Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE INFORMATION TECHNOLOGY INFRASTRUCTURE AND OPERATIONS OFFICE HAD INADEQUATE INFORMATION SECURITY CONTROLS

Inquires 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

April 2015
A-18-14-30420

Office of Inspector General

http://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.

The Information Technology Infrastructure and Operations office at the U.S. Department of Health and Human Services had not fully implemented or monitored information security controls at some Health and Human Services operating divisions.

This summary report provides an overview of the results of our audit of the information security controls at the Information Technology Infrastructure and Operations (ITIO) office at the Department of Health and Human Services (HHS). It does not include specific details of the vulnerabilities that we identified because of the sensitive nature of the information. We have provided more detailed information and recommendations to HHS so that it can address the issues we identified.

WHY WE DID THIS REVIEW

Security controls are the management, operational, and technical safeguards that an organization uses to protect the confidentiality, integrity, and availability of its information systems. Selecting and implementing appropriate information system security controls is critical to the operations and assets of an organization, as well as to the welfare of the individuals that the organization serves.

Our objective was to assess the adequacy of ITIO information security controls at a selection of HHS operating divisions (OPDIVs) that are managed by ITIO.

BACKGROUND

Agencies implement and maintain an information security program to ensure that adequate security is provided for all support systems and major applications (Office of Management and Budget Circular A-130, Appendix III). Federal statute contains a comprehensive framework for ensuring the effectiveness of information security controls over information resources and provides for development and maintenance of minimum controls required to protect Federal information and information systems (the Federal Information Security Management Act of 2002).

The ITIO office provides enterprise network and security infrastructure services to HHS staff divisions and several of the HHS OPDIVs, including Administration for Children and Family, Administration for Community Living, and Health Resources and Services Administration. The ITIO network operations center provides monitoring and troubleshooting of network-related activities. The ITIO security operations center also provides monitoring and troubleshooting of security-related activities on the Office of the Secretary's enterprise network, including support for HHS's headquarters, interconnections to the regional offices, and incident response.

The information technology (IT) needs of HHS are supported by a service contract. The contractor is responsible for managing the network infrastructure (i.e., the network, routers, firewalls, and general-use servers) and user desktops for the smaller OPDIVs. ITIO oversees the contractor to ensure that all aspects of the contract are successfully completed. ITIO is also responsible for antivirus and patching updates for workstations at the smaller OPDIVs for which ITIO provides network and security services.

HOW WE CONDUCTED THIS REVIEW

We reviewed selected ITIO information security controls in effect as of November 2013. Specifically, we reviewed controls over inventory management, patch management, antivirus management, event management, logical access, encryption, configuration management, Web vulnerability management, and Universal Serial Bus (USB) port control management. We interviewed ITIO's security and IT personnel, reviewed policies and procedures, and tested controls in place at ITIO and selected OPDIVs. Our objective did not require us to review ITIO's overall internal control structure. The Appendix contains a summary of our audit scope and methodology.

WHAT WE FOUND

We found that ITIO had not fully implemented or monitored some information security controls. We identified the following six categories of vulnerabilities:

- **IT asset inventory management**—ITIO did not track and manage IT asset inventories effectively.

- **Patch management**—ITIO monitored patch management security controls over computers that it managed, but we identified some vulnerabilities that, if exploited, could have led to unauthorized disclosure, modification, or unavailability of critical data.

- **Logical access**—ITIO did not conduct sufficient reviews of its logical access control process.

- **Configuration management**—ITIO did not implement a standard configuration management program that ensured that all ITIO-managed devices were configured properly.

- **USB port control access**—ITIO did not have any policies or procedures to effectively secure USB port control access.

- **Antivirus management**—ITIO did not manage its antivirus security controls effectively.

Because of the sensitive nature of the specific findings identified during our testing, we include only a summary of the findings in this report. We have provided a more detailed description of our findings to ITIO.

WHAT WE RECOMMENDED

We recommended that ITIO implement our detailed recommendations to address the specific findings we identified. This report summarizes our recommendations because of the sensitive nature of the information discussed. We have given more detailed recommendations to ITIO.

AUDITEE COMMENTS

In written comments on our draft report, the HHS Office of the Chief Information Officer concurred with all of our recommendations and described actions it has taken and plans to take to implement them.

APPENDIX: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed selected IT security controls in effect as of November 2013. Specifically, we reviewed controls over inventory management, patch management, antivirus management, event management, logical access, encryption, configuration management, Web vulnerability management, and USB port control management. We did not review ITIO's overall internal control structure.

We performed our fieldwork at ITIO and selected OPDIVs from November 2013 through April 2014.

METHODOLOGY

We audited ITIO's information security controls by reviewing policies and procedures, interviewing employees, reviewing and analyzing records, and reviewing documentation. To accomplish our objective, we reviewed:

- applicable Federal and State requirements and industry best practices;

- inventory management processes for IT assets to ensure that management monitors and protects property and other assets against waste, loss, unauthorized use, or misappropriation;

- patch management procedures for patch installations and monitoring of ITIO-managed desktops and laptops at select OPDIVs and all critical and important[1] patches released over a 6-month period in 2013;

- antivirus versions and signature timestamps to ensure that they were current;

- logical access processes and performed an analysis of the accounts for ITIO-managed Active Directory and remote user virtual private networks;

- baseline configurations to determine whether controls governing them were monitored and whether the configurations remained current;

- the results of Web vulnerability scans to ensure that the scans were performed;

- encryption and USB port controls that prevent unauthorized export of information, particularly personally identifiable information and other sensitive data; and

[1] Microsoft describes a critical patch as one that addresses a vulnerability whose exploitation could allow the propagation of an Internet worm without a user action and an important patch that addresses a vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data or the integrity or availability of processing resources.

We also discussed our findings with ITIO officials.

We conducted the 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 provided a reasonable basis for our findings and conclusions based on our audit objectives.