker. In addition, inadequate detection and response to security violations could embolden the insider, making the organization even more vulnerable to an insider crime. In fact, in 18 of the cases documented in the CERT Insider Threat Case database, the organization experienced repeat insider incidents of a similar nature. Insider incident management should leverage existing security policies and formal procedures for handling policy violations. Some of the cases from the CERT Insider Threat Case database illustrate insider attacks in which an organization's lack of incident response procedures limited its ability to manage its response effort, sometimes even resulting in multiple criminal acts by the same insider.

USCIS is a complex organization with many different components involved in detecting, tracking, investigating, and following up on employee misconduct. This complexity and widely distributed function creates a situation in which it is very difficult to obtain a complete picture of an individual's insider threat risk level. Because of this, it is practically impossible for USCIS to implement a proactive program to mitigate insider threat. CERT strongly recommends that USCIS create a central repository of employee misconduct so it can detect indicators of increasing insider threat risk and mitigate them as quickly as possible.

Furthermore, 81 of the insiders documented in the CERT Insider Threat Case database displayed concerning behaviors in the workplace prior to, or while carrying out, their criminal activities online. Supervisors and employees should be trained to recognize and respond to indicators of risk for violence, sabotage, fraud, theft, and other malicious insider acts. Even if it is not possible to require non-supervisors to report concerns, this training may increase the frequency of reporting and the deterrence of insider actions.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Lack of Central Repository of Employee Misconduct	**USCIS Leadership** **Physical Security** **Office of Security and Integrity**	If Field Security receives a Significant Incident Report (SIR), then it investigates. Employee misconduct is then reported to Office of Security and Integrity (OSI). If the OSI investigation substantiates an employee's misconduct, it provides Counterintelligence (CI) a monthly report. It also provides the employee's management a copy. CI is starting to get more reports of acceptable use violations and security violations. It tracks everything in a file for later use in reinvestigations. Labor Employee Relations (LER) has a record of the reports it receives of misconduct, complaints against an employee, rule violations, and so on. HR maintains the Official Personnel File, which contains records of suspensions, etc. LER contacts HR only for those types of actions. The OSI evaluates all complaints it receives and logs them into the case management system. It assigns them to a field office. At that point, any complaints are the responsibility of the special agent in charge at the field office. The field office investigates	There is no single place to go for an employee's disciplinary records. The number of organizations involved and management of records is very complex and distributed throughout the organization. According to Physical Security, the field office does not tell the OSI about problems– the OSI finds out when it "hits the press." For example, the OSI is not informed of a disgruntled system administrator who is exhibiting concerning behaviors.	USCIS should consider requiring mandatory reporting of all incidents to the OSI. This communication stream will allow the OSI to get involved as early as possible and to document and maintain a central repository of all incidents. This central repository is critical for adequately managing insider threats in USCIS.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		and sends the case for corrective action to the regional director in the chain of command, and then the regional director returns a management report of action to the special agent in charge. The OSI contacts the DHS OIG for potentially criminal behavior or serious misconduct. If the DHS OIG turns the case down, then it is sent to the field office or to law enforcement. The Personnel Security division (PERSEC) notifies the OSI monthly of arrests (tracked in the case management system) and the OSI notifies PERSEC of investigations.		
Tracking of Online Incidents	**Information Technology**	Computer or network violation incidents are tracked by a Remedy system tied to a unique computer identifier rather than a user in an attempt to keep PII out of the ticket.	It is difficult to tie an event to a particular person. Even if the identity of an offender is known, repeat offenders are not tracked in any automated or correlated way.	USCIS should consider including user information for each incident so that repeat offenders can be easily identified, as repeat offenses could indicate an insider of higher risk.
Consistency in Response to Security Violations and Concerning Behaviors	**USCIS Leadership** **Human Resources** **Physical Security**	No evidence provided	There is no required training for supervisors on how to respond to a range of behaviors associated with many forms of insider risk. Computer use violations are not	Eighty-one of the insiders documented in the CERT Insider Threat Case database displayed concerning behaviors prior to or while carrying out their criminal activities. Employees should be

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			handled consistently across departments, supervisors, and type of employee. Egregious violations are referred to the OSI for a full investigation, but the criterion for deciding when that is warranted is a gut reaction.	trained to recognize and respond to indicators of risk for violence, sabotage, fraud, theft, and other insider acts. Even if it is not possible to require non-supervisors to report concerns, this training may increase the frequency of reporting and deterrence of insider actions.
U.S. Department of State Investigations	**Office of Security and Integrity**	OSI Investigations have been subject to allegations of violations involving Foreign Service Nationals (FSN), but the OIS relies on the U.S. Department of State to investigate.	USCIS has no visibility into U.S. Department of State investigations.	FSNs who have access to USCIS systems and data should be included in an insider threat risk mitigation strategy.
Preparation for Negative Work Related Events	**USCIS Leadership** **Human Resources** **Physical Security**	No evidence provided	There do not appear to be any guidelines, training, or personnel available to evaluate employee insider risk before or after frequently precipitating events, such as termination, demotions, transfers, or other disappointments or unmet expectations. There also does not appear to be a group charged with evaluating insider risk from organizational events or developments affecting groups of employees, such as relocations, contract changes, layoffs, and reorganizations.	Fifty-five insiders documented in the CERT Insider Threat Case database had negative employment issues. Ninety-four had a change in employment status prior to their attacks; 20 had compensation or benefit issues, and 65 were disgruntled. Supervisors should be trained in these risk indicators. There should also be an available panel of specialists from the OSI or the Labor Employee Relations (LER) trained to assess such risk.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				Similar specialists should be available to participate in planning and execution of response plans in preparation for negative workplace events that potentially could lead to disgruntlement among the workforce at USCIS.
Contractor Management	**USCIS Leadership** **Physical Security** **Human Resources**	Personnel screening procedures for contractors are similar to those for employees. Contracting companies are required to report any adverse information regarding their employees immediately (in all contracts).	LER has no involvement with contractors. They have no record of contractor misbehaviors or complaints against contractors. Supervisors, the OSI, LER, and others concerned with organizational security may be largely unaware of insider risks related to contractors. Contractors are not subject to government monitoring or risk assessment. A contractor on a critical system may develop or have significant insider risk factors that may remain unknown to government employees due to lack of reporting requirements.	Sixty-two of the insiders documented in the CERT Insider Threat Case database were contractors. USCIS contract management staff should consider the need for reporting a range of potential indicators of insider risk among contract staff. Incident response plans should include response to employee and contractor issues.
Employee or Contractor Concerning Behavior	**USCIS Leadership** **Human Resources**	By policy, it is every employee's responsibility to report suspicious behavior or misconduct. Supervisors	Self-reported drug use, arrest, and associations with foreign nationals during employment are sent to the	Supervisors need to be notified immediately when an employee reports drug use, arrests, or

