OFFICE OF INSPECTOR GENERAL

# USSS Faces Challenges Protecting Sensitive Case Management Systems and Data

Homeland Security

October 7, 2016

OIG-17-01

# DHS OIG Highlights

## *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*

**October 7, 2016**

## Why We Did This Audit

We performed this audit as a follow-up to a September 2015 Office of Inspector General (OIG) investigation regarding United States Secret Service (USSS) employees improperly accessing and distributing sensitive information on the agency's Master Central Index (MCI) mainframe system. Our objective was to determine whether adequate controls and data protections were in place on systems to which MCI information was migrated.

## What We Recommend

We are making 10 recommendations to USSS and 1 recommendation to the DHS Privacy Office to reduce the risk of future unauthorized access and disclosure of sensitive information.

**For Further Information:**
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

## What We Found

USSS did not have adequate protections in place on systems to which MCI information was migrated. USSS information technology (IT) management was ineffective, including inadequate system security plans, systems with expired authorities to operate, inadequate access and audit controls, noncompliance with logical access requirements, inadequate privacy protections, and over-retention of records.

These problems occurred because USSS has not consistently made IT management a priority. The USSS Chief Information Officer (CIO) lacked authority for all IT resources and was not effectively positioned to provide necessary oversight. Inadequate attention was given to updating USSS IT policies to reflect processes currently in place. High turnover and vacancies within the Office of the CIO meant a lack of leadership to ensure IT systems were properly managed. In addition, USSS personnel were not adequately trained to successfully perform their duties.

USSS initiated steps in late 2015 to improve its IT program, including centralizing all IT resources under a full-time CIO and drafting plans for an improved IT governance framework. However, until these improvements are implemented and can demonstrate effectiveness, USSS systems and data will remain vulnerable to unauthorized access and disclosure, and the potential for incidents similar to what the OIG investigated in 2015 will remain.

## USSS and DHS Privacy Office Responses

USSS concurred with all 10 of our recommendations. The DHS Privacy Office concurred with our 1 recommendation.

**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

October 7, 2016

MEMORANDUM FOR: Kevin Nally
Chief Information Officer
United States Secret Service

Jonathan R. Cantor
Acting Chief Privacy Officer
DHS Privacy Office

FROM: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*

Attached for your action is our final report, *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*. We incorporated the formal comments from the United States Secret Service (USSS) in the final report.

The report contains eleven recommendations to reduce the risk of future unauthorized access and disclosure of USSS sensitive information. We made 10 recommendations to USSS and 1 recommendation to the DHS Privacy Office. USSS and the DHS Privacy Office concurred with these recommendations. Based on information provided in your response to the draft report, we consider all recommendations to be open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Richard Saunders, Director, Advanced Technology Projects Division, at (202) 254-5440.

Attachment

## Table of Contents



## Appendixes

## Abbreviations

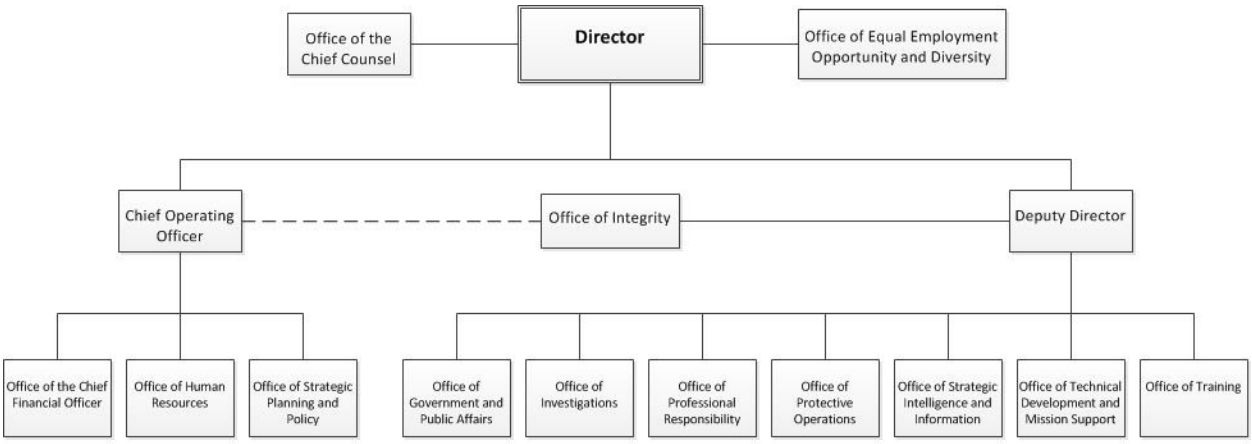
| | |
|---|---|
| ATO | authority to operate |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CLEAR | Clearances, Logistics, Employees, Applicants, and Recruitment |
| eCase | Electronic Case Management System |
| eCheck | Electronic Name Check System |
| FIPS | Federal Information Processing Standards |
| FIRS | Field Investigative Reporting System |
| FISMA | *Federal Information Security Management Act* |
| FOIA | *Freedom of Information Act* |
| HCMS | Human Capital Management System |
| HSPD | Homeland Security Presidential Directive |
| IRMD | Information Resources Management Division |
| ISSM | Information System Security Manager |
| ISSO | Information System Security Officer |
| IT | information technology |
| MCI | Master Central Index |
| NARA | National Archives and Records Administration |
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PIA | Privacy Impact Assessment |
| PII | personally identifiable information |
| PIV | personal identity verification |
| PTA | Privacy Threshold Analysis |
| PTMS | Protective Threat Management System |
| SSP | System Security Plan |
| USSS | United States Secret Service |

## Background

The United States Secret Service (USSS) became part of the Department of Homeland Security with the passage of the *Homeland Security Act of 2002*.[1] USSS carries out a combined mission of protection and investigation. Specifically, USSS protects the President, Vice President, former presidents and their spouses, foreign visiting heads of state and government, and National Special Security Events. It is responsible for ensuring security of the White House, the Vice President's residence, and other designated buildings within the Washington, DC area. The agency also investigates financial and cyber-crimes and safeguards the Nation's financial infrastructure and payments systems to preserve the integrity of the economy.

At the end of fiscal year 2015, USSS consisted of 6,307 Federal employees in more than 150 locations worldwide. Figure 1 shows the USSS organizational structure.

**Figure 1: Secret Service Organizational Structure as of May 2015**




*Source:* USSS

USSS Information Technology System History

Information technology (IT) is critical for USSS to accomplish its dual protective-investigative mission. To support this mission, in 1984, USSS developed and implemented the Master Central Index (MCI) mainframe application as an essential system for use by USSS personnel in carrying out their law enforcement mission.

[1] Public Law 107–296, November 25, 2002.

As part of its functionality, MCI facilitated the USSS investigative process by serving as a case management tool, providing for the retrieval of investigative and criminal history information. It contained a collection of data pertaining to all aspects of cases handled by USSS, such as case management, arrest history, and collections and statistical analysis of arrest and prosecution data for all defendants. In addition, MCI served as a report generation tool, enabling USSS personnel to compile information regarding case status, subjects, and arrest credit. Protective, investigative, and human capital names were copied from other USSS systems of record into MCI to provide a single access point for case agents conducting investigations.

In 2007, at the request of the USSS, the National Security Agency performed an independent security review of the USSS mainframe system, including the MCI application residing on this mainframe. Its review identified IT security vulnerabilities within all applications hosted on the mainframe. According to USSS personnel, one of the key deficiencies of MCI was that once a user was granted access to the MCI, the user had access to all data within MCI regardless of whether it was necessary for the user's role.

In response to the 2007 review, in 2011, USSS initiated the Mainframe Application Refactoring project. Its intent was for 48 mainframe applications, system capabilities, and associated data to be migrated to a non-mainframe environment. In 2013, the Mainframe Application Refactoring project was accelerated and completed on July 24, 2015. At that time, all of the legacy mainframe data was migrated to a non-mainframe environment and all USSS personnel access was revoked from the mainframe. USSS began final mainframe disassembly on August 12, 2015, and physically removed it from the USSS data center on September 16, 2015.

According to the USSS Acting Chief Information Officer (CIO), MCI legacy mainframe data and information migrated to the following five USSS information systems in July 2015:

(1) **Field Investigative Reporting System (FIRS)** – Used by USSS field agents to document investigative cases, threat assessments, crime patterns, standard operating procedures, and lessons learned.

(2) **Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR)** – Used by the Security Clearance Division, Uniformed Division, and the Personnel Division (Human Resources) to manage and store information related to job vacancies and employment applications.

(3) **Protective Threat Management System (PTMS)** – Used by the USSS Protective Intelligence and Assessment Division to provide consolidated incident and threat case management information.

(4) **Electronic Name Check System (eCheck)** – Used by the USSS Dignitary Protective Division to conduct security name checks on National Special Security Event workers to grant access to events and produce physical credentials. These name checks are performed through the National Crime Information Center information system, a nationwide information system established by the Federal Bureau of Investigation.

(5) **Electronic Case Management System (eCase)** – Used by USSS as a case management system to track general protection of detailees and applicant security clearance cases.

Access and Distribution of a Congressman's Personally Identifiable Information

In September 25, 2015, the DHS Office of Inspector General (OIG) issued a memorandum summarizing an investigation into allegations of improper access and distribution of U.S. Congressman Jason Chaffetz's[2] personally identifiable information (PII) contained within a USSS mainframe database.[3] The investigation began in April 2015 and was completed in August 2015, around the same time that the MCI legacy data were transferred to the non-mainframe environment. The investigation concluded that 45 USSS employees accessed the MCI mainframe database containing sensitive PII pertaining to Congressman Chaffetz on approximately 60 occasions. Of those 45 employees, only 4 had a legitimate business need to access this information.

The OIG investigation determined that USSS agents used an internal email system to distribute to their colleagues a screenshot of a database record containing sensitive PII. This PII was also leaked to two media outlets. The information, such as Congressman Chaffetz's social security number and date of birth, was from September 2003 when he applied for employment with USSS. OIG concluded that the vast majority of USSS personnel who accessed

[2] U.S. Congressman Jason Chaffetz is the Chairman of the House Committee on Oversight and Government Reform. This committee oversees government agencies including the USSS.
[3] Memorandum from DHS Inspector General John Roth to Secretary Johnson and USSS Director Clancy, *Investigation into the Improper Access and Distribution of Information Contained Within a Secret Service Data System* (September 25, 2015).

Congressman Chaffetz's record did so in violation of the *Privacy Act*,[4] as well as DHS policy and *USSS IT Rules of General Behavior*.[5]

Prior Related OIG Report and Testimony

In a 2011 report, the OIG discussed numerous challenges USSS faced in its IT management and the need to strengthen the USSS CIO's IT investment authority.[6] The report recommended that USSS develop an information technology staffing plan, formalize the IT Executive Steering Committee, and provide its CIO with agency-wide information technology budget and investment review authority. The USSS Assistant Director, Office of Professional Responsibility disagreed with the findings and recommendations from the report, stating that the report does not meet the objectives of the audit and that it disregards the details of the actions taken and the necessary management decisions made to staff and resource the Information Integration and Transformation program while continuing to execute IT operations. Also, the Assistant Director stated that the report disregards the collaboration and coordination between the USSS and the Department.

