Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

INFORMATION SECURITY AT THE HEALTH RESOURCES AND SERVICES ADMINISTRATION NEEDS IMPROVEMENT BECAUSE CONTROLS WERE NOT FULLY IMPLEMENTED AND MONITORED

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

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

April 2015
A-18-14-30430

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.

Information security at the Health Resources and Services Administration needs improvement because controls were not fully implemented and monitored.

This summary report provides an overview of the results of our audit of the information security controls at the Health Resources and Services Administration (HRSA). 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 HRSA 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 the welfare of individuals that the organization serves.

Our objective was to assess the adequacy of HRSA's information security controls.

BACKGROUND

Agencies implement and maintain a 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 the development and maintenance of minimum controls required to protect Federal information and information systems (the Federal Information Security Management Act of 2002).

HRSA is an agency of the U.S. Department of Health and Human Services (HHS). HRSA focuses on improving access to health care by strengthening the health care workforce, building healthy communities, and achieving health equity. HRSA works with States, local public health agencies, and partners throughout the Nation to accomplish its mission.

HRSA is an information-intensive organization. Solutions for HRSA's information technology (IT) needs must be timely, comprehensive, reliable, and cost-effective. Effectively managing IT resources is essential in achieving HRSA's goals.

HRSA's Office of Information Technology (OIT) develops and coordinates HRSA-wide plans, budgets, policies, and procedures for IT infrastructure services. These services include support for Microsoft Windows-enabled desktop and laptop hardware and software, customer service, email, infrastructure software, application server hosting, IT security, networking, remote access, telecommunications, and video conferencing.

HOW WE CONDUCTED THIS REVIEW

We reviewed selected HRSA information security controls in effect as of December 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 HRSA's security and IT personnel, reviewed policies and procedures, and tested controls in place at HRSA. Our objective did not require us to review HRSA's overall internal control structure. The Appendix contains a summary of our audit scope and methodology.

WHAT WE FOUND

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

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

- **Patch management**—HRSA's patch management controls were not implemented and monitored effectively. HRSA had vulnerabilities that, if exploited, could have allowed unauthorized disclosure, modification, or unavailability of critical data.

- **Antivirus management**—HRSA did not monitor the antivirus status of HRSA-managed assets effectively.

- **Logical access**—HRSA's Active Directory user accounts were not consistently reviewed as outlined in HRSA's policies.

- **Encryption**—HRSA did not consistently apply their encryption policies.

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

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 HRSA.

WHAT WE RECOMMEND

We recommended that HRSA 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 HRSA.

AUDITEE COMMENTS

In written comments on our draft report, HRSA concurred with 17 of 18 recommendations and partially concurred with one recommendation 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 December 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 HRSA's overall internal control structure.

We performed our fieldwork at HRSA offices from January through July 2014.

METHODOLOGY

We audited HRSA'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 requirements and industry best practices;
- inventory management processes for IT assets to ensure that management monitors and protects assets against waste, loss, unauthorized use, or misappropriation;
- patch management procedures for patch installation and monitoring, including a review of patches deployed on HRSA-managed desktops and laptops;
- antivirus versions and signature timestamps to ensure that they were current;
- logical access processes and performed an analysis of HRSA's Active Directory and remote user virtual private network accounts;
- event management processes to determine whether audit logs were generated and monitored;
- configuration management to determine whether standard configurations controls were monitored and baseline configurations remained current on HRSA's computers and network devices;
- the results of Web vulnerability scans to ensure that the scans were performed; and
- encryption and USB port controls that prevent unauthorized access to sensitive data.

We also discussed our findings with HRSA officials.

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.