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
	Physical Security **Office of Security and Integrity** **Labor Employee Relations**	who observe concerning or suspicious behavior report it to LER or the OSI. For low-level misconduct, LER advises the field office management on handling the matter. LER reports more serious misconduct with more severe consequences to HR. Misconduct can also be reported via Significant Incident Reports (SIRs). SIRs are sent to Physical Security or to the OSI for investigation. If CI discovers something suspicious during a reinvestigation, it informs the employee's supervisor. The supervisor works with LER and counsel to decide on follow-up actions.	OSI. The OSI sends results to supervisor following investigation.	association with foreign nationals, so they have an accurate perception of the risk associated with each of their employees. In addition, 18 of the insiders documented in the CERT Insider Threat Case database had possible psychological issues. In collaboration with the OSI and LER, supervisors confronting employees who display concerning behaviors should have the ability to remove them from the workforce pending a medical or psychological evaluation to determine whether they have a disorder or illness that may impair their trustworthiness or judgment or make them a danger to themselves or others. Similarly, empowering supervisors to make an employee assistance program referral and evaluation mandatory, in collaboration with LER or the OSI, might help remove at-risk individuals from the workforce until they can safely and securely return.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Electronic Investigations	**Information Technology** **Office of Security and Integrity**	Most allegations reported to the OSI are not very technical; the OIT provides forensic support for investigations (primarily database transactions).	PERSEC has never asked the OIT to review a user's online activity. Only one person in OSI is qualified to do a forensic inspection.	USCIS should consider including the OIT in investigations of suspicious activity. CERT's insider threat research has shown that nontechnical concerning behaviors can be associated with online criminal activity. It would be beneficial to check for past technical security violations and have the OIT analyze current online activity as part of the OSI investigations.

Appendix F: Software Engineering

[redacted] Code Reviews / Configuration Management / Logging / Critical Data Controls

Malicious insiders, both employees and contractors, in the cases documented in the CERT database injected code into source code to facilitate both fraud and IT sabotage. In most cases, the modifications to source code were intended to sabotage the organization's systems, but in a few cases the code was used to facilitate fraud. In many cases the code was set to execute following the insider's termination; in one case, the code was planted for a year before finally executing. It is important that USCIS recognize the potential illicit activity that could be carried out by software engineers, and implement appropriate controls, particularly for the most critical systems and system components. [redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
[redacted] **Code Reviews**	**ISSOs** **Data Owners** **Information Technology**	Contractors are required to maintain a certain level of process maturity (CMMI Level 3) to be in compliance with USCIS policies. Source code is restricted to those with the need to know. Version Manager is used to control and track changes to source code. Separation of duties is implemented in the software release process: CSC checks new source code into Version Manager; a USCIS employee checks out the source code and releases it into production. The USCIS DBA moves new database objects into the production database.	[redacted] Another interviewee mentioned that an "Easter egg" was found in source code after the contract was given to a new company.[4]	[redacted]

[4] A virtual Easter egg is an intentional hidden message, joke or feature in a program, movie, book, etc.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Configuration Management and/or Change Control Process Not Enforced	**ISSOs** **Data Owners** **Information Technology**	No evidence provided	When contractors develop software remotely, they are supposed to register code in Version Manager, but this is not always done consistently. Contractors sometimes release code to fix problems without following the change management process.	In 17 cases documented in the CERT Insider Threat Case database, the insider was able to attack because of the lack of adequate configuration management. [redacted]
Software Engineering Controls in the Service Centers	**ISSOs** **Data Owners** **Information Technology**	No evidence provided	Software is being developed in the Service Centers without consistently enforcing the same change management processes enforced at the national (enterprise) level. The centers use a code repository, but not Version Manager, to track software changes. They do peer reviews of code and believe that enterprise controls for code review are more detailed (although that belief appears to be false, according to interviews at headquarters).	USCIS should consider consistent policies and procedures for software engineering for the entire enterprise, including the Service Centers.
[redacted]	**ISSOs**	[redacted]	[redacted]	Most insiders documented in the CERT Insider Threat Case data-

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
	Data Owners **Information Technology**		[redacted]	base were detected or identified using some kind of system log. Logs used include database logs, application logs, system logs, remote access logs, and many others. [redacted]
Production Data in Development Envi-	**ISSOs**	Development and production systems should be separate in terms of	In some cases, contractors have access to both systems, including pro-	Only one insider documented in the CERT Insider Threat Case da-

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
ronment	**Data Owners** **Information Technology**	data sharing and access control.	duction data in the development environment.	tabase stole production data that should not have been available to developers in the development environment. However, it was extremely sensitive data with very strict controls in the production environment, and was not subject to those same controls in the development environment. This is very similar to the situation at USCIS. USCIS should examine data being used in the development environment and either sanitize or anonymize the data or enforce the same level of security controls exercised for the production data.
[redacted]		[redacted]	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]

Appendix G: Information Technology

Account Management

Research has demonstrated that if an organization's computer accounts can be compromised, insiders have an opportunity to circumvent manual and automated control mechanisms intended to prevent insider attacks. Effective computer account and password management policies and practices are critical to impede an insider's ability to use the organization's systems for illicit purposes. In a variety of cases documented in the CERT Insider Threat Case database, insiders exploited password vulnerabilities, shared accounts, and backdoor accounts to carry out attacks. It is important for organizations to limit computer accounts to those that are absolutely necessary, using strict procedures and technical controls that facilitate attribution of all online activity associated with each account to an individual user. Furthermore, an organization's account and password management policies must be applied consistently across the enterprise to include contractors, subcontractors, and vendors who have access to the organization's information systems or networks.