Additionally, on March 19, 2013, the DHS Deputy Inspector General testified before the house Committee on Homeland Security regarding IT management issues and challenges that the Department faces.[7] In his statement, the Deputy Inspector General discussed USSS' need to "provide the CIO with agency-wide IT budget and investment review authority to ensure that IT initiatives and decisions support accomplishment of the USSS and department-wide mission objectives."

We conducted the current audit to determine whether adequate controls and data protections were in place on systems to which MCI data were migrated, as a follow-up to the investigation regarding unauthorized access and disclosure of Congressman Chaffetz's sensitive PII.

[4] 5 United States Code (U.S.C.) § 552a.
[5] *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, March 2012; *USSS Information Technology (IT) Rules of General Behavior*, IRM-10(03), April 23, 2007.
[6] *U.S. Secret Service's Information Technology Modernization Effort*, OIG-11-56, March 2011.
[7] *DHS Information Technology: How Effectively Has DHS Harnessed It To Secure Our Borders and Uphold Immigration Laws?,* March 2013.

## Results of Audit

USSS did not have adequate protections in place on systems to which MCI information was migrated. USSS IT management was ineffective, including inadequate system security plans, systems with expired authorities to operate, inadequate access and audit controls, noncompliance with logical access requirements, inadequate privacy protections, and over-retention of records.

These problems occurred because USSS has not consistently made IT management a priority. The USSS CIO lacked authority for all IT resources and was not effectively positioned to provide necessary oversight. Inadequate attention was given to updating USSS IT policies to reflect processes currently in place. High turnover and vacancies within the Office of the CIO meant a lack of leadership to ensure IT systems were properly managed. In addition, USSS personnel were not adequately trained to successfully perform their duties.

USSS initiated steps in late 2015 to improve its IT program, including centralizing all IT resources under a full-time CIO and drafting plans for an improved IT governance framework. However, until these improvements are implemented and can demonstrate effectiveness, USSS systems and data we reviewed will remain vulnerable to unauthorized access and disclosure, and the potential for incidents similar to what the OIG investigated in 2015 will remain.

## Ineffective Systems and Data Management

USSS did not have adequate protections in place on systems to which MCI information was migrated. Specifically, we found inadequate system security plans, systems with expired authorities to operate, inadequate access and audit controls, noncompliance with logical access requirements, a lack of privacy protections, and over-retention of records.

### Inadequate System Security Plans

Essential USSS system security plans were inaccurate, incomplete, or in one case, non-existent. *DHS Sensitive Systems Policy Directive 4300A* requires the system owner or designee to develop and maintain such a document, referred to as a System Security Plan (SSP), for each Federal information system in use. The purpose of this documentation is "to provide an overview of the security

requirements of the system and describe the controls in place or planned for meeting those requirements."[8]

However, our review identified several deficiencies in USSS' security plans. Specifically, using NIST Special Publication, *Guide for Developing Security Plans for Federal Information Systems*, as criteria, we examined the SSP for each system replacing the MCI application to ensure it included, at a minimum, the following information:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description and Purpose;
- System Environment;
- System Interconnection;
- Laws, Regulations, and Policies affecting the system;
- Minimum Security Controls; and
- Completion and Approval Dates.

We determined that many of the plans were missing key items. For example, not all required security controls, such as access and auditing controls, were included in the plans. In addition, some of the controls listed in the plans were not actually present on the systems. An Authorizing Official was not listed in one of the plans. According to NIST, the authorizing official (or designated authority) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. Further, a number of the plans were not signed and dated under the section Information System Security Plan Approval to grant approval for the plan. One of the systems did not have a documented SSP, as required by *DHS Sensitive System Policy Directive 4300A*.

Moreover, the accuracy of some of the plan documentation was an issue. Some of the plans incorrectly listed system security personnel in positions they no

[8] The National Institute of Standards and Technology (NIST) publication, *Guide for Developing Security Plans for Federal Information Systems,* provides guidance on creating and maintaining an up-to-date SSP for each information system in use by the agency.

longer held, making it unclear as to who to contact in case of an incident or system performance issue. According to NIST, "A designated system owner must be identified in the system security plan for each system. This person is the key point of contact for the system and is responsible for coordinating system development life cycle activities specific to the system. It is important that this person have expert knowledge of the system capabilities and functionality."

Without these key SSP items in place, USSS had no reasonable assurance that mission-critical case management and investigative information was properly maintained and protected. In addition, those relying on the system to protect their identities (e.g., informants) or PII (e.g., information on applicants seeking employment with the agency) could have no assurance of proper data maintenance or protection against unauthorized disclosure, access, or theft.

Without complete and accurate documentation, authorizing officials lack information necessary to make credible risk-based decisions that the protections assigned to each information system were adequate and effective. For example, authorizing officials review SSPs to determine whether adequate security protections, such as access and auditing controls, are implemented for a system. This serves as a basis to determine whether a system should be authorized to operate.

**Systems with Expired Authorities to Operate**

USSS was operating systems without valid authorities to operate (ATO). According to NIST, an ATO is an official management decision given by a senior organizational official to authorize operation of an information system. An ATO explicitly accepts the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. *DHS Sensitive Systems Policy Directive 4300A* prohibits components from operating systems with sensitive information without ATOs.

As shown in table 1, two of the five systems we examined (FIRS and CLEAR) were operating with expired ATOs.

**Table 1: Authority to Operate Status for Systems Reviewed**

| System Name | ATO Status |
|---|---|
| Field Investigative Reporting System (FIRS) | Expired 8/22/2015 |
| Protective Threat Management System (PTMS) | Valid until 9/03/2018 |
| Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR) | Expired 3/12/2016 |
| Electronic Case Management System (eCase) | ATO memo not provided |
| Electronic Name Check System (eCheck) | Valid until 8/31/2018 |

*Source:* DHS OIG analysis of USSS documentation and auditee statements

We requested USSS to provide documentation that eCase has a valid ATO. However, USSS officials stated that eCase was a new system and the ATO was not completed. In April 2016, USSS officials stated that eCase was placed within the new Human Capital Management System as part of a USSS-initiated and self-described "system and application inventory overhaul."

Where information systems lack valid ATOs, USSS has no reasonable assurance it has implemented effective controls to protect the sensitive information stored and processed on these systems.

**Inadequate Access and Audit Controls**

USSS had not implemented adequate access and audit controls for information systems we reviewed, significantly impeding its ability to reconcile system events with the responsible individuals. NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, issued in April 2013, provides guidance for implementing access controls and audit controls for information systems supporting the Federal Government. Further, the *Federal Information Security Modernization Act* (FISMA)[9] requires agencies to secure its IT systems through the use of cost-effective management, operational, and technical controls.

[9] Public Law 113-283, December 18, 2014.

Access Controls

USSS policies for access controls were outdated. NIST publication 800-53 states that organizations should review and update access control policies and procedures. However, USSS access control policies were last updated on August 7, 2003. As such, it was not clear who should have access to the sensitive information retained on the USSS systems we reviewed. The outdated policies did not accurately reflect the current operational and technical environment.

Further, USSS access control policies did not address the principle of least privilege that requires each user of a system to be granted the most restrictive set of privileges needed for performance of authorized tasks. According to USSS personnel, 5,414 employees had access to the legacy MCI application data before it was retired in July 2015. One of the key deficiencies of the MCI application was that once a user was granted access, the user had access to all data within MCI regardless of whether it was necessary for his/her role. By not properly implementing least privilege policies for its information systems users, USSS lacked the means to protect against potential unauthorized access, disclosure, modification, or destruction of mission-critical information or PII.

According to the Deputy Chief Information Security Officer (CISO), USSS anticipated establishing an organization-wide process to review all privileged users with elevated access to information systems to ensure that they had the appropriate access for performing their job functions. By auditing these privileged accounts, USSS would be able to verify that users with elevated access commensurate with their current job functions had been approved.

In addition, we conducted onsite technical testing, confirming that user accounts accessing high-impact systems were not configured as required for automatic logout after a specified amount of inactivity and the number of concurrent user sessions was not limited (to one). Through interviews with USSS personnel and reviews of system documentation, we concluded that inactive user accounts were not disabled after a predetermined 45-day timeframe, usage conditions for high-impact systems had not been defined, and not all USSS systems ensured automated session terminations. During our audit fieldwork, USSS personnel stated they were in the process of implementing these controls. However, the existing deficiencies increased the likelihood that a user could gain unauthorized access to sensitive information, compromising the confidentiality, integrity, and availability of that information.

Audit Controls

Audit controls were not fully implemented, hindering USSS' ability to detect unusual user activities, or provide appropriate response to potential or actual security risks, attacks, or anomalies. For example, audit and accountability policies were out of date, last updated on January 6, 2006. This was in noncompliance with NIST publication 800-53, which states that organizations should review and update audit and accountability policies and procedures. Policies need to be current for employees to know what is expected to effectively perform roles and responsibilities. The policies also need to be pertinent to the systems and environment to effectively address the security required for each system.

Further, based on our interviews with USSS personnel and a review of system documentation, and despite NIST publication 800-53 guidelines, we identified systems for which USSS had not defined types of system-specific events that should be audited. During our December 2015 fieldwork, USSS communicated that personnel with system security responsibilities were in the process of identifying system-specific audit events to support appropriate incident response in case of security incidents or threats.

In addition, contrary to the NIST requirements, not all USSS systems had an automated audit event analysis and reporting capability designed to alert responsible system security personnel of potential or actual security anomalies or attacks. One legacy system was not able to support auditing capabilities at all. USSS personnel stated the system was developed prior to USSS implementing auditing requirements across all systems. USSS officials stated that they had plans to replace the legacy system with a new system with auditing capabilities.

**Noncompliance with Logical Access Requirements**

USSS had not fully implemented Personal Identity Verification (PIV) cards for logical access to USSS IT systems as required by the Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, approved August 2004. This policy established a government-wide standard for secure and reliable forms of identification for Federal employees and contractors. NIST developed Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors*, to satisfy HSPD-12 by requiring authentication of an individual's identity for physical and logical access to security-sensitive buildings, computer systems, and data. These requirements

are aimed at enhancing security, reducing identity fraud, and protecting personal privacy.

However, as of November 2015, we identified the following USSS deficiencies:

- 2.87 percent of privileged users were not using PIV to access USSS information systems.[10]
- 99.84 percent of non-privileged users were not using PIV cards to access USSS information systems.

Table 2 provides a breakdown of USSS PIV compliance.

