Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

SECURITY CONTROLS OVER THE IMPLEMENTATION OF PERSONAL IDENTITY VERIFICATION CARDS AT THE DEPARTMENT OF HEALTH AND HUMAN SERVICES WERE INADEQUATE DUE TO LACK OF SOME ESSENTIAL INFORMATION SECURITY REQUIREMENTS

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Thomas M. Salmon
Assistant Inspector General
for Audit Services

July 2014
A-18-12-30410

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Security controls over the implementation of Homeland Security Presidential Directive 12 at the Department of Health and Human Services were inadequate because essential information security requirements were not implemented.

This report provides an overview of the results of our audit of the Department of Health and Human Services (HHS) implementation of Homeland Security Presidential Directive 12 (HSPD-12). Due to the sensitive nature of the specific findings identified during our audit, only a summary of the findings are included in this report. We have provided more detailed information and recommendations to HHS so that it can address the issues we identified.

WHY WE DID THIS REVIEW

The HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004, mandated the promulgation by 2006 of a Federal standard for secure and reliable forms of identification for Federal employees and contractors and mandates the use of governmentwide identification credentials for employees and contractors. The HSPD-12 and other Federal guidance require executive departments and agencies to (1) implement the standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access (the authorized and authenticated access to computer applications and data files) to controlled information systems and (2) implement and maintain adequate security for all their support systems and applications. We evaluated HHS' progress in implementing a reliable and effective system of personal identity verification (PIV) in compliance with the HSPD-12.

Our objective was to determine whether HHS complied with Federal guidance when implementing its HSPD-12 system.

BACKGROUND

Federal guidance has established the minimum architecture and technical requirements for a Federal personal identification system, including requirements for PIV, registration, card issuance, and interoperability of PIV credentials and systems among Federal Departments and agencies, as well as detailing technical specifications. Federal guidance also provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources and provides for development and maintenance of the minimum controls required to protect Federal information and information systems.

HHS's mission is to protect the health of all Americans and provide essential human services, especially for those who are least able to help themselves. HHS's programs are administered by its divisions. In addition to the services they deliver, the HHS programs enable the collection of national health and other data.

At the beginning of our audit, the HHS Program Management Office (PMO) was responsible for implementing and monitoring HSPD-12 systems. The PMO took a decentralized approach to implementing the HSPD-12, providing the same guidance to the divisions but allowing each one to determine how it implemented the HSPD-12. During our audit, the overall responsibility for the implementation and monitoring of the HSPD-12 was transitioning from the PMO to the Office of Security and Strategic Information (OSSI).

HOW WE CONDUCTED THIS REVIEW

We evaluated the HHS implementation of the HSPD-12 and the security controls over a sample of its critical HSPD-12 systems to determine whether the guidance had been followed. Specifically, we assessed (l) whether the HHS PIV card application and issuance processes were effective and complied with HHS guidance and regulations and (2) whether information security controls over critical HHS PIV systems complied with Federal information security standards.

We reviewed the following information technology (IT) security controls in effect as of August 2012: security management, program and system-specific controls, encryption, change controls, Web vulnerability management, and physical security. Appendix A contains a summary of our audit scope and methodology.

Risk Level Definitions for Findings

To assign risk levels (i.e., High, Medium, Low) to our findings, we used the risk scale of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*, Appendix D, which describes the need for corrective actions and the relative timeframes in which they must occur based on the levels of risk associated with system vulnerabilities.

WHAT WE FOUND

HHS did not always comply with Federal guidance when implementing its HSPD-12 system. Specifically, security controls over the implementation of the HSPD-12 at HHS were inadequate because essential information security requirements were not implemented. We found six categories of vulnerabilities:

- **Enrollment and issuance process**—The implementation of the HSPD-12 lacked controls to ensure that all credentialing requirements were met and that training was provided to employees who performed HSPD-12 roles. In addition, a standard had not been established under which key roles had to be held by different employees to ensure adequate separation of duties, and verify integrity of PIV credentials (high risk).

- **Deactivation of PIV cards**—PIV cards were not deactivated in a timely manner (high risk).

- **Security over system access—**The implementation of the HSPD-12 lacked controls to ensure that management had implemented policies and procedures associated with access to the PIV system and protection of sensitive system information (high risk).

- **Security management**—The data center facility's network firewall configuration policies did not comply with HHS policy or guidelines. Also, security management controls, including patch management, antivirus management, and configuration management, were not implemented on HSPD-12 workstations at any of the division PIV Card Issuance Facilities (PCIF) that we audited. HHS allowed nongovernmental computers to connect to card management systems (high risk).

- **Physical security**—Physical security controls, which help ensure that physical access to key areas within the PCIF is restricted to authorized personnel, were not adequate for the PIV system (high risk).

- **Web vulnerabilities**—Vulnerabilities were identified in 17 categories on the HHS PIV system Web portal test sites that were scanned (moderate risk).

Due to the sensitive nature of the specific findings identified during our testing, only a summary of the findings are included in this report. We have provided more detailed, technical findings to HHS/OSSI.

WHAT WE RECOMMEND

We recommend that HHS/OSSI implement essential security requirements in the areas of enrollment and issuance, deactivation of PIV cards, system access, security management, physical security, and PIV Web portals.

This report summarizes our recommendations due to the sensitive nature of the information discussed. We have provided more detailed recommendations to HHS/OSSI.

AUDITEE COMMENTS

In written comments on our draft report, OSSI concurred with 14 recommendations and did not concur with 4 recommendations. Their comments also described the actions they will take to implement our recommendations.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed selected IT security controls in effect as of August 2012. These controls were security management, program and system-specific controls, encryption, change controls, Web vulnerability management, and physical security. We performed our fieldwork from August 2012 to March 2013 at select HHS PCIF locations.

HSPD-12 security management did not permit us to complete vulnerability scans during the audit period. Therefore, we were unable to obtain sufficient evidence to determine whether the vulnerabilities we identified in the test environment were corrected in the production environment and that other more serious Web vulnerabilities did not exist. We also were unable to determine whether the vulnerabilities we identified in the test environment were remediated by corrective actions.

METHODOLOGY

To accomplish our objective, we:

- reviewed the HSPD-12 program policies and procedures;
- interviewed the HSPD-12 program employees who were knowledgeable of the areas we addressed;
- assessed the HSPD-12 program's program and system-specific controls;
- reviewed the HSPD-12 program's change controls;
- judgmentally selected 50 PIV applicants at divisions to determine the following:
    - whether PCIFs were screening applicant fingerprints before authorizing and issuing PIV cards and
    - whether PCIFs verified the existence and results of a background investigation for each applicant before card issuance;
- judgmentally selected eight role holders at divisions to determine whether training was provided for all of the roles they held;
- assessed the key system roles throughout the PIV card enrollment and issuance process to determine whether there was separation of duties;
- reviewed active accounts to determine whether PIV cards were deactivated in a timely manner for terminated and separated personnel within the past year;

- assessed the HSPD-12 program's security management controls on PCIF workstations and servers to include patch, antivirus, and configuration management to determine whether they were implemented;

- assessed the HSPD-12 program's physical security at select HHS PCIF locations;

- reviewed the HSPD-12 program's Web vulnerability management and scanned two HSPD-12 Web portal test sites; and

- discussed our findings with division management.

We assigned risk levels to these vulnerabilities according to NIST Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*.

We conducted this performance audit in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.