In some areas, computer accounts are managed fairly well at USCIS. USCIS is implementing Homeland Security Presidential Directive 12 (HSPD-12) for physical and electronic account management. In addition, most shared accounts are controlled and all actions performed using those accounts can be attributed to a single user. However, some account management lies outside the control of USCIS. This presents a high degree of risk. First of all, accounts and access for FSNs should be considered carefully by USCIS. Although FSNs must submit paperwork through proper channels, which requires authorization by the CSO and CIO of DHS, such paperwork was not submitted consistently prior to 2007. As a result, there may be active accounts for which there is little to no accounting for the creation of the account. Furthermore, an FSN account and a U.S. citizen federal employee account cannot be distinguished once it is created. Although account naming conventions are dictated by DHS and the U.S. Department of State, USCIS could request a naming convention to differentiate between FSN and U.S. citizen federal employee accounts. In addition, USCIS should consistently track the authorization and creation of all USCIS accounts. To determine if unauthorized or legacy accounts exist, USCIS should consider conducting an account audit with the assistance of U.S. Department of State personnel to validate all existing FSN accounts.

Second, access to some critical USCIS systems is controlled by the Password Issuance and Control System (PICS). The purpose of PICS is to facilitate the administration of usernames and passwords to certain ICE and USCIS information systems. One area of concern regarding PICS is that it is administered by ICE, and there are more than 2,000 Local PICS Officers (LPOs) across various components of DHS. These LPOs use PICS to grant authorized access to ICE and USCIS systems for the personnel at their respective site or agency, such as local sheriffs, petitioners, Customs and Border Patrol (CBP), Department of Justice (DOJ), Transportation Security Administration (TSA), Terrorism Task Force, and DHS OIG. Each LPO can grant access to any system controlled by PICS. In other words, LPOs throughout USCIS and ICE can grant access for *any* of their staff to *any* USCIS system. Furthermore, USCIS has no visibility into who has access to its systems. Given the distributed nature of account administration, it is very difficult for USCIS data owners and OIT staff to manage authorization of user accounts to USCIS critical systems. Finally, the process for communicating changes in employee status and disabling accounts varies widely among individual field offices, Service Centers, and offices in the NCR. Dormant accounts provide a convenient unknown access path for current and former employees to use for illicit activity.

A lack of consistency exists in the application of account management practices under the control of USCIS. For example, disabling or terminating accounts for employees is not always completed in a timely manner upon the employee's change in status. This lack of consistency is made worse when decentralized LPOs across USCIS do not follow the same procedures. In other cases, employees are retaining access after a transfer when they should not, which requires the losing and gaining supervisors to notify proper account management personnel.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Account Establishment	**USCIS Leadership** **Information Technology**	In order for FSNs to gain access to USCIS systems, they must submit paperwork through proper channels, which eventually requires authorization by the CSO and CIO of DHS.	Prior to 2007, waiver paperwork for FSNs requesting account access was not submitted consistently. As a result, there may be active accounts for which there is little to no accounting for the creation of the account.	USCIS should consider conducting an account audit with the assistance of U.S. Department of State personnel to validate all existing FSN accounts.
	Information Technology	Different personnel are responsible for account creation and deletion across the entire enterprise, depending on the system or network in	Database administrators may be able to create and delete database and application accounts without a second person verifying that action.	Because database administrators have access to such critical data, USCIS should consider separating the task of authorizing access to

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		question.		USCIS databases from the task of managing the data in the databases. This separation of duties may reduce the risk of a database administrator creating an unauthorized account and using that account to carry out a malicious act.
	USCIS Leadership **Information Technology**	A computer account is established only after a number of criteria have been met, including security awareness training. In addition to the steps required of all personnel for account access, contractors have to go through extra steps, some of which include verification by the COTR.	Computer account access is sometimes granted before security awareness training is completed. This practice may be true especially for contractors, since the on-boarding process depends on the contracting agency and the COTR to verify that the training is completed.	USCIS should consider requiring computer security awareness training for all personnel – full-time employees, part-time employees, and contractors – and verify that it is complete before creating any system accounts for these personnel.
Account Management - General	**Information Technology**	PICS is administered by ICE, which has over 2,000 LPOs across various components of DHS. These LPOs are responsible for granting authorized access to PICS for the personnel at their respective work sites. Each LPO can grant access to any system controlled by PICS. In other words, LPOs throughout USCIS and ICE can grant access for any of their staff to	Although the PICS account process requires the account to be linked to a valid employee, PICS administrators could create unauthorized accounts in the name of valid employees without their knowledge. Invalid accounts are typically flagged only when the account is dormant for a certain period of time. An LPO can also assign rights for any system controlled by	In 12 of the cases documented in the CERT Insider Threat Case database, insufficient account management enabled the insiders to commit their crimes. USCIS should consider conducting account audits at the local site level, which would allow the validation of current PICS accounts and roles versus current