**Table 2: Breakdown of USSS PIV Compliance**

| **Privileged Users** | | | | | |
|---|---|---|---|---|---|
| | **PIV Assigned** | **Total Employees** | **Percentage** | **PIV Not Assigned** | **Percentage** |
| Federal Employees | 99 | 105 | 94.29% | 6 | 5.71% |
| Contractors | 104 | 104 | 100% | 0 | 0% |
| **Totals** | **203** | **209** | **97.13%** | **6** | **2.87%** |
| **Non-Privileged Users** | | | | | |
| | **PIV Assigned** | **Total Employees** | **Percentage** | **PIV Not Assigned** | **Percentage** |
| Federal Employees | 8 | 6338 | 0.13% | 6330 | 99.87% |
| Contractors | 3 | 400 | 0.75% | 397 | 99.25% |
| **Totals** | **11** | **6738** | **0.16%** | **6727** | **99.84%** |

*Source:* DHS OIG analysis of USSS documentation and auditee statements

According to USSS personnel, technical and resource challenges prevented USSS from fully implementing PIV cards. For example, as of December 2015, 58 open vacancies rendered USSS unable to dedicate full-time staff to the deployment and configuration of PIV cards. In addition, compatibility issues with older IT systems hindered PIV implementation. Other reasons included not establishing digital identities and credentialing, and not identifying access

[10] Privileged users have accounts with privileges that grant them greater access to IT resources than non-privileged users have. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators.

management information necessary to successfully implement PIV cards. Given these challenges, USSS hired a full-time contractor in October 2015 to assist with the implementation of PIV cards as required by HSPD-12.

PIV implementation provides an added layer of security and stronger authentication to access information systems than traditional user name and password allows. By not fully implementing PIV cards, USSS was hindered in its ability to limit system and data access to only authorized users with a legitimate need. In addition, it decreased the ability of responsible personnel to trace operational events, security incidents, and criminal activities to the person of origin.

**Lack of Privacy Protections**

USSS was not compliant with privacy protection requirements for its information systems. Privacy protections are required per NIST Special Publication 800-53, as of April 2013, and include administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling, processing, storing, and transmitting of PII.

We reviewed 8 of 26 NIST privacy controls for the five systems containing MCI data. Those controls included documentation and processes that dealt with USSS' ability to adequately monitor and audit systems containing PII, retain and dispose of privacy records, train employees on their specific roles and responsibilities related to privacy, maintain an inventory of PII, and use and disclose PII (both internally and externally) in an acceptable manner. We selected these controls based on USSS' statutory requirement to safeguard PII in line with its organizational mission.

Privacy Documentation

USSS privacy documentation was incomplete, not up to date, or missing documented assessments on how privacy controls were implemented. The *E-Government Act of 2002*[11] and *DHS 4300A Sensitive Systems Handbook* requires an agency to maintain privacy documentation for any information system that collects, maintains, and disseminates PII. Privacy documentation includes a Privacy Threshold Analysis (PTA), a Privacy Impact Assessment (PIA), and provisions for privacy controls within the SSP.[12] While both

[11] Public Law 107-347, December 17, 2002.
[12] The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new information system is being developed or an existing system is significantly modified. A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected,

documents should identify which privacy controls are in place on any information system that collects, maintains, and disseminates PII, the SSP is for internal agency use, while the PIA is for external use and is a method for USSS to inform the public about its privacy practices.

We requested USSS provide an SSP for each of the five systems that were part of the scope of this audit. Only four SSPs were provided, and we determined that all four were incomplete, as each was missing documented assessments describing how selected NIST privacy controls were implemented on its applicable system. Further, some of the system PIAs had not been updated since 2012 and 2013, indicating that USSS had not re-assessed these PIAs to reflect the new privacy data risks when the MCI data was migrated to the non-mainframe environment in 2015.

System owners and Information System Security Officers (ISSO) indicated they were unaware of the requirements for documenting privacy controls on information systems nor had they received guidance from the DHS Chief Privacy Officer or the USSS Privacy Officer on how these requirements should be documented. According to *DHS Sensitive Systems Policy Directive 4300A*, the DHS Chief Privacy Office is responsible for leading and coordinating efforts to implement privacy controls at USSS. This coordination could include defining the roles and responsibilities of component system owners and ISSOs regarding privacy documentation. The DHS Chief Privacy Officer is also responsible for issuing an approval signifying a system is in compliance with privacy requirements. This approval process should include a review of system documentation, such as the SSP, and the PIA to verify they accurately reflect the status of privacy controls. Without this approval, a system should not be issued an ATO.

Lacking complete and up-to-date system documentation, the DHS Chief Privacy Officer cannot make a valid determination to approve a system, signifying compliance with privacy requirements. Further, without an up-to-date PTA and/or PIA, the public, especially those stakeholders with an interest in how USSS collects, maintains, and disseminates privacy data, does not have a reasonable assurance that actions taken to protect their PII are valid.

---

stored, and shared. PIAs are required (as determined by the PTA) whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and Program Manager.

Privacy Processes

USSS did not develop and publish component-specific policies and procedures to comply with DHS policy. According to the DHS Privacy Office's *Guide to Implementing Privacy*, components are responsible for developing and implementing component-specific privacy policies and procedures that comply with the department-level guidance.[13] These USSS policies and procedures should address required roles and division of responsibility between USSS and DHS Privacy Office personnel for implementing, monitoring, and assessing privacy protections. In addition, role-based training should provide USSS personnel with the guidance needed to properly implement privacy protections.

The responsible system owners and ISSOs were not aware of their responsibilities for the documentation and implementation of the required privacy protections on USSS systems. Further, personnel stated they were not aware of USSS component-specific privacy policy detailing roles and responsibilities for protecting PII.

The USSS Privacy Officer stated it was challenging to maintain a working relationship with the Office of the Chief Information Officer (OCIO) to develop the required privacy documentation. This was due to key personnel vacancies and high rate of turnover within OCIO. In addition, staff within the USSS Office of Chief Information Security Officer required additional training on documenting privacy requirements.

Without effective privacy processes and policies in place, personnel with system security responsibilities lacked guidance on their respective roles and responsibilities for ensuring proper privacy protections on USSS information systems. Such protections can decrease the risk of unauthorized access to PII. Breaches can be serious, resulting in identify theft or personal harm to employees, their families, informants working for USSS, or subjects of USSS investigations.

[13] According to the DHS Privacy Office, *Guide to Implementing Privacy* (Version 1), "[c]omponent Privacy Officers and [privacy points of contact] develop component-level privacy policies as needed to reflect and further the mission of the component, ensuring that privacy policies are consistent with the DHS Privacy Office policies and the [Fair Information Practice Principles (FIPPs)]. Such policies often address specific mission roles or programs" and "can inform development of DHS-wide policies. The [DHS Privacy] Office reviews privacy policies and guidance developed by component Privacy Officers and [privacy points of contact] to ensure consistency in privacy policy across the Department."

Privacy Leadership

USSS did not comply with a DHS requirement to designate a full-time component privacy officer reporting directly to the USSS Director. On June 5, 2009, the DHS Deputy Secretary issued *DHS Memorandum Designation of Component Privacy Officers* directing 10 DHS components, including USSS, to each designate a senior-level Federal employee as a full-time Privacy Officer reporting to the Component Head. The memorandum states that each component's designee would serve as the DHS Chief Privacy Officer's main point of contact for implementing privacy requirements. Further, the components' Privacy Officers were to possess experience and background in privacy and receive adequate support and resources to complete their duties effectively.

We found that the USSS Privacy Officer did not report directly to the USSS Director. Additional layers in the management chain restricted the USSS Privacy Officer's access to the Component Head. Specifically, the USSS Privacy Officer position was aligned under the Freedom of Information Act and Privacy Branch, which reported to the Liaison Division, which reported to the Assistant Director of the Office of Government and Public Affairs. This Assistant Director, in turn, reported to the Deputy Director, who reported to the USSS Director. According to USSS officials, the USSS Privacy Officer attended regularly scheduled meetings with the Assistant Director of the Office of Government and Public Affairs to keep abreast of privacy issues.

Fifty percent of the USSS Privacy Officer's duties related to *Freedom of Information Act* (FOIA)[14] requirements. Thus, the Privacy Officer was not available full time to monitor USSS compliance with all Federal privacy laws and regulations; implement corrective, remedial, and preventative actions to ensure privacy protections; draft privacy documents; and carry out other privacy-related responsibilities.

The lack of a full-time, dedicated USSS Privacy Officer reporting directly to the USSS Director increased the likelihood that privacy requirements would continue to not be fully addressed. A lack of transparency or outdated reporting on how USSS collects, maintains, and uses PII could tarnish the component's reputation and credibility with the public. This, in turn, could result in unnecessary legal liabilities.

[14] 5 U.S.C. § 552.

**Over-Retention of Records in Violation of the Privacy Act**

USSS retained job applicant data on information systems longer than was relevant and necessary to accomplish an agency purpose, in violation of the *Privacy Act*.[15] USSS compiles records on individuals who apply for employment with the agency, including rejected applicants. These records typically contain sensitive information covered by the *Privacy Act*.[16] Under the *Privacy Act*, each agency must "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[17] Thereafter, when information ceases to be relevant or necessary, the record should be expunged.[18] The *Privacy Act* also requires each agency to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[19]

Our review of CLEAR and eCase, two USSS systems to which MCI data were migrated, revealed that job applicant records were being retained in violation of the *Privacy Act*. From CLEAR, we obtained screen prints of the records of many "rejected" and "no longer interested" applicants that were more than 5 years old, including records that were up to 14 years old. We also determined that, notwithstanding OIG's determination that most USSS personnel who accessed Congressman Chaffetz's record did so in violation of the *Privacy Act*, as of November 2015, *Privacy Act* protected information from Congressman Chaffetz's 2003 application for employment with the USSS was still retained in both CLEAR and eCase, and therefore was still susceptible to access by USSS personnel. CLEAR contained Congressman Chaffetz's name, social security number, race, the type of position to which he applied, and the status of his application. eCase also contained Congressman Chaffetz's name, social security number, race, and the status of his employment application, as well as the date and place of his birth. According to the USSS Information Technology

[15] 5 U.S.C. § 552a(e)(1).
[16] The Privacy Act protects records containing "information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4).
[17] 5 U.S.C. § 552a(e)(1).
[18] *See Instructions for Complying with the President's Memorandum of May 14, 1998*, OMB Memorandum 99-05, Attachment B (Privacy and Personal Information in Federal Records), *available* at https://www.whitehouse.gov/omb/memoranda_m99-05-b/.
[19] 5 U.S.C. § 552a(e)(10).

Operations Division, Congressman Chaffetz's record and corresponding PII were deleted from CLEAR on December 29, 2015, and from eCase on January 5, 2016. Additionally, on January 11, 2016, USSS officials advised us that they were working towards implementing the new 2 year/5 year retention protocol for USSS information systems, discussed further under "Delayed Adherence to New Records Retention Standards," which USSS anticipated would be a time-consuming process. As such, USSS could not provide reassurance that other applicants' records and corresponding PII had been expunged from CLEAR and eCase. Therefore, the records of many other applicants remain susceptible to access and disclosure in violation of the *Privacy Act*.

