Department of Health and Human Services

**OFFICE OF INSPECTOR GENERAL**

# PUBLIC SUMMARY REPORT: THE DEPARTMENT OF HEALTH AND HUMAN SERVICES SECURITY MANAGEMENT PRACTICES FOR COMPUTER SYSTEMS WITH ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION

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

Daniel R. Levinson
Inspector General

August 2016
A-18-16-30150

# *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.

# *Notices*

---

**THIS REPORT IS AVAILABLE TO THE PUBLIC**
at http://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

## OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

***This report provides information collected from the Department of Health and Human Services and its operating divisions about the security management practices for computer systems that provides access to personally identifiable information.***

## WHY WE DID THIS REVIEW

The Cybersecurity Act of 2015 (Cybersecurity Act)[1] requires the Inspector General of each covered agency to collect and report to Congress information about the covered agency's covered systems within 240 days of the enactment of the Cybersecurity Act. A covered agency is an agency that operates a covered system, which is a Federal computer system that provides access to classified information or personally identifiable information. Our use of the terms "covered agency" and "covered system" is consistent with the definition for such terms in the Cybersecurity Act. Reportable areas include logical access controls, multifactor authentication, and information security management practices regarding the covered systems.

This public summary does not include specific details that we obtained from the Department of Health and Human Services (HHS) and its operating divisions (OPDIVs) because of the sensitive nature of the information. We have provided such information to Congress and HHS.

## OBJECTIVE

Our objective was to provide information collected from HHS and its OPDIVs regarding HHS's covered systems.

## HOW WE CONDUCTED THIS REVIEW

We obtained a list of covered systems (588) from the HHS Office of the Chief Information Officer and requested that each OPDIV provide us with information needed to respond to each of the areas described in the Cybersecurity Act. We did not test or validate the information provided by each OPDIV because the Cybersecurity Act did not require us to do so. However, during our annual Federal Information Security Modernization Act (FISMA) audit, we review the information security programs at HHS and selected OPDIVs. The FISMA audit includes testing the following controls outlined in the Cybersecurity Act: logical access, multifactor authentication, data loss prevention, digital rights management, and forensic and visibility capabilities. Our FY 2015 FISMA report is available at http://oig.hhs.gov/oas/reports/region1/181530300.pdf.

## RESULTS

HHS has 11 OPDIVs[2] that administer a wide variety of health and human services and conduct life-saving research. The HHS Office of the Chief Information Officer published

[1] P.L. No. 114-113, 129 Stat 2242 (2015), section 406.

[2] Staff Divisions are included in the Office of the Secretary, which is an OPDIV.

*HHS-OCIO Information Systems Security and Privacy Policy* (*HHS IS2P*). This policy establishes information technology (IT) security and privacy requirements for the OPDIVs' IT security programs and information systems. Each OPDIV may complement *HHS IS2P* by developing its own policies and procedures.

**Logical Access Policies and Practices**

HHS provided us with information indicating that its logical access policies and practices are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The foundation of HHS's logical access policies and procedures for covered systems can be found in the Access Controls (AC) section of NIST SP 800-53. All HHS OPDIVs (covering 100 percent of HHS's covered systems) use this common standard as a foundation.

The *HHS IS2P* requires HHS OPDIVs to follow NIST SP 800-53 security controls. HHS logical access controls[3] include policies and procedures for account management, access enforcement, separation of duties, least privilege, and use of external information systems. HHS's logical access control policies are addressed through the following NIST controls: AC-3, "Access Enforcement," and CM-5, "Access Restrictions for Change." AC-3 requires that the information system enforce approved authorizations[4] for logical access to information and system resources in accordance with applicable access control policies. CM-5 requires organizations to define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

We recognize NIST SP 800-53 as the appropriate standard.

**Logical Access Controls and Multifactor Authentication Governing Privileged Users' Access to Covered Systems**

HHS and its OPDIVs use a variety of logical access controls as well as multifactor authentication to govern privileged users' access to covered systems. The Cybersecurity Act defines a privileged user as "a user who has access to system control, monitoring, or administrative functions."[5]

[3] A logical access control is a process of granting or denying specific requests to obtain and use information and related information processing services.

[4] The process whereby access is granted (authorized) and approved within a network. Access control policies (e.g., role-based policies) and access enforcement mechanisms (e.g., access control lists) are employed by organizations to control access between users and objects (e.g., devices, files, records, domains) in the information system.

[5] Cybersecurity Act § 406 (a)(5).

HHS in *HHS IS2P* lists the following logical access controls: require each individual user to have a separate user account; follow the principles of least privilege;[6] monitor the use of information system accounts; review all user accounts annually; disable all inactive user accounts after 60 days of nonuse; establish, administer, and monitor privileged user accounts in accordance with a role-based access scheme;[7] and restrict privileged accounts to personnel or roles as specified by the OPDIV. According to HHS, OPDIVs have implemented logical access controls on all covered systems, and all users, including privileged users, are subject to them.

For privileged users, HHS requires two-factor authentication (personal identity verification (PIV) and personal identification number (PIN)) to gain network-level access.[8] This form of multifactor authentication is primarily controlled through the Active Directory[9] (single sign-on). Once a user's PIV and PIN are authenticated, some HHS systems do not require additional verification. Other systems require additional authentication, such as user names and passwords and PIV cards with a PIN; user names and passwords and RSA tokens; and user names and passwords and PIV cards with a PIN and additional alternate logon tokens or smart cards.