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		any USCIS system. [redacted]	PICS. Furthermore, ICE administers this system and could affect USCIS records unbeknownst to USCIS.	employee lists. USCIS should explore a means of segregating account management in PICS so that LPOs can administer accounts only for their own organization's systems. In other words, USCIS LPOs would only be able to administer authorizations for USCIS systems in PICS, and ICE LPOs would only be able to administer authorizations for ICE systems.
	Information Technology	Account management is handled by a number of different groups across USCIS. Although there is an effort to centralize account management, local and regional offices of USCIS have historically done their own account management. If an account has not been used for a certain period of time, it is automatically disabled. The time period stated by various interviewees varied from 30, 60, or 90 days.	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]
	USCIS Leadership **Information Technology**	When an employee moves from one position to another or transfers to another department, the management in those departments must initiate the required computer account changes.	The issue of account management for employee transfers is not being addressed in a consistent manner. The OIT relies on notification by either the new or old supervisor when an employee transfers, but there have been cases in USCIS in which employees have retained access when they should not have.	Six insiders documented in the CERT Insider Threat Case database were able to carry out their illegal activities because of "privilege creep." USCIS should review account management procedures to ensure that the steps currently taken to remove or alter account access are complete and being consistently followed. In particular, the procedures used when someone changes locations or departments within USCIS should be examined. As employees transfer throughout an agency, they should not be accumulating privileges. They should only retain privileges commensurate with their job responsibilities.
Changing Password of Shared Account Upon Termination	**Information Technology**	There are operating system images used throughout USCIS that permit an administrator to install a standard configuration of an operating system and accompanying software. [redacted]	[redacted] Though it would require physical access to a USCIS machine, that former	Twelve percent (46) of the insiders documented in the CERT Insider Threat Case database used system administrator privileges to sabotage systems or data; shared accounts were used by insiders following termination in

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		[redacted]	administrator would have administrator rights to GFE.	14 cases. Although an administrator would need physical access to a piece of equipment, [redacted]
Disabling Accounts or Connections Upon Employee Termination	**USCIS Leadership** **Information Technology** **Human Resources**	The OIT typically is notified of an account termination in one of three ways: 1) A standard form, called an exit clearance form, is distributed and signed by other parties, such as Human Resources and the Office of Security and Integrity (OSI). This form lets the OIT know that an employee's accounts should be disabled or terminated. 2) The supervisor of the departing employee contacts the OIT directly and informs them of the employee's departure. 3) When a contractor is involved, it is the responsibility of the COTR to inform the OIT.	It is clear from interviews with USCIS personnel that a single process is neither understood nor followed for disabling accounts following an employee or contractor termination. The procedures used are not consistent between supervisors or field offices, and for federal employees versus contractors. Sometimes the exit clearance form makes it to the OIT and sometimes it does not. The OIT's task is made even more difficult by the fact that it would need to know exactly which accounts an individual has access to.	The lack of consistency and awareness of the standard procedures may permit the account of an insider to be used following termination.
	Information Technology	The OIT receives an "attrition list" every 2 weeks. When this list is re-	Though this process is fairly effective, it potentially allows unauthorized	Terminating accounts even 2 weeks following termination may

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
	Human Resources	ceived, a manual check is done to ensure that employees who have departed in the last 2 weeks have their account access deleted.	access for 2 weeks following termination. Because this is a manual process, there is currently no automatic way to ensure that it happens. USCIS personnel cited an instance in which these procedures failed for an employee who was terminated as a contractor and later hired as a federal employee.	not be enough to prevent unauthorized or criminal activity. As soon as HR is aware of the change, a more automated mechanism of deleting these accounts should be implemented.
	Information Technology	LPOs work in their respective regions or offices and are decentralized by nature. The policies and procedures followed often depend on how things have been done historically in that particular office.	Because account authorization procedures are not standardized throughout all organizations using the PICS s, LPOs across the entire USCIS enterprise have not been consistent in how they have handled account deletion following employee termination.	USCIS should continue its efforts to centralize or reduce the number of LPOs in order for standard procedures to be followed. If this cannot be accomplished, standard procedures should be published, instructed, and consistently enforced.
Disabling Accounts or Connections During Employee Leave of Absences	**Information Technology** **Human Resources**	[redacted]	There is no official guidance or practice in the proper way to suspend access for an employee on a leave of absence. In one case provided by USCIS, an employee retained access to critical systems even after being placed on an administrative leave of absence.	A few insiders documented in the CERT Insider Threat Case database retained access to organization systems while on a leave of absence and used that access to steal information or commit fraud. USCIS should implement a policy to outline exactly what should be done when a government employee or contractor goes on a leave of absence, con-

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				sidering the risks versus benefits of allowing system access.
Sharing Account and Password Information	**Information Technology**	[redacted]	Although concern has been expressed about the existence of these accounts, the business justification has taken precedence over the risk being assumed.	Access to these accounts should be carefully documented and tracked so that credentials can be changed if someone in that restricted group no longer warrants access.

Access Control

An organization's lack of sufficient access control mechanisms was a common theme in many of the insider threat cases examined by CERT. Insiders have been able to exploit excessive privileges to gain access to systems and information they otherwise would not have been authorized to access. Additionally, insiders have been known to use remote access after termination to attack an organization's internal network. Organizations should ensure that network monitoring and logging is enabled for external access. Monitoring of network activity is extremely important, especially in the period between employee resignation and termination.

Given the distributed nature of access authorization via PICS, ICE, and the U.S. Department of State, non-USCIS employees and contractors could be granted access to USCIS critical systems. It is possible that the non-USCIS employees and contractors have not been through the rigorous preemployment screening required of USCIS employees and contractors, particularly those granted access through the U.S. Department of State for access from embassies overseas. USCIS should consider the risk these insiders pose to the protection of the critical USCIS data and systems, and implement protection mechanisms to limit the damage that these insiders might cause.