It was reasonable for USSS to retain Congressman Chaffetz's background investigative information for some time after he submitted his application in September 2003, consistent with the *Privacy Act* provision allowing an individual access to his records and the opportunity to correct any inaccuracies in them.[20] However, it was not reasonable to maintain this information for more than 10 years after Congressman Chaffetz submitted his application, and therefore, the continued retention of his records violated the *Privacy Act*. Similarly, it was reasonable for USSS to retain the records of other "rejected" or "no longer interested" applicants for a period of time after they submitted their applications but not reasonable to maintain this information for up to 14 years thereafter. Although the *Privacy Act* does not define a period of time after which information is no longer relevant or necessary, a *Privacy Act* System of Records Notice issued by the Office of Personnel Management and referenced on the USSS job applicants website suggests a much shorter retention period for job applicant records: 1–2 years for most records and a maximum of 5 years for certain records.[21]

During this audit, USSS provided documents showing that USSS was operating with the understanding that a 20-year retention period had been prescribed for these records under a USSS-specific records disposition authority approved by the National Archives and Records Administration (NARA) in 1982. USSS also provided documents demonstrating that with NARA's assistance, the USSS Chief Records Officer had attempted to understand why the records disposition authority had provided such a lengthy retention period for applicants' background investigation records. Based on information provided by NARA, the USSS Chief Records Officer concluded that the historical decision to retain these records for 20 years "was likely just precautionary" and the reasoning

[20] *See* 5 U.S.C. § 552a(d).
[21] *See* "Privacy Act Statement for Applicants" at http://www.secretservice.gov/join/apply/privacy-act/; OPM GOVT-5 System of Records Notice (SORN), *Recruiting, Examining, and Placement Records*, 79 Fed. Reg. 16,834, 16,837 (March 26, 2014).

was no longer valid. However, the OIG has concluded that retention of such records for 20 years as a "precautionary" measure was not a reasonable basis to maintain the records, "relevant and necessary" to an agency purpose, and therefore violated the *Privacy Act*.

Further, USSS' inclusion of Congressman Chaffetz's record in the MCI application and later in CLEAR and eCase (electronic data systems accessible to USSS personnel) violated the requirement for an agency to establish "safeguards to insure the security and confidentiality" of *Privacy Act* records and prevent "threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[22] USSS did not institute safeguards to limit access to PII contained in the MCI, which allowed USSS employees to search for and view Congressman Chaffetz's record, notwithstanding whether doing so was within the scope of their official duties.

**Delayed Adherence to New Records Retention Standards**

In addition to violating the *Privacy Act*, maintenance of historical applicant data in USSS' data systems violated newer records retention rules. Our review determined that before October 1, 2015, USSS retained job applicant data for 20 years based on a USSS-specific records disposition authority approved by NARA in 1982. Effective October 1, 2015, however, USSS began to follow NARA's General Records Schedules (GRS-1 and GRS-18). As a result of this change, USSS' rejected applicant files are now managed under the following protocols:

- Records for those applicants that are rejected during the suitability determination process (before a formal background investigation is opened) are to be held for 2 years after the case file is closed, then destroyed.

- Records for those applicants that are rejected after a formal background investigation is opened are to be held until notification of death or no later than 5 years after the termination of the applicant relationship, whichever is applicable. The records should then be destroyed.

USSS subject matter experts acknowledged that systems holding applicant records were not meeting the 2 year/5 year retention requirements in existence at the time of our January 2016 fieldwork. They indicated that USSS was working to address these issues.

[22] 5 U.S.C. § 552a(e)(10).

These retention problems could be attributed to USSS challenges in adhering to records management requirements and protocols. According to USSS personnel, the requirements included reviewing applicant record files on a case-by-case basis to identify records that did not meet the current retention protocol. This was a manual and, therefore, labor-intensive and time-consuming process.

According to the Chief Records Officer, identifying and disposing of records that have surpassed required retention requirements would also require continual record-by-record reviews. Such reviews would entail verifying that no overriding legal preservation requirement or "freeze order" (due to an active criminal case, or litigation, associated with an individual person or class) existed, which would mean retaining the records until the related litigation or investigation is resolved.

Technical challenges with records retention requirements also existed. For example, discussions with USSS system security personnel disclosed that four of the five information systems we reviewed did not include controls to automatically remove data at the end of the retention period or alert of the need to do so.

By retaining sensitive or personally identifiable applicant records longer than authorized, USSS risked information being accessed by unauthorized employees and contractors in violation of the *Privacy Act*. This could result in internal or external disclosure, abuse, or misuse of the information.

## IT Management Has Not Been a USSS Priority

The systems and data management problems we identified can be attributed to the lack of priority that USSS historically has placed on IT management. Our audit disclosed that USSS OCIO lacked authority for all IT resources and was not effectively positioned to provide necessary oversight. Inadequate attention was given to updating USSS IT policies to reflect processes currently in place. A number of critical IT management positions within OCIO were vacant. In addition, USSS personnel had not received adequate training to successfully perform their responsibilities.

In December 2015, USSS initiated steps to improve its IT program management, including centralizing all IT resources under a full-time CIO and developing plans for an improved IT governance framework. However, it will take time for these improvements to be fully implemented and demonstrate effectiveness in safeguarding sensitive systems and data.

**Limited CIO Responsibility and Authority**

Our audit disclosed that USSS CIO lacked the placement and authority needed to provide effective oversight of IT resources agency-wide. The *Clinger-Cohen Act* requires that CIOs have statutory responsibilities to facilitate effective IT governance and management of Federal IT Programs.[23] According to Federal guidance, agencies are required to implement IT governance structures to ensure effective management of IT resources.[24] Additionally, the Office of Management and Budget (OMB) issued guidance in 2011 and 2013 aimed at increasing CIO authority in areas such as IT management.[25]

Historically, USSS CIO has not been effectively positioned to provide needed IT oversight and authority. In 1988, USSS established the Information Resources Management Division (IRMD) under USSS OCIO to develop, provide, and manage IT to support the investigative and protective operations and associated administrative functions of the agency. At some point, a Senior Executive Service official had the dual role of CIO and IRMD Chief. According to a former Acting CIO, IRMD staff expressed concerns that the CIO was failing, as he was not effective in developing the internal and external coalitions and relationships needed to succeed in that environment. As a result, IRMD and OCIO were split into two separate entities in 2006. Senior USSS management decided to remove the CIO from over IRMD and place the CIO position under a USSS Deputy Assistant Director. The CIO's deputy, a Special Agent-in-Charge, was subsequently placed in charge of IRMD.

As a result of this 2006 decision, the CIO no longer had oversight and authority over USSS agency-wide IT. Instead, IRMD was given the responsibility for developing, providing, and managing IT within the agency. This included supporting and maintaining IT network infrastructure communications; IT programs, plans, and policies; and IT administration, property management, security engineering, and application development. Almost all OCIO employees remained in IRMD.

According to a former Acting USSS CIO, the repositioned CIO struggled to rebuild the office after the split and was unable to make a valid case to senior

[23] 40 U.S.C. § 1401 *et seq*.
[24] *National Defense Authorization Act for Fiscal Year 1996*, Public Law 104–106, February 10, 1996, and *Omnibus Consolidated Appropriations Act, 1997*, Public Law 104–208, September 30, 1996; OMB Circular A-130 (Revised), Management of Federal Information Resources, November 28, 2000.
[25] OMB Memorandum M-11-29, *Chief Information Officer Authorities*, August 8, 2011; OMB Memorandum M-13-09, *FY 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, March 27, 2013.

management to obtain the funding and staffing needed to do so. A new CIO was subsequently hired and, although more knowledgeable of laws and policies governing CIO authorities (e.g., the *Clinger-Cohen Act*), still faced organizational opposition to rebuilding OCIO into a functional capability. The former Acting USSS CIO went on to say that personalities and clashing egos hindered this CIO's efforts as well. The former Acting USSS CIO concluded that splitting IT into two groups was not an effective decision and did not demonstrate good business acumen. According to the former Acting USSS CIO, the split resulted in giving a law enforcement Special Agent-in-Charge, with limited IT management and leadership experience, responsibility for a technology division with a diverse portfolio of IT services, programs, acquisitions, and operational elements. In a culture where agents were reluctant to relinquish control, the split contributed significantly to a lack of IT leadership and inability to build a strong technology program within USSS.

Once he became Acting CIO in April 2015, the former official faced the same challenges as his predecessors: inadequate oversight of IT spending and a depleted staff. USSS also had no CISO as required by DHS policy and had to fulfill these responsibilities. Due to the limited staff, contract employees were required to not only respond to help desk calls for IT support, but carry out other administrative and program review activities.

In March 2011, OIG reported on these conditions, concluding that the USSS had not positioned its CIO with the necessary authority to review and approve IT investments.[26] Further, the CIO was not a member of the USSS Director's management team and therefore did not play a significant role in overseeing IT systems development and acquisition efforts.

USSS acknowledged these issues still existed at the time of our 2015 audit. In an email dated January 14, 2016, the Assistant Division Chief of IT Governance and Accountability stated that "the CIO program had little to no funding, little authority, and did not have control over USSS IT spending from inception until December 2015." As such, there was no central authority within USSS to ensure adequate controls and security protections were in place for USSS IT personnel, systems, and data.

**Lack of Focus on IT Policy Management**

Inadequate attention was given to keeping critical USSS IT policies updated to accurately reflect current IT processes. According to *DHS Sensitive Systems Policy Directive 4300A*, component CISOs are responsible for the development

[26] *U.S. Secret Service's Information Technology Modernization Effort*, OIG-11-56, March 2011.

and management of information security guidance and procedures unique to component requirements.

Based on our discussion with USSS officials, responsibility to review and update IT policies previously belonged to IRMD, but USSS no longer had a technical policy writer within IRMD to coordinate these efforts. The CIO was given the authority and responsibility to review and update all IT policies in December 2015. The CIO and the Assistant Division Chief of IT Governance plan to update these policies.

In the interim, we found that key guidance such as documentation describing the stages involved in an information system development (e.g., the system development lifecycle) dated back to 1992 when USSS was part of the Department of the Treasury, reflecting that IT was not a priority. Some policies had not been updated since USSS became part of DHS in March 2003 and policies do not reflect the current IT operating and technical environment. For example, *Account Management* policy IRM-12(01), dated August 7, 2003, contained references to the MCI mainframe application that was disassembled in 2015. Further, *Password Change Policy* IRM-12(03) referenced DHS policies and guidance from the year 2005. Those policies and guidance were superseded by the *DHS Sensitive Systems Policy Directive 4300A,* dated February 12, 2016, and did not reflect the most recent DHS guidance.

Table 3 provides the outdated USSS IT policies we found still in place at the time of our October 2015 fieldwork.

**Table 3: Outdated USSS IT Policies Identified**

| Policy Name | Last Updated | Description |
|---|---|---|
| IRM-07(02) – *The System Development Life Cycle* (SDLC) | 09/23/1992 | Establishes policy for USSS System Development Lifecycle Methodology for application systems development and maintenance. |
| IRM-09(01) – *Information Assurance Program* | 02/01/2003 | Establishes policy that identifies the information assurance roles and responsibilities of entities within and outside USSS. |
| IRM-10(03) – *Information Technology General Rules of Behavior* | 04/23/2007 | Establishes policy for rules of behavior for all individuals who use USSS computers, systems, and IT resources. |
| IRM-12(03) – *Access Controls* | 08/07/2003 | Establishes policy to implement technical controls for access to IT systems. |
| IRM-11(03) – *Information Assurance Training and Awareness* | 07/01/2002 | Establishes policy requiring development and implementation of an awareness and training program for information assurance. |
| IRM-12(04) – *Audit Trails* | 01/06/2006 | Establishes policy for defining requirements for USSS to conduct system audits. |
| IRM-12(01) – *Account Management* | 08/07/2003 | Establishes policy for USSS user account management. |
| IRM-12(02) – *Password Change Policy* | 03/31/2006 | Establishes policy for defining responsibilities of USSS employees for changing passwords used to access USSS IT systems and services. |
| IRM-12(13) – *Information Technology Patch Management* | 08/19/2005 | Establishes policy regarding patch management of IT computers and systems. |
| IRM-11(04) – *Media Controls and Labeling* | 10/22/2007 | Establishes policy requiring for media controls and labeling. |
| IRM-11(19) – *Standard Computer Image and Configuration* | 06/09/2005 | Establishes policy regarding the use of standard security configurations and standard personal computer images. |

*Source:* DHS OIG analysis of USSS documentation and auditee statements

Outdated IT policies leave the organization hindered in its ability to implement and enforce IT system security requirements. Further, outdated policies may

not clearly define current IT roles and responsibilities and reflect the current IT operational and technical environment.