HHS reported that approximately 99 percent of its covered systems use multifactor authentication. Seven of HHS's 588 covered systems (about 1 percent) do not require multifactor authentication for access by privileged users. HHS reported the following reasons for not using multifactor authentication for those covered systems: (1) multifactor authentication is cost prohibitive in relation to the cost associated with the loss of the information or services; (2) application-specific credentials are required, and there are a limited number of privileged users; (3) multifactor authentication is not supported in the environment where the covered system resides; and (4) the covered system is on an isolated network. Two OPDIVs that have covered systems that are not using multifactor authentication are investigating the use of multifactor authentication.

**Software and Licenses Inventory Policies and Procedures**

HHS's policies and procedures for conducting inventories of software on covered systems and associated licenses are documented in the *HHS IS2P*, Appendix H, "System Component Inventory Requirements." According to *HHS IS2P*, OPDIVs must develop and document a component inventory for all information systems. The inventory must include all components within the "authorization boundary" of the information system and be sufficiently detailed to allow for tracking and reporting. At a minimum, the inventory record for each system component, including software and associated licenses, must include the following elements:

[6] Least privilege refers to the security objective of granting users only the access they need to perform their official duties. Data-entry clerks, for example, may not have any need to run analysis reports using their database.

[7] Access to information may also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access. The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization.

[8] NIST SP 800-53 addresses multifactor authentication in IA-2, "Network Access to Privileged Accounts."

[9] The Active Directory is a Windows Operating System directory service that allows a single computer (the Active Directory computer) to communicate with numerous computers, applications, and devices on a network.

- unique identifier and/or serial number;
- system name, of which the component is a part;
- type of system component (e.g., server, desktop, network device, storage, application);
- manufacturer/model;
- operating system type and version/service pack level;
- presence of virtual machines;
- application software version/license information;
- physical location (e.g., building/room number);
- logical location (e.g., Internet Protocol (IP) address);
- Media Access Control address;
- owner name;
- operational status; and
- names of primary and secondary administrators.

Software usage controls are also included in the *HHS IS2P*. CM-10 ("Software Usage Restrictions") states that the organization tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution. Software license tracking can be manual (e.g., simple spreadsheets) or automated (e.g., specialized tracking applications), depending on organizational needs.

CM-11 ("User-Installed Software") states that the organization should prohibit the installation of software by users on all Government-furnished equipment, enforce software prohibition policies through methods defined by the OPDIV, and monitor policy compliance at least monthly.

In addition to the controls required by *HHS IS2P*, some OPDIVs have their own policies and specific procedures for software and licensing inventory. Other OPDIVs reported that policies for conducting inventory of software and associated licenses are under development.

**Capabilities To Monitor and Detect Exfiltration and Other Threats**

The HHS Computer Security Incident Response Center (CSIRC) works with HHS OPDIVs to monitor and collect information from a wide range of sources to detect information system security incidents and events including exfiltration and data loss. The HHS CSIRC obtains data

about vulnerabilities and threats to HHS covered systems through OPDIV incident reports, suspicious files or malware, and cyber intelligence. The HHS CSIRC also obtains data by monitoring Intrusion Detection/Intrusion Prevention[10] Sensors, EINSTEIN[11] alerts from the United States Computer Emergency Readiness Team, and audit logs.

According to the *HHS CSIRC Concept of Operations*, the HHS CSIRC employs a tiered structure:

- **Tier 1:** Triages and manages incident tickets; acts as the single point of contact for coordinating incident response communications with OPDIVs; takes responsibility for quality control, situational awareness, correlation of data, and reactive analysis.

- **Tier 2:** Conducts reactive analysis[12] based on cyber security reports and suspicious files.

- **Tier 3:** Provides subject matter expertise and strategic analysis of a given incident; conducts open-source research, trending analysis, and visualization.

**Ensuring Entities, Including Contractors, Implement Information Security Management Policies and Procedures**

HHS requires all entities, including contractors, to follow HHS and OPDIV information security policies and procedures. The *HHS IS2P* states that "all organizations collecting or maintaining information, or using or operating information systems on behalf of the Department, are also subject to the stipulations of this Policy." OPDIVs may have additional polices that expand on HHS policy. Contractors are required to follow the same information security management policies and procedures for covered systems as HHS employees. These requirements include specific training such as the following:

- Security Awareness Training—HHS provides basic security awareness training to all information system users (including managers, senior executives, and contractors). Users should also review and sign the *Rules of Behavior for Use of HHS Information Resources* after completing initial and annual refresher training. According to the HHS Chief Information Officer (CIO) 2015 *Annual FISMA Report*, 99 percent of users successfully completed annual security awareness training.

- Role-based Security Training—HHS provides role-based security-related training to all personnel with significant information security responsibilities. According to the HHS CIO 2015 *Annual FISMA Report*, 76 percent of users with significant security

[10] Intrusion detection and prevention systems are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

[11] EINSTEIN is an intrusion detection system (IDS) for monitoring and analyzing Internet traffic as it moves in and out of U.S. Government networks.

[12] Reactive analysis relies on the organization's ability to analyze and detect the presence of an adversary on the organization's networks and systems and craft an effective response and recovery strategy.

responsibilities who were required to complete the training during FY 2015[13] successfully completed it.

## CONCLUSION

HHS and its OPDIVs have developed logical access policies and practices based on NIST standards. HHS and its OPDIVs use logical access controls to access all covered systems. HHS and its OPDIVs reported to us that multifactor authentication is required by privileged users to access nearly all of its covered systems, which includes the use of a PIV card at the network/system level. Seven of HHS's 588 (about 1 percent) covered systems do not require privileged users to provide additional authentication to access those covered systems. The majority of OPDIVs have developed policies and procedures to conduct inventories of software and licenses associated with covered