Other access control issues that should be considered include unrestricted access to some critical systems by OIT staff, lack of consistent processes for managing employee access as they move from one department to the next within USCIS, ability to use personal computers for USCIS work, and lack of monitoring and controls for some critical system administration functions.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Access Control - Foreign Service Nationals	**Information Technology** **Human Resources** **Office of Security and Integrity**	Currently, a Foreign Service National (FSN) requiring access to USCIS systems submits paperwork, including a waiver, through the USCIS director and the CIO and CSO of DHS.	Although the assessment team was able to get limited visibility into this practice, it seems to be aligned with the policy. If true, it has given USCIS and DHS better visibility into this activity.	The practice should be continued and expanded as needed to inform all relevant USCIS personnel.
	Information Technology **Human Resources** **Personnel Security** **Office of Security and Integrity**	When FSNs require access to USCIS systems in embassies and consulates abroad, they are vetted by the U.S. Department of State.	Because the U.S. Department of State is performing the vetting process, USCIS has very little control or visibility into the process for granting FSNs access to USCIS systems and networks. Interviewees stated that, in some cases, FSNs have administrative control over some systems and that, in other cases, they are serving as information system security officers (ISSOs).	USCIS should gain a better understanding of the U.S. Department of State's vetting process and clarify its own requirements for granting and tracking access for FSNs to USCIS systems. If continued access is required, the procedures to document and control that access should be negotiated with the U.S. Department of State and consistently enforced.
	Information Technology	Once a traditional user account is created, there is little to no way to distinguish an FSN account from one belonging to a U.S. citizen.	Because an FSN account is not distinguishable from other accounts, it would be extremely difficult to associate specific online activities with accounts belonging to FSNs. E-mail	USCIS should consider whether or not it wants the ability to distinguish what online activities and accesses FSNs are engaging in. If so, it should incorporate

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			addresses appear the same and violation activities would not easily be attributed to an FSN.	those steps into the procedures mentioned above.
	Information Technology	DHS is in the process of building a secure intranet called OneNet, which will better enable information sharing among DHS components. This project will be enabled by interconnection agreements between segments.	Once the appropriate interconnection agreements are in place, it will be harder to restrict access for FSNs to specific systems (e.g., SharePoint).	USCIS should make a determination about whether or not FSN access should be any different from other, similar accounts of U.S. citizens. If the lack of restrictions is unacceptable, that issue should be brought to DHS personnel responsible for implementing the OneNet solution.
Access controls		There are business process and resources (e.g., PICS, CLAIMS 3, and CLAIMS 4) that are shared with ICE. This partnership is an artifact of the past and current relationships between departments within DHS.	For these shared resources to function properly, they require careful coordination, which does not take place in all cases. For example, USCIS does not receive a copy of the formal access request submitted to ICE for an ICE employee to access a USCIS system.	USCIS should carefully document what access is being granted to any parties external to USCIS. If additional coordination is required, it should be done with the relevant departments of DHS.
		For certain information systems, local and remote logins are not permitted between the hours of 11:30 p.m. and 6:00 a.m.	This practice closely adheres to the policy for specific systems.	Enforcing a mandatory access period may help ensure that a malicious insider is not using systems when supervision is lessened. Eight percent (29) of the insiders documented in the CERT Insider Threat Case database

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				used access outside of normal working hours to carry out their illicit activities.
		When an employee attempts to log into a restricted system during off-peak hours, an automatic e-mail notice is sent by the OIT to persons in the employee's management chain of command.	This practice is not consistent across all systems and is not part of other incident response procedures.	USCIS should consider implementing this practice into the larger system of incident response, to include correlation with other events and over a period of time.
Access Privileges – General	**USCIS Leadership** **Information Technology**	At the Vermont Service Center, OIT staff are the only ones present late at night. As part of their duties, they also have electronic access to the CLAIMS3 information system.	As a function of the electronic access and the physical layout of the Service Center, OIT personnel have access to CLAIMS3 as well as the physical files in the building.	USCIS should consider the minimum level of access (least privilege) needed for all personnel to accomplish their job duties. Thirteen percent (49) of the insiders documented in the CERT Insider Threat Case database violated a need to know in order to perpetrate their crimes, including stealing PII and proprietary information. In addition, several insiders committed their crimes while working on the night shift, where they enjoyed a reduced level of scrutiny. Unrestricted electronic and physical access to such high-risk data and systems outside of normal working hours presents a high degree of risk to

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				USCIS.
	[redacted]	[redacted]	[redacted]	[redacted]
	Information Technology **Office of Security and Integrity**	The U.S. Department of State Consular Affairs network grants access to FSNs working in embassies and consulates and it connects to USCIS systems.	According to one interviewee, some FSNs on the Consular Affairs network are suspected to be working for arms of foreign intelligence or security agencies. USCIS has used technical methods (e.g., firewalls) to ensure that USCIS systems are protected from any interconnections with the U.S. Department of State's networks.	Since USCIS cannot determine what access the U.S. Department of State grants to FSNs on its systems, USCIS should continue to use technical measures to prevent unauthorized access while working with counterintelligence personnel to deal with suspected foreign agents working around U.S. government facilities.
Access Privileges – System Administrator		There is a single person who has the knowledge of and responsibility for administering the voicemail systems	This single point of failure makes it difficult to recover from a malicious act on this particular system.	A few insiders in the cases analyzed by CERT used their unrevoked access to the organiza-

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		for USCIS.		tion's phone system to harm the organization. In one case, the entire customer service voice mail system was redirected to a pornographic phone site. In another, derogatory comments about the organization were recorded and played for every voice mailbox. USCIS should place additional staff in the role of administrators for the USCIS voicemail system. This would allow USCIS to implement some form of separation of duties, or at the very least, minimal checks and balances to prevent tampering with the voicemail system. USCIS should ensure that it manages accounts and passwords for internal systems such as voice mail, as well as external accounts. One insider documented in the CERT Insider Threat Case database changed the domain name system registry for his organization's website so that visitors were sent to a pornographic