**IT Staff Vacancies**

Key positions responsible for the management of IT resources and assets were not filled. According to *DHS Sensitive Systems Policy Directive 4300A*, critical roles should be filled to provide effective oversight and management of the organization's IT security program. However, some vacancies, just recently filled, had lasted for almost 1 year; other vacancies still existed at USSS. For example:

- **Chief Information Officer (CIO)**: From December 2014 to November 2015, USSS lacked a full-time CIO. Although an acting CIO was assigned in April 2015, there was no full-time CIO appointed until November 2015. *DHS Sensitive Systems Policy Directive 4300A* requires the CIO to develop and maintain the Information Security Program that includes information systems security and FISMA compliance.

- **Chief Information Security Officer (CISO)**: As of March 2015, USSS did not have a full-time CISO. An acting CISO departed in September 2015. *DHS Sensitive Systems Policy Directive 4300A* requires designation of a full-time CISO to implement and manage aspects of the information security program. Further, the CISO is responsible for areas such as serving as the principal advisor on information security matters, reporting to the CIO on matters relating to the security of information systems, and overseeing facets of the information security program. According to USSS personnel, as of January 2016, USSS leadership had interviewed several individuals for the CISO position. The top candidate declined the offer, so USSS began reevaluating the remaining candidates. USSS hired a Deputy CISO who started work on January 11, 2016.

- **Information System Security Manager (ISSM)**: USSS did not have a full-time ISSM. On April 2016, the Deputy CISO was not aware of USSS ever having a formal ISSM. DHS policy states that ISSMs play a critical role in ensuring that the organization's information security program is implemented and maintained. Further, ISSMs are responsible for areas such as overseeing certain aspects of the component's information security program, validating component information system security reporting, and testing the security of information systems periodically.

Further, a significant number of vacant staff positions existed in OCIO. As described by officials we interviewed, OCIO operated with limited personnel

prior to the December 2015 reorganization. As of December 2015, OCIO reported having 139 employees and 58 vacancies, which is a staff vacancy rate of 29 percent.

According to USSS officials, their inability to hire staff was attributed to the lengthy hiring process, which required background checks, including polygraphs for Federal employment. All USSS employees must hold a top secret security clearance, which requires a background investigation. Additionally, a polygraph is required for some positions, including many administrative, professional, and technical positions in the OCIO. Potential hires frequently accepted other jobs while waiting to be granted clearances. In some cases, selectees were not able to successfully pass polygraphs and complete background checks.

As a result, USSS relied heavily on contractors to fill IT security positions rather than on Federal employees. USSS background checks for contractors did not require polygraphs. However, contractor ISSOs stated they felt they were not getting sufficient guidance to perform their responsibilities. For example, during our interviews, they were not aware how to properly complete SSPs.

**Inadequate IT Training**

USSS personnel had not received adequate IT training. For example, not all employees and contractors completed mandatory IT security awareness, specialized role-based training, or privacy training. As a result, many employees lacked awareness of their specific roles and responsibilities in properly safeguarding mission critical data and promoting an effective information assurance framework within the organization.

IT Security Awareness Training

All USSS employees and contractors had not completed mandatory IT security awareness training, as required by *DHS Sensitive Systems Policy Directive 4300A* for all DHS personnel accessing DHS systems. This training is the primary method by which the USSS can inform employees about their roles and the expectations regarding information security. This includes basic instruction and guidance on how to protect information systems and sensitive data from internal and external threats.

For fiscal year 2015, we found that only 85 percent of USSS' employee population had completed the required IT security awareness training. USSS had a total of 6,307 Federal employees and 397 contractors. However, the total

number of Federal and contractor employees that completed mandatory training during fiscal year 2015 was 5,670.

Officials we interviewed stated that USSS employees and contractors did not all complete the mandatory IT security awareness training because it was not being enforced by USSS management.

Specialized Role-Based Training

USSS also had not enforced specialized role-based training for individuals with significant security responsibilities. For example, for some of the systems that we reviewed, system security personnel did not receive annual specialized security training for fiscal year 2015.

DHS requires that personnel and contractors with significant security responsibilities receive this specialized training annually. This training is designed to inform personnel with system security responsibilities with specific training tailored to assigned duties. The training would include role-based training that addresses management, operational, and technical roles and responsibilities.

When required specialized training is not provided, USSS cannot ensure that their personnel with significant security responsibilities have the appropriate skills and knowledge to properly administer and secure systems against potential attacks.

Privacy Training

USSS has not enforced mandatory privacy training for all employees. Such training was designed to raise employees' awareness of the importance of properly safeguarding privacy data, including acceptable methods for handling and sharing PII. As of fiscal year 2015, USSS had a total of 6,307 Federal employees. The number of employees that completed mandatory privacy training for fiscal year 2015 was 5,612, which is approximately 89 percent.

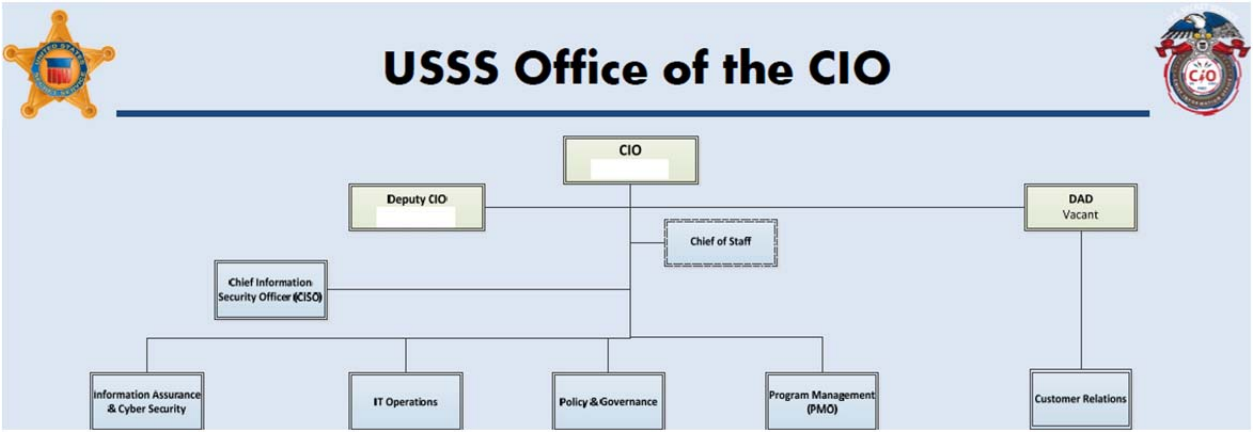
The DHS Privacy Office requires all employees and contractors to complete the annual DHS privacy training, entitled *Privacy at DHS: Protecting Personal Information* that meets OMB M-07-16 mandatory training requirements.[27]

[27] OMB Memorandum M-07-16, *Memorandum for the Heads of Executive Departments and Agencies*, May 22, 2007.

**Recent Steps to Improve IT Management**

USSS recently initiated steps to improve its IT management structure, which may give more priority to the leadership, policies, personnel, and training needed to ensure protections for sensitive systems and data. Specifically, in December 2015, the USSS Director announced agency-wide that IRMD was placed under OCIO, giving the CIO control of all IT assets. It aligned IRMD under OCIO with the intent to improve IT oversight and centralize all IT resources under the authority of the CIO. Additionally, it established five new divisions: (1) Information Assurance and Cyber Security, (2) IT Operations, (3) Policy and Governance, (4) Program Management, and (5) Customer Relations. Figure 2 shows the new OCIO organization chart.

**Figure 2: OCIO Organizational Structure as of December 2015**




*Source:* USSS, OCIO

On December 16, 2015, the USSS Director distributed an email to USSS personnel stating that "[e]ffective Sunday, December 20, 2015, IRMD will report to the CIO." Further, the email stated that "[t]his consolidation of all IT and communications functions under the CIO is being done to improve corporate oversight and investment control for enterprise IT spending and accountability, to establish management practices that ensure IT resources and delivered capabilities are consistent with the Service's mission, goals and programmatic priorities, and, to better conform with statutory requirements." In addition, the CIO communicated that other steps to address USSS' lack of effective IT management were underway, including developing plans for an improving IT governance framework.

These changes are initial steps to address the various IT deficiencies we identified. However, it will take time for these improvements to be fully

implemented and demonstrate effectiveness in safeguarding sensitive systems and data from unauthorized access and disclosure. For example, USSS still needs to staff OCIO with the appropriate subject matter experts, update policies and procedures to reflect the current USSS IT environment, and align them with DHS requirements. OCIO also must identify training gaps, develop new curriculums as needed, and ensure all employees complete the training as required.

## USSS Systems and Data Remain at Risk

For now, USSS has no reasonable assurance that its information systems are properly secured to protect Law Enforcement Sensitive case management information. USSS systems and data remain vulnerable to unauthorized access and disclosure. As discussed, contributing factors included inadequate system security plans, systems with expired authorities to operate, inadequate access and audit controls, noncompliance with logical access requirements, inadequate privacy protections, and over-retention of records. Such deficiencies increase risks to the confidentiality, integrity, and availability of mission-critical information systems and data.

Further, the potential for incidents similar to the Congressman Chaffetz breach of March 2015 remain. Insider threats present within the organization may be able to:

- steal, alter, or destroy mission critical data;
- export malicious code to other systems;
- install covert backdoors that would permit unauthorized access to data or network resources; or
- impact the availability of any information system's resources or networks.

Any loss, theft, corruption, destruction, or unavailability of Law Enforcement Sensitive data or PII could have grave adverse effects on the USSS' ability to protect employees or the general public. Table 4 provides examples of the negative impacts that could result if USSS case investigative information is obtained by unauthorized individuals, stolen, or destroyed.