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				website. These types of accounts are used very infrequently, and are often not included in formal termination procedures.
Management of Remote Access	**Information Technology** **Security Network Operations Center**	Port security would prevent a user from connecting a personal machine directly to a USCIS network. This security mechanism is handled by the SNOC. Remote access, on the other hand, is handled by DHS. USCIS has access to very limited information, including logs, for remote connections because of contract stipulations with Sprint. The assessment team received conflicting opinions about whether a personal machine could be connected with a remote account.	Although connecting a personal laptop to a USCIS network via a remote connection may or may not be blocked, the SNOC was not confident it would be blocked because it does not control that access. It is possible that a user could connect with a personal machine if DHS allowed it.	USCIS should coordinate with DHS personnel to ensure that desired USCIS security policies are enforced for personnel accessing USCIS systems and data. Seven percent (26) of the insiders documented in the CERT Insider Threat Case database were able to attack in part because of insufficient monitoring of external access.
	Information Technology	[redacted]	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]
	USCIS Leadership **Information Technology**	[redacted]	The contractors responsible for VIS have implemented a strict access control solution with Firepass and it appears to accomplish its goal of ensuring that only the proper personnel are granted access and that they perform authorized actions once they are connected. Unfortunately, they are the only contractors and system using Firepass and it will not be used once the move is made to Stennis Space Center. They are unsure of what controls will be used at Stennis.	Implementing a Firepass solution for all USCIS systems might not be cost-effective. USCIS management should at least examine the risk posed to the most critical systems and implement a Firepass-like solution for those that require remote access. As stated above, one in ten insiders documented in the CERT Insider Threat Case database used the creation of unknown paths into organization systems; proper measures might have prevented many of those instances.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		[redacted]		
Non-System Administrators With Authorized Access to Administrator Accounts	**USCIS Leadership** **Information Technology**	According to one interviewee, FSNs are system administrators on some U.S. Department of State systems in embassies or consulates abroad. The U.S. Department of State has authorized access for some FSNs to some USCIS systems needed for the performance of their duties.	An FSN who is a system administrator for U.S. Department of State systems does not necessarily have administrator rights on USCIS systems. One interviewee expressed concern, however, that an administrator who is a citizen of a foreign country could escalate privileges or use social engineering tactics to gain unauthorized access to USCIS systems.	Ten percent (39) of insiders documented in the CERT Insider Threat Case database took advantage of insufficient access controls to conduct their crimes. USCIS should examine USCIS system access for U.S. Department of State system administrators, as well as how those connections are monitored or logged. They should also work with the U.S. Department of State to understand its processes for granting FSNs access to U.S. Department of State systems.
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	USCIS Leadership **Information Technology**	There are currently no limits on which A-files an adjudicator can request in the National File Tracking System (NFTS).	The lack of limits placed on requesting A-files in NFTS may allow adjudicators to request a file by name even if they should not be accessing that file.	There should be logical controls to detect "extraordinary" or suspicious file transfer requests. In one USCIS case, the insider requested a file transfer to a region for an individual whose files were in another region and whose forms had been previously denied.

Protection of Controlled Information

Protecting controlled information (i.e., information that is classified, sensitive but unclassified, or proprietary) is critical to mitigating the insider threat risk to organizations. A variety of insider threat cases studied by CERT revealed circumstances in which insiders carried out an attack through the unauthorized download of information to portable media or external storage devices. In some instances, malicious insiders used email to plan their attacks or to communicate sensitive information to competitors or conspirators. Organizations must ensure that employees understand policies regarding what constitutes acceptable use of company resources, including information assets, and enforce compliance through technical means. The unauthorized exfiltration of controlled information by malicious insiders can have devastating effects on an organization. Protecting controlled information (i.e., information that is classified, sensitive but unclassified, or proprietary) is critical to mitigating the insider threat risk to organizations.

USCIS has implemented network monitoring strategies that would detect large amounts of data downloaded or an anomalous increase in network traffic, either by total volume or type of traffic (e.g., by port or protocol). Though monitoring network traffic may help protect controlled information, [redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Data Download to Media	**Information Technology**	[redacted]	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		[redacted]	[redacted]	[redacted] USCIS should consider two options: 1) Except for authorized instances that are appropriately tracked, these devices could be technically prohibited from functioning in USCIS systems. The fact that they are prohibited should be the content of a security awareness campaign. 2) If USB devices are permitted for use, then all uses of them should be logged and those logs audited for suspicious activity by employees leaving the organization, employees exhibiting other signs of potential malicious behavior, etc.
Data Download to or From Home	[redacted]	There is a policy against using personally owned computer equipment to perform official duties for USCIS. Telework should be done with government furnished equipment (GFE) only.	A case from the USCIS Convictions Task Force showed that one insider performed a significant amount of official business, including telework, on his personal laptop. He accessed systems and e-mail in order to de-	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			velop a system that he was rewarded for producing. There are no technical controls to catch this activity unless the device is physically plugged into the network.	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Protecting Critical Files	**Information Technology**	The SNOC responds to spills of PII, which occur on a weekly basis. The information about the incident is transferred from the data owner who becomes aware of the spill to the OSI, which creates a Serious Incident Report (SIR) that it forwards to the Privacy Officer and finally to the SNOC.	[redacted] The response effort to a PII spillage involves many parties and appears to be a complicated process for an event that happens on a weekly basis. Though these spillages are accidental events, [redacted]	USCIS responds to PII spillages often enough that its staff is well versed in response procedures. Unfortunately, the frequency to which incidents occur and the response procedures in place do not seem to reduce the number of incidents or provide automated detection when spillage occurs. [redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			[redacted]	[redacted]
	Information Technology	Access to network resources is terminated immediately when a spill or misconduct is suspected.	This practice appears to be done consistently.	USCIS should continue this practice as part of its incident response procedures. Incorporating an appropriate level of monitoring would also be a prudent measure.

Audit / Monitor / Backup / Recovery

Insider threat research conducted by CERT has shown that logging, monitoring, and auditing employee online actions can provide an organization the opportunity to discover and investigate suspicious insider activity before more serious consequences ensue. Organizations should leverage automated processes and tools whenever possible. Moreover, network auditing should be ongoing and conducted randomly, and employees should be aware that certain activities are regularly monitored. This employee awareness can potentially serve as a deterrent to insider threats.