**Table 4: Negative Impact of Unauthorized Disclosure of Law Enforcement Sensitive Data or PII**

| Action | Potential Adverse Effect |
|---|---|
| Unauthorized access to Confidential Source/Informant/ Cooperating Witness information | Loss or theft could result in the identification of certain individuals and potentially expose them to physical danger or more severe forms of retribution. |
| Unauthorized access to PII | Law Enforcement Sensitive data contain a great deal of PII pertaining to subjects and witnesses involved in criminal cases. Aside from liability for violating the *Privacy Act*, loss or theft of PII may lead to identity theft, fraud, coercion, or extortion. |
| Divulging sources and methods to parties other than those for whom they are intended | Unauthorized access could result in divulging component methods of conducting business, especially activities such as surveillances (human and technical), use of informants/undercovers, and warrant service. This could result in arming subjects with knowledge (intelligence) needed to circumvent being caught. |
| Compromised officer safety | Loss or theft of PII could divulge the identities and participation of certain law enforcement officers/agents (especially undercovers and case agents), thus exposing them to physical harm or more severe forms of retribution. |
| Unnecessary civil liability | Information that would not be releasable pursuant to the FOIA or the *Privacy Act* could lead to lawsuits that, even if dismissed in favor of the agency, tend to tie up resources and expose law enforcement agents/officers unnecessarily to legal liability, media, and possibly congressional scrutiny. |
| Continuity of law enforcement operations | Loss or corruption of Law Enforcement Sensitive data may prevent agents/officers from obtaining valuable criminal history/intelligence in performance of their jobs, and worse, hinder proper threat assessment of potentially violent or otherwise dangerous contacts. |

*Source:* DHS OIG, Office of Special Investigations

## Conclusion

USSS' primary mission is protecting the President, other dignitaries, and events, and investigating financial and cyber crimes to help preserve the integrity of the Nation's economy. This statutory responsibility leaves little, if any, room for error. As such, the systems and information supporting this mission must be managed in an efficient and secure manner.

USSS has much work to do to make IT a priority. This requires establishing and implementing an IT governance framework that addresses, at a minimum, the IT organizational and management deficiencies identified in this report. It also requires that USSS leadership fully understand and address the potential for insider risks, not only from system administrators and inadequately managed IT contractors, but also from employees and business partners.

In discussions, the new USSS CIO was aware of the severity of these issues and had begun formulating a strategic plan, including corrective actions plans to address long-standing IT deficiencies. Time will tell how effective these efforts prove in changing the USSS culture so that a premium is placed on ensuring a holistic information security program with effective technical, operational, and management controls.

## Recommendations

We recommend that the USSS Director:

**Recommendation #1:** Provide a plan for ensuring specialized training for all system owners and Information System Security Officers on their roles and responsibilities as well as the proper methods for documenting and validating system security plans, privacy controls, and system deficiencies in the plan of actions and milestones.

**Recommendation #2:** Provide a plan, including milestones and an estimated completion date, for ensuring that each USSS system has a valid authority to operate in accordance with DHS policy.

**Recommendation #3:** Provide a plan, including milestones and an estimated completion date, for fully implementing Personal Identity Verification cards as mandated for logical access to all USSS networks and information systems.

**Recommendation #4:** Provide a plan, including defined roles and responsibilities of the DHS Privacy Office, the USSS Privacy Office, and the

USSS Office of the Chief Information Officer for implementing privacy controls on all USSS systems.

**Recommendation #5:** Appoint a full-time, senior-level Privacy Officer reporting directly to the USSS Director to ensure compliance with DHS guidance for implementing privacy protections.

**Recommendation #6:** Provide a plan, including milestones and an estimated completion date, for ensuring compliance with the current USSS requirements and the National Archives and Records Administration's regulations for retention and destruction of applicant records.

**Recommendation #7:** Provide an information technology strategic plan, including milestones and an estimated completion date, outlining the responsibilities, resources, and initiatives needed to accomplish USSS goals and objectives.

**Recommendation #8:** Provide a plan and process for creating, reviewing, and updating information technology policies and procedures on a regular basis.

**Recommendation #9:** Provide a plan, including milestones and an estimated completion date, for addressing staff vacancies in critical information technology management positions, such as the Chief Information Security Officer.

**Recommendation #10:** Establish a repeatable process for ensuring that all USSS employees and contractors annually complete information security awareness, privacy, and role-based training.

Further, we recommend that the DHS Chief Privacy Officer:

**Recommendation #11:** Conduct a systematic review with recommendations for ensuring USSS compliance with DHS privacy requirements.

## USSS Comments

We obtained written comments on a draft report from the Director for USSS. We have included a copy of the comments, in their entirety, in appendix B. USSS concurred with OIG recommendations 1 through 10, and the DHS Privacy Office concurred with recommendation 11.

## OIG Analysis of USSS and DHS Privacy Office Comments

**Management Comments to Recommendation 1**
USSS concurs with recommendation 1. USSS Office of the Chief Information Security Officer in partnership with the USSS Privacy Office, DHS Privacy Office (PRIV), the Office of Training, and the James J. Rowley Training Center, is developing a specialized role-based training course for all system owners, administrators, and ISSOs. When completed, this course will be available via the USSS' Learning Management System and will include specific training objectives related to all Risk Management Framework steps, to include SSPs, privacy controls, and system deficiencies.

USSS will continue to follow all pertinent DHS, National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB) guidance when preparing authority to operate (ATO) related documents for SSPs, privacy controls, and Plan of Action and Milestones. USSS enters all ATO documentation into the DHS Information Assurance Compliance System.

The estimated completion date for this recommendation is December 31, 2016.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides documentation to support that the planned corrective actions are completed.

**Management Comments to Recommendation 2**
USSS concurs with recommendation 2. USSS follows the specific steps as set forth by DHS, NIST, and OMB guidance when preparing all the necessary documents for ATOs. Currently, the Field Investigative Reporting System (FIRS) and Protective Threat Management System (PTMS) have completed all of the RFM steps except the Security Control Assessment. The assessments for both of these systems are expected to be completed no later than mid-September 2016, and both systems should have a signed ATO letter shortly thereafter.

The eCheck system has completed all RFM steps and is pending the privacy reviews which are completed by both the USSS Privacy Office as well as PRIV.

After these privacy reviews are completed, eCheck will undergo the Security Control Assessment. USSS estimates that the Security Control Assessment for eCheck will be completed, and a signed ATO letter is expected shortly thereafter.

The Clearances, Logistics, Employees, Applicants, and Recruitment System (CLEAR) and Enterprise Case Management System (eCASE) have been combined and are now part of the Human Capital Management System (HCMS). Because it is a new system, HCMS is early in the RFM process. The main ISSO and system owner related steps are expected to be completed by late October 2016. Privacy reviews by both USSS and PRIV are expected to take place in November 2016, followed by the Security Control Assessment. The signed ATO letter for HCMS is expected shortly thereafter.

All USSS systems are expected to have a valid ATO no later than December 31, 2016. The estimated completion date for this recommendation is December 31, 2016.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides documentation to support that the planned corrective actions are completed.

**Management Comments to Recommendation 3**
USSS concurs with recommendation 3. USSS mandated the use of PIV card access. When the OIG's review began, USSS was in the process of deploying the necessary software changes in order to comply with Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. USSS accomplished that goal and are now 100 percent compliant, thanks in part to assistance from DHS. As of June 2016, USSS has fully implemented the mandate for PIV card access and usage to all networks and information services for employees and contractors. Documentation of this policy change will be sent to the OIG under separate cover.

USSS requested that the OIG close the recommendation.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides documentation of this policy change and supporting documentation that the USSS has fully implemented the mandate for PIV card access and usage to all networks and information services for employee and contractors.

**Management Comments to Recommendation 4**
USSS concurs with recommendation 4. The Acting Chief Information Security Officer will work with the individual system ISSO to complete a Privacy Threshold Analysis (PTA) for each system. The PTA will be sent to the USSS Privacy Office which will coordinate with appropriate CISO and operational program staff to evaluate the PTA and send it to PRIV for adjudication. PRIV will evaluate the PTA to determine whether a program, system and/or activity has privacy implications. Where there are privacy implications, controls and privacy compliance documentation will be developed and maintained as appropriate. The USSS Privacy Office in collaboration with the ISSO and operational program will draft all required privacy compliance documentation, and all privacy compliance documentation must be approved by PRIV. PRIV is responsible for determining and applying privacy controls during the privacy review stage of the ATO process.

The estimated completion date for this recommendation is December 31, 2016.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides documentation to support that the planned corrective actions are completed.

**Management Comments to Recommendation 5**
USSS concurs with recommendation 5. The USSS Chief Operating Officer will work with the DHS Chief Privacy Officer and others, as appropriate, to determine how best to fulfill the requirements of the Deputy Secretary's memorandum.

The estimated completion date for this recommendation is December 31, 2016.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides documentation to support that the planned corrective actions are completed.

**Management Comments to Recommendation 6**
USSS concurs with recommendation 6. As noted in the OIG report, specific USSS policy regarding retention and destruction of applicant records has been issued. The Management and Organization Division within the Office of Strategic Planning and Policy will develop a plan outlining additional activities, milestones, and estimated completion dates to support compliance with the current USSS policy and associated NARA regulations.

The estimated completion date for this recommendation is November 30, 2016.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides documentation to support that the planned corrective actions are completed.

**Management Comments to Recommendation 7**
USSS concurs with recommendation 7. In February 2016, the USSS released its Information Technology Strategic Plan for FY 2016 – FY 2021. The plan includes the CIO's Mission Statement, Vision Statement, and Strategic Goals and Objectives necessary for the USSS to address the changing needs of the agency and its workforce. A copy of the IT Strategic Plan will be sent to the OIG under separate cover.

USSS requested that the OIG close the recommendation.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides a copy of the USSS Information Technology Strategic Plan for FY 2016 – FY 2021 and the contents of the plan addresses the recommendation.

**Management Comments to Recommendation 8**
USSS concurs with recommendation 8. The Information Technology Governance and Accountability Program developed a robust policy production process for the OCIO effective July 2016. All policies from the OCIO are initiated and formalized utilizing this process and managed via a yearly review schedule. A copy of the IT Policy Update Process will be sent to the OIG under separate cover.

USSS requested that the OIG close the recommendation.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides a copy of the USSS IT Policy Update Process and the contents of the process addresses the recommendation.

**Management Comments to Recommendation 9**
USSS concurs with recommendation 9. Maintaining an optimally staffed OCIO is an ongoing, iterative process that will require sustained efforts. Filling vacant management positions in the OCIO is a current priority. The USSS is in the

process of reviewing resumes for the Deputy CIO position and re-soliciting applications for the CISO position.

The USSS Office of Human Resources has been tasked with recruiting and staffing open positions within the OCIO. As the OIG draft report noted, there are a variety of factors that make filling these vacancies particularly challenging. Through targeted recruiting, expansion of hiring authorities, and efficiencies in applicant processing, the USSS will be able to bring individuals with the necessary skills on board. Since the new CIO's arrival, the OCIO has increased to 226 authorized government full-time positions. Of the 41 current vacancies in the OCIO, 35 are in various phases of the hiring process. The USSS goal is to fill 80 percent of these vacancies by January 2017.

The estimated completion date is January 31, 2017.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides documentation to support that the planned corrective actions are completed.

**Management Comments to Recommendation 10**
USSS concurs with recommendation 10. The USSS requires all employees and contractors to complete Information Security Awareness training on an annual basis. The majority of training is completed in the Learning Management System, managed by the Office of Training, and is available to all USSS employees online. Through the Learning Management System, all employees are assigned training modules appropriate to their roles, permissions, and job functions. All USSS employees and contractors are required to take the "Privacy at DHS: Protecting Personal Information" course annually. All personnel in specific job series, which includes all law enforcement officers who use social media for operational purposes, are required to take "Operational Use of Social Media" training, which was developed by the USSS Privacy Office and Office of Chief Counsel.