Preventing insider attacks is the first line of defense. Nonetheless, effective backup and recovery processes need to be in place and operationally effective so that if a compromise occurs business operations can be sustained with minimal interruption. In one case documented in the CERT Insider Threat Case database, an insider was able to magnify the impact of his attack by accessing and destroying backup media. Organiza-

tions need to consider the importance of backup and recovery processes; and care must be taken that backups are performed regularly, protected, and tested to ensure business continuity in the event of damage to or loss of centralized data.

[redacted]

In addition, the SNOC lacks the resources to focus on monitoring for suspicious insider activity, focusing instead primarily on protection from external incidents.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Modification / Disabling Log Files	**Information Technology**	Log files are accessible by the domain administrators and system administrators of each respective system.	[redacted]	[redacted] USCIS should send critical logs to a centralized log server and protect the log files to permit a forensic reconstruction of network or host-based events.
	Information Technology	[redacted]	The lack of consistency for what is logged across USCIS servers, systems, applications, and workstations is concerning. Several parties addressed	Although six percent (23) of the insiders documented in the CERT Insider Threat Case database were able to modify or disable

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		are sometimes limited to 24 hours or less of collection. [redacted]	the fact that IT personnel must be able to physically reach a machine in a timely fashion if they hope to capture logs related to an incident. This assumption makes it likely that critical log information will be missed. [redacted]	log files, [redacted]
Monitoring Suspicious Activity	**Information Technology**	[redacted]	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]
	Information Technology	[redacted]	[redacted]	[redacted]
	Information Technology	Database administrators are responsible for monitoring and alerting when data access attempts are made to critical data in USCIS databases.	[redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
			[redacted]	USCIS should consider clearly defining the responsibility of database administrators and the SNOC for monitoring, alerting, and responding to unauthorized data access. Once the responsibility is assigned, the appropriate group should diligently prevent, detect, and respond to unauthorized data access, modification, and exfiltration attempts.
	Information Technology	USCIS has the ability to create inbound firewall rules to filter potentially malicious network traffic.	Network traffic filtering is happening only on inbound traffic, not outbound traffic. The resources do not exist to examine outbound traffic, only inbound traffic. Furthermore, the intrusion detection systems are not optimized to detect security events.	USCIS should consider implementing a network monitoring strategy that monitors and filters inbound and outbound network traffic. This strategy may prevent or detect the unauthorized transfer of USCIS data outside the organization.
	Information Technology	No evidence provided	[redacted]	Many insiders documented in the CERT Insider Threat Case database were able to commit their malicious activities using laptops. [redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]
	Information Technology	The SNOC is responsible for determining the root cause of an incident, including using forensic tools to identify affected workstations, desktops, and laptops.	The SNOC has had problems identifying the root cause of an affected workstation or user because of the lack of network forensic applications. Ideally, the SNOC should be able to trace network traffic from source to destination and watch activity. It has a stand-alone forensic capability but nothing on the network.	USCIS should consider implementing a network monitoring strategy that includes forensic tools to aid investigations.
Backups	**Information Technology**	Backup testing for many systems occurs once per year. In some cases, the backups are only tested with a tabletop exercise and do not use similar or identical hardware to that used in the production environment.	Tabletop exercises may not give USCIS a true indication of its ability to recover from a systemic failure. When possible, backups should be implemented on similar hardware to ensure that the backup tape is functional and the backup is operational.	In six percent (22) of the cases documented in the CERT Insider Threat Case database, the impact of the crime was magnified because of insufficient backups. [redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				[redacted]
	Information Technology	Years of backup tapes are kept on-site at the Vermont Service Center, and system administrators have access to these backup files.	Administrators who have access to the backup tapes would be able to [redacted]	Backup media should be controlled carefully, documented, and stored offsite with limited access. Without those controls, USCIS cannot be sure its backups will give it the ability to recover.

Technical Security Vulnerabilities

Proactively addressing known security vulnerabilities should be a priority for any organization seeking to mitigate the risk of insider threats as well as external threats. Case studies have shown that malicious insiders, following termination, will sometimes exploit known technical security vulnerabilities that they know have not been patched to obtain system access and carry out an attack. Organizations should have a process to ensure that operating systems and other software have been hardened or patched in a timely manner when possible. Failure to address known vulnerabilities provides an insider ample opportunity and pathways for attack, making it more difficult for an organization to protect itself.

[redacted]

[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Addressing Known Security Vulnerabilities	**Information Technology**	[redacted]	[redacted]	[redacted]
Addressing Known Security Vulnerabilities	**Information Technology**	The OIT relies on two mechanisms to detect the download of malicious code: 1) DHS [redacted] monitors the Internet gateway, and 2) [redacted] agent on workstations. [redacted] alerts the OIT immediately upon discovery of known malware. The OIT shuts down the port to block malicious code where appropriate. [redacted] also detects installa-	The presence of perimeter and host protection for malware puts USCIS in a relatively secure position regarding malicious downloads. [redacted]	[redacted]

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		tion of malicious code from USBs and other media.		[redacted]
Unmanaged Systems	**Information Technology**	USCIS users have local administrator rights on their own machines. This allows users to install software on their systems. Some authorized software does require administrator rights to install. Some applications actually require administrator rights to run.	[redacted] A mitigating factor is that the departing employee would need physical access to the system to log in. [redacted] A user with administrator privileges must not rely solely on automatic mechanisms to safeguard his or her computer. Administrator rights give inadvertently downloaded malware the ability to completely compromise a system, sometimes without the knowledge of the user.	Twelve percent (46) of the cases documented in the CERT Insider Threat Case database involve users abusing administrator privileges to sabotage systems or data. Although USCIS users need for administrator rights to install or run authorized software, the OIT should consider giving users separate administrator accounts for these explicit purposes. Users could then use non-administrator accounts for their daily work. This would greatly minimize the risk of malware compromise.