An additional related training course, "Social Engineering Awareness and Prevention," was recently released via the Learning Management System and must be completed by all employees. The purpose of the course is to educate our workforce on the dangers of social engineering. Per DHS and OMB, the training is a mandatory annual requirement for all DHS employees.

The USSS verifies and ensures that employees remain current with required training in two ways. An employees's direct supervisor is able to review the status of Learning Management System courses assigned to that employee. An

employee's annual and semi-annual performance evaluations include first-line supervisory review and verification that all of their assigned training is current.

Additionally, each USSS office undergoes a compliance inspection every four years. The purpose of the compliance inspections is to verify that all offices are operating in accordance with USSS policy, procedures, and protocols. One aspect of the inspection is a review of the status of all employees' Learning Management System training requirements. Failure to keep current with all assigned training modules is noted by the Inspection Division team and may be included in that office's evaluation, which is distributed to the respective Assistant Director. Thus, managers are kept aware of the status of their personnel's mandatory training.

To improve and streamline all of our computer-based training, the USSS will migrate from the Learning Management System to the DHS Performance and Learning Management System (PALMS) on November 30, 2016. PALMS offers additional functionalities including the ability of supervisors to view real time status of employee completion of mandatory training as well as automated notifications and reminders.

Documentation of the training verification portion of the Compliance Inspection Checklist will be provided to the OIG under separate cover.

USSS requested that the OIG close the recommendation.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USSS provides supporting documentation that a repeatable process has been established to ensure that all USSS employees and contractors annually complete information security awareness, privacy, and role-based training.

**Management Comments to Recommendation 11**
DHS Privacy Office concurs with recommendation 11. PRIV will conduct a Privacy Compliance Review of the USSS. PRIV will determine the scope of the Privacy Compliance Review and develop an initial set of questions and document requests to submit to the USSS at the beginning of fiscal year 2017.

The estimated completion date for this recommendation is July 30, 2017.

**OIG Analysis**
We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until the DHS Privacy

Office provides documentation to support that the planned corrective actions are completed.

## Appendix A
## Objective, Scope, and Methodology

DHS 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.

We performed this audit as a follow-up to a September 2015 OIG investigation regarding USSS employees improperly accessing and distributing sensitive information on the agency's MCI mainframe system. Our objective was to determine whether adequate system and data protections were currently in place on any systems to which MCI information was migrated.

During the audit, we conducted technical security assessments on information systems to which the MCI data was migrated. The assessments included the following unclassified systems that contain PII:

- Field Investigative Reporting System (FIRS);
- Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR);
- Protective Threat Management System (PTMS);
- Electronic Name Check System (eCheck); and
- Electronic Case Management System (eCase).

We interviewed USSS personnel to determine their level of understanding with regards to policy implementation, rules of behavior, assigned roles and responsibilities, and the information security posture for the systems reviewed. Interviews were conducted with the following USSS personnel:

- Chief Information Officer;
- Deputy Chief Information Officer;
- Chief Privacy Officer;
- Chief Records Officer;
- Deputy Chief Information Security Officer;
- System Owners;
- Information System Security Officers;
- System Administrators; and
- Technical Subject Matter Experts.

We reviewed relevant USSS and DHS policies, selected system security plans, system artifacts that depicted system settings, training documentation, management plans, and other information.

We performed our fieldwork at the USSS Headquarters in Washington, DC.

We conducted this performance audit between September 2015 and March 2016 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate USSS' efforts to provide the necessary information and access to accomplish this audit. Appendix E contains major contributors to this report.

# Appendix B
# USSS Comments to the Draft Report

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

DIRECTOR

August 22, 2016

MEMORANDUM FOR: John Roth
Inspector General
Office of Inspector General
U.S. Department of Homeland Security

FROM: Joseph P. Clancy
Director

SUBJECT: Management's Response to OIG Draft Report: "USSS Faces Challenges Protecting Sensitive Case Management Systems and Data" (Project No.: 15-134-ITA-USSS)

Thank you for the opportunity to review and comment on the subject draft report. The U.S. Secret Service (Secret Service) appreciates the Office of Inspector General's (OIG) work in conducting its review and issuing this report. In accordance with the Department of Homeland Security Directive 077-01, this memorandum provides formal management comments on the draft report.

The Secret Service concurs with OIG recommendations 1-10 and the Department of Homeland Security (DHS) Privacy Office (PRIV) concurs with the eleventh recommendation. The Secret Service will continue to do our utmost to ensure that all of the information with which we are entrusted is properly protected and secured to the greatest degree possible. We understand and value individual privacy and are committed to ensuring that personally identifiable information (PII) is protected from improper disclosure.

To continue accomplishing our integrated mission, the Secret Service requires a modern and secure information technology (IT) infrastructure capable of meeting the needs of its workforce. On November 16, 2015, retired Brigadier General Kevin Nally was hired as the new Secret Service Chief Information Officer (CIO). Responsible for the management, oversight, implementation, and coordination of IT objectives and programs for the Secret Service, he brings a breadth and depth of experience as well as a new, outside perspective to the Secret Service IT organization. His past experience as the CIO for the U.S. Marine Corps makes him well qualified to lead the Secret Service through the changes and improvements our IT systems require. The impact of his leadership is already being demonstrated in the sweeping and unprecedented improvements being

made in our IT systems, processes, organization structure, and overall management practices.

Significant organizational changes and realignment of internal resources have already taken place. Our previous enterprise Information Resource Management Division (IRM) and its branches and personnel have been realigned under the CIO in order to centralize the accountability and management of all IT programs within the Secret Service.

Updated agency directives have been issued to charge the Secret Service CIO with complete oversight and approving authority over all IT spending, to give the CIO oversight and accountability for Federal Information Systems Management Act (FISMA) systems, and to make the CIO the sole Designated Approving Authority (DAA) at the Secret Service.

The Office of the CIO (OCIO) has released the FY 2015 - FY 2021 Information Technology Strategic Plan, which not only lays out the many changes to the organizational structure of IT divisions, but also provides a clear mission and vision for the OCIO to provide the Secret Service with seamless, secure, redundant, reliable, and timely IT enterprise capabilities.

A wholesale inventory and evaluation of IT systems and operations has been accomplished, which identified inefficient and/or non-compliant IT operations, and the OCIO initiated swift corrective actions and/or associated work plans. Recent accomplishments include:

- Improved Secret Service classified communications by being the first DHS component to achieve 100 percent compliance for Homeland Secure Data Network Public Key Infrastructure;
- Improved metrics on the DHS Scorecard for Weakness Remediation, Vulnerability Management, Software Asset Management, and Configuration Settings Management;
- Made all Secret Service employees and contractors Personal Identity Verification (PIV) Card Mandatory as per the Cybersecurity Sprint 1 Memo issued by the DHS Under Secretary for Management;
- Reduced the number of personnel with elevated access privileges by 60 percent;
- Prepared for the Common Appropriations Structure merger of two major Secret Service investments; and
- Reinstituted Program Management Reviews (PMRs) and conducted 17 PMRs, ensuring proper oversight on the planning and execution of Secret Service programs and projects.

While more work remains to be done, the Secret Service has made considerable improvements in a remarkably short period of time. All of these improvements have been and will continue to be accomplished in close coordination with the CIO Deputy Under Secretary for Management, CIO, and their respective offices, who have supported our continuing efforts to make these improvements both financially and administratively.

Timely and efficient disposal of PII is another important focus area for the Secret Service. As electronic records replace paper ones, promptly destroying unnecessary PII records as soon as they are eligible for disposal remains important as a means to prevent unintended access or sharing. We must strike a very delicate balance to ensure compliance with preservation requirements set by the National Archives and Records Administration (NARA), as well as any applicable judicial and legal freezes, while ensuring that PII is disposed of in the fastest manner possible. The OIG's findings in this report serve to direct our focus to areas where we can better achieve this outcome. The Secret Service is using the OIG's findings in this report to inform and direct our focus to areas where we can better achieve this balance.

We take our motto of being "worthy of trust and confidence" very seriously in all areas in which we operate. All individuals who entrust the Secret Service with their personal information should be confident not only that we will protect their information, but also that we will use it only when necessary for the purpose for which it was collected. To reinforce and reiterate our commitment to privacy, not only are all employees and contractors required to take an annual training course on privacy awareness, but also our Privacy Office supplements formal training through official messages, posters, brochures, flyers, banners, and an Annual Privacy Awareness Day. In addition, we have established a PII working group to examine the agency's policies and practices regarding the collection and use of PII, including Social Security Numbers (SSN), throughout Secret Service operations with the objective of recommending changes to minimize the use of PII. We have also established employee privacy training in order to improve the agency's handling of PII, particularly in light of any policy or procedural changes that the group may recommend. The goal of these activities is to serve as a reminder to employees of their obligations with respect to the collection, use, and maintenance of PII to safeguard and respect privacy in their daily roles and responsibilities.

Please find our detailed response to each recommendation attached. We are confident that our actions, in coordination with DHS and other appropriate entities identified in this report, demonstrate a focused and deliberate effort to ensure our IT, records management, and privacy risk matters are managed as required by policy. We look forward to working with the OIG to close these recommendations. Technical comments will be provided under separate cover.

Attachment

**Attachment: Management Response to Recommendations Contained in OIG Draft Report for Project #15-134-ITA-USSS**

**Recommendation 1:** *Provide a plan for ensuring specialized training for all system owners and Information System Security Officers on their roles and responsibilities as well as the proper methods for documenting and validating system security plans, privacy controls, and system deficiencies in the plan of actions and milestones.*

**Response:** Concur. The Secret Service Office of the Chief Information Security Officer, in partnership with the Secret Service Privacy Office, PRIV, the Office of Training, and the James J. Rowley Training Center, is developing a specialized role-based training course for all system owners, administrators, and Information System Security Officers (ISSOs). When completed, this course will be available via the Secret Service's Learning Management System (LMS) and will include specific training objectives related to all Risk Management Framework (RFM) steps, to include system security plans, privacy controls, and system deficiencies.

The Secret Service will continue to follow all pertinent DHS, National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB) guidance when preparing authority to operate (ATO) related documents for system security plans, privacy controls[1], and Plan of Action and Milestones (POAM). The Secret Service enters all ATO documentation into the DHS Information Assurance Compliance System (IACS).

Estimated Completion Date (ECD): December 31, 2016

**Recommendation 2:** *Provide a plan, including milestones and an estimated completion date, for ensuring that each USSS system has a valid authority to operate in accordance with DHS policy.*

**Response:** Concur. The Secret Service follows the specific steps as set forth by DHS, NIST, and OMB guidance when preparing all the necessary documents for ATOs. Currently, the Field Investigative Research System (FIRS) and Protective Threat Management System (PTMS) have completed all of the RFM steps except the Security Control Assessment (SCA). The assessments for both of these systems are expected to be completed no later than mid-September 2016, and both systems should have a signed ATO letter shortly thereafter.

[1] The Senior Agency Official for Privacy oversees and is responsible for the implementation of the NIST 800-53 Rev. 4, Appendix J controls.