Configuration Management

Effective configuration management helps ensure the accuracy, integrity, and documentation of all computer and network system configurations. A wide variety of cases in the CERT Insider Threat Case database document insiders who relied heavily on the misconfiguration of systems. They highlight the need for stronger, more effective implementation of automated configuration management controls. Organizations should also consider consistent definition and enforcement of approved configurations. Changes or deviations from the approved configuration baseline should be logged so they can be investigated for potential malicious intent. Configuration management also applies to software, source code, and application files. Organizations that do not enforce configuration management across the enterprise are opening vulnerabilities for exploit by technical insiders with sufficient motivation and a lack of ethics.

The OIT has a configuration management policy that provides baseline software configurations for USCIS desktops and laptops. The OIT scans for incorrect, outdated, or un-patched versions of software on the approved software list. The OIT keeps track of different baselines for different contracts. Despite tracking and a rigorous configuration management policy, the OIT has difficulty keeping track of the 90-150 different system images in the USCIS environment. Rogue software or malware is often discovered through a deliberate manual scan, rather than through an automated process. To make this task more difficult, there have been USCIS employees with seniority or influence who are able to use local administrator privileges to install software for the sake of convenience.

Concerns regarding configuration management make it difficult for the OIT to adequately prevent, detect, and respond to rogue software or malware using its current procedures. We suggest some considerations for leveraging existing deployments and modifying incident response practices to increase effectiveness.

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
Configuration Management	**USCIS Leadership** **Information Technology**	The OIT has a configuration management policy for software configuration baselines. The OIT scans for incorrect, outdated, or unpatched versions of software on the ap-	Despite rigorous configuration management policy, the OIT has difficulty keeping track of the 90 to 150 different system images in the USCIS environment. Rogue software or malware	Seventeen cases documented in the CERT Insider Threat Case database involve users exploiting the lack or weakness of a configuration management system

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
		proved software list. The OIT keeps track of different baselines for different contracts.	is often discovered through a deliberate manual scan rather than through an automated process.	to carry out their attacks. The OIT could leverage the existing ePO deployment to complement its configuration management efforts. ePO can define a baseline for software applications and alert on any deviations from that baseline.
	USCIS Leadership	No evidence provided	In some cases, individuals with seniority or influence are able to use administrator privileges to install software for the sake of convenience.	USCIS should ensure that configuration policy is consistently communicated and enforced throughout the organization. Even senior leadership should not be able to casually circumvent these policies without going through the proper channels as defined by the configuration management policy.
Configuration Management	**USCIS Leadership** **Information Technology**	Service Centers are responsible for locking down desktops to prevent unauthorized software from running.	The lockdown process relies on human intervention. If call volume to the Service Center is heavy, this may increase response time to an unacceptable level.	The OIT should explore ways to automate lockdown of potentially compromised systems. This would require a careful balance of service versus security. On the service side, delayed response by the Service Center may result in loss of productivity. On the security side, delayed response could

Area of Concern	Responsible Personnel	Policy and/or Security Measure	Policy or Practice Gaps	Suggested Countermeasures
				lead to system compromise. Management should evaluate the risks of a compromise and weigh those risks against the potential consequences of service disruption.

Appendix H
Acronyms

C3-LAN	CLAIMS 3 – Local Area Network
CBP	Customs and Border Protection
CI	Counterintelligence
CIO	Chief Information Officer
CLAIMS	Computer Linked Application Information Management System
CMMI	Capability Maturity Model Integration
COTR	Contracting Officer's Technical Representative
CSC	Computer Sciences Corporation
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CMU	Carnegie Mellon University
DBA	Database Administrator
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FDNS-DS	Fraud Detection and National Security Data System
FISMA	Federal Information Security Management Act
FSD	Field Security Division
FSN	Foreign Service National
GFE	Government-furnished Equipment
HR	Human Resources
HSPD-12	Homeland Security Presidential Directive 12
ICE	Immigration and Customs Enforcement
ISSO	Information System Security Officer
IT	Information Technology
LER	Labor and Employee Relations
LPO	Local PICS Officer
NCR	National Capital Region
NFTS	National File Tracking System
ODBC	Open Database Connectivity
OIG	Office of Inspector General
OIT	Office of Information Technology
OSI	Office of Security and Integrity
PERSEC	Personnel Security
PICS	Password Issuance and Control System
PII	Personally Identifiable Information
QA	Quality Assurance
SEI	Software Engineering Institute
SIEM	Security Information and Event Management
SIR	Significant Incident Report
SNOC	Security Network Operations Center
TSA	Transportation Security Administration
USB	Universal Serial Bus

USCIS	U.S. Citizenship and Immigration Services
VIS	Verification Information System

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director MS-2000
Washington, DC 20529-2000

U.S. Citizenship and Immigration Services

Memorandum

TO: Frank Deffer, Assistant Inspector General for IT Audits
Office of Inspector General

11/17/10

FROM: Lauren Kielsmeier
Acting Deputy Director

SUBJECT: USCIS Responses to OIG Draft Report *Examining Insider Threat Risk at U.S. Citizenship and Immigration Services*

United States Citizenship and Immigration Services (USCIS) appreciates the opportunity to review and comment on the subject report and agrees with the findings and recommendations identified by the Department of Homeland Security's Office of the Inspector General (OIG). USCIS and OIG staff have discussed the report contents in detail and USCIS has provided the OIG with substantive responses to its findings and recommendations.

We take seriously our obligations to protect USCIS's information technology systems and the information contained in those systems. Your report will be of great assistance to us as we seek to further strengthen our internal controls in this area.

If you have any questions, please contact Mary Thomas, Chief, Internal Review Division, Office of Security and Integrity at (202) 272 1500.

Software Engineering Institute, Carnegie Mellon University

Insider Threat Center at CERT

Department of Homeland Security, Office of Inspector General

Richard Saunders, Director, Advanced Technology Division
Steve Matthews, IT Audit Manager, Advanced Technology Division
Philip Greene, IT Auditor/Team Lead, Advanced Technology Division

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer
Chief Information Security Officer
USCIS Chief Information Officer
USCIS Chief Information Security Officer
USCIS Audit Liaison Office

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, please call the Office of Inspector General (OIG) at (202) 254-4100, 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.