The eCheck system has completed all RFM steps and is pending the privacy reviews which are completed by both the Secret Service Privacy Office as well as PRIV. After these privacy reviews are completed, eCheck will undergo the SCA. We estimate that the SCA for eCheck will be completed in late September 2016, and a signed ATO letter is expected shortly thereafter.

The Clearances, Logistics, Employees, Applicants, and Recruitment System (CLEAR) and Enterprise Case Management System (eCASE) have been combined and are now part of the Human Capital Management System (HCMS). Because it is a new system, HCMS is early in the RFM process. The main ISSO and system owner related steps are expected to be completed by late October 2016. Privacy reviews by both the Secret Service and PRIV are expected to take place in November 2016, followed by the SCA. The signed ATO letter for HCMS is expected shortly thereafter.

ECD: All Secret Service systems are expected to have a valid ATO no later than December 31, 2016 (see below).

| System | Estimated ATO approval |
|---|---|
| FIRS | September 30, 2016 |
| PTMS | September 30, 2016 |
| eCheck | October 31, 2016 |
| CLEAR and eCASE, now HCMS | December 31, 2016 |

**Recommendation 3:** *Provide a plan, including milestones and an estimated completion date, for fully implementing Personal Identity Verification cards as mandated for logical access to all USSS networks and information systems.*

**Response:** Concur. As of June 2016, PIV card access and usage was made mandatory at the Secret Service. When the OIG's review began, we were in the process of deploying the necessary software changes in order to comply with Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors." We are pleased to report that we accomplished that goal and are now 100 percent compliant, thanks in part to assistance from DHS. As of June 2016, we have fully implemented the mandate for PIV card access and usage to all networks and information services for employees and contractors. Documentation of this policy change will be sent to the OIG under separate cover.

The Secret Service requests that the OIG consider this recommendation resolved and closed.

**Recommendation 4:** *Provide a plan, including defined roles and responsibilities of the DHS Privacy Office, the USSS Privacy Office, and the USSS Office of the Chief Information Officer for implementing privacy controls on all USSS systems.*

**Response:** Concur. The Acting Chief Information Security Officer will work with the individual system ISSO to complete a Privacy Threshold Analysis (PTA) for each system. The PTA will be sent to the Secret Service Privacy Office which will coordinate with appropriate CISO and operational program staff to evaluate the PTA and send it to PRIV for adjudication. PRIV will evaluate the PTA to determine whether a program, system and/or activity has privacy implications. Where there are privacy implications, controls and privacy compliance documentation will be developed and maintained as appropriate. The Secret Service Privacy Office in collaboration with the ISSO and operational program will draft all required privacy compliance documentation, and all privacy compliance documentation must be approved by PRIV. PRIV is responsible for determining and applying privacy controls during the privacy review stage of the ATO process.

ECD: December 31, 2016

**Recommendation 5:** *Appoint a full-time, senior-level Privacy Officer reporting directly to the USSS Director to ensure compliance with DHS guidance for implementing privacy protections, consistent with the DHS Privacy Act Compliance Management Directive 0470.2.*

**Response:** Concur. The Secret Service Chief Operating Officer will work with the DHS Chief Privacy Officer and others, as appropriate, to determine how best to fulfill the requirements of the Deputy Secretary's memorandum.

ECD: December 31, 2016

**Recommendation 6:** *Provide a plan, including milestones and an estimated completion date, for ensuring compliance with the current USSS requirements and the National Archives and Records Administration's regulations for retention and destruction of applicant records.*

**Response:** Concur. As noted in the OIG report, specific Secret Service policy regarding retention and destruction of applicant records has been issued. The Management and Organization Division within the Office of Strategic Planning and Policy will develop a plan outlining additional activities, milestones, and estimated completion dates to support compliance with the current Secret Service policy and associated NARA regulations.

ECD: November 30, 2016

**Recommendation 7:** *Provide an information technology strategic plan, including milestones and an estimated completion date, outlining the responsibilities, resources, and initiatives needed to accomplish USSS goals and objectives.*

**Response:** Concur. In February 2016, the Secret Service released its Information Technology Strategic Plan for FY 2016 - FY 2021. The plan includes the CIO's Mission Statement, Vision Statement, and Strategic Goals and Objectives necessary for the Secret Service to address the changing needs of the agency and its workforce. A copy of the IT Strategic Plan will be sent to the OIG under separate cover.

The Secret Service requests that the OIG consider this recommendation resolved and closed.

**Recommendation 8:** *Provide a plan and process for creating, reviewing, and updating information technology policies and procedures on a regular basis.*

**Response:** Concur. The Information Technology Governance and Accountability Program developed a robust policy production process for the OCIO effective July 2016. All policies from the OCIO are initiated and formalized utilizing this process and managed via a yearly review schedule. A copy of the IT Policy Update Process will be sent to the OIG under separate cover.

The Secret Service requests that the OIG consider this recommendation resolved and closed.

**Recommendation 9:** *Provide a plan, including milestones and an estimated completion date, for addressing staff vacancies in critical information technology management positions, such as the Chief Information Security Officer [CISO].*

**Response:** Concur. Maintaining an optimally staffed OCIO is an ongoing, iterative process that will require sustained efforts. Filling vacant management positions in the OCIO is a current priority. We are in the process of reviewing resumes for the Deputy CIO position and re-soliciting applications for the CISO position.

The Secret Service Office of Human Resources has been tasked with recruiting and staffing open positions within the OCIO. As the OIG draft report noted, there are a variety of factors that make filling these vacancies particularly challenging. Through targeted recruiting, expansion of hiring authorities, and efficiencies in applicant

processing, we will be able to bring individuals with the necessary skills on board. Since the new CIO's arrival, the OCIO has increased to 226 authorized government full-time positions. Of the 41 current vacancies in OCIO, 35 are in various phases of the hiring process. Our goal is to fill 80 percent of these vacancies by January 2017.

ECD: January 31, 2017

**Recommendation 10:** *Establish a repeatable process for ensuring that all USSS employees and contractors annually complete information security awareness, privacy, and role-based training.*

**Response:** Concur. The Secret Service requires all employees and contractors to complete Information Security Awareness training on an annual basis. The majority of training is completed in LMS, managed by the Office of Training, and is available to all Secret Service employees online. Through LMS, all employees are assigned training modules appropriate to their roles, permissions, and job functions. All Secret Service employees and contractors are required to take the "Privacy at DHS: Protecting Personal Information" course annually. All personnel in specific job series, which includes all law enforcement officers who use social media for operational purposes, are required to take "Operational Use of Social Media" training which was developed by the Secret Service Privacy Office and Office of Chief Counsel.

An additional related training course, "Social Engineering Awareness and Prevention," was recently released via LMS and must be completed by all employees before September 30, 2016. The purpose of the course is to educate our workforce on the dangers of social engineering. Per DHS and OMB, the training is a mandatory annual requirement for all DHS employees.

The Secret Service verifies and ensures that employees remain current with required training in two ways. An employee's direct supervisor is able to review the status of LMS courses assigned to that employee. An employee's annual and semi-annual performance evaluations include first-line supervisory review and verification that all of their assigned training is current.

Additionally, each Secret Service office undergoes a compliance inspection every four years. The purpose of compliance inspections is to verify that all offices are operating in accordance with Secret Service policy, procedures, and protocols. One aspect of the inspection is a review of the status of all employees' LMS training requirements. Failure to keep current with all assigned training modules is noted by the Inspection Division team and may be included in that office's evaluation, which is distributed to the respective Assistant Director. Thus, managers are kept aware of the status of their personnel's mandatory training.

To improve and streamline all of our computer-based training, the Secret Service will migrate from LMS to the DHS Performance and Learning Management System (PALMS) on November 30, 2016. PALMS offers additional functionalities including the ability of supervisors to view the real time status of employee completion of mandatory training as well as automated notifications and reminders.

Documentation of the training verification portion of the Compliance Inspection Checklist will be provided to the OIG under separate cover.

The Secret Service requests that the OIG consider this recommendation resolved and closed.

**Recommendation 11:** *Conduct a systematic review with recommendations for ensuring USSS compliance with DHS privacy requirements.*

**Response:** Concur. PRIV will conduct a Privacy Compliance Review (PCR) of the Secret Service. PRIV will determine the scope of the PCR and develop an initial set of questions and document requests to submit to the Secret Service at the beginning of Fiscal Year 2017.

ECD: July 30, 2017

## Appendix C
## USSS Systems Reviewed

The USSS unclassified systems reviewed are provided in the following table.

**USSS Systems Reviewed**

| System Name | Primary Function |
|---|---|
| Field Investigative Reporting System (FIRS) | Used by USSS field agents to document investigative cases, threat assessments, crime patterns, standard operating procedures, and lessons learned. |
| Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR) | Used by the Security Clearance Division, Uniformed Division, and the Personnel Division (Human Resources) to manage and store information related to job vacancies and employment applications. |
| Protective Threat Management System (PTMS) | Used by the USSS Protective Intelligence and Assessment Division to provide consolidated incident and threat case management information. |
| Electronic Name Check System (eCheck) | Used by the USSS Dignitary Protective Division to conduct security name checks on National Special Security Event workers to grant access to the event and produce physical credentials. These name checks are performed through the National Crime Information Center information system, a nationwide information system established by the Federal Bureau of Investigation. |
| Electronic Case Management System (eCase) | Used by USSS as a case management system to track general protection of detailees and applicant security clearance cases. |

*Source:* DHS OIG analysis of USSS documentation and auditee statements

# Appendix D
# NIST Control Areas Reviewed

We selected three key systems (FIRS, CLEAR, and PTMS) to perform security controls assessments, which included document reviews, interviews, and technical testing. This helped to determine whether adequate systems and data protections were in place.

NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, issued in April 2013, provides guidance for implementing a variety of security controls for information systems supporting the Federal Government. We reviewed selected controls from each of the following control families provided in the following table.

**Control Areas and Descriptions**

| Control Family | Description |
|---|---|
| Access Controls | Includes areas such as policy and procedures, account management, access enforcement, separation of duties, and least privilege. |
| Awareness and Training | Includes areas such as policy and procedures, information technology security awareness training, and specialized role-based security training. |
| Audit and Accountability | Includes areas such as policy and procedures, audit events, audit review, analysis, and reporting. |
| Configuration Management | Includes areas such as policy and procedures, baseline configuration, access restrictions for change, and least functionality. |
| Identification and Authentication | Includes areas such as policy and procedures and multi-factor authentication to access information systems. |

*Source:* DHS OIG-developed based on NIST requirements

## Appendix E
## Major Contributors to This Report

Richard Saunders, Director, Office of IT Audits
Philip Greene, Audit Manager, Office of IT Audits
Jason Dominguez, IT Specialist/Technical Lead, Office of IT Audits
Richard Elias, IT Auditor/Privacy Lead, Office of IT Audits
Alexander Granado, Senior IT Auditor, Office of IT Audits
Jacqueline Ferrand, Attorney, Assistant Counsel to the Inspector General
Anthony Monaco, Senior Special Agent, Special Investigations
Craig Adelman, Referencer

# Appendix F
# Report Distribution

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
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 Privacy Officer

**United States Secret Service**

Chief Operating Officer
Chief Information Officer
Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

## ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

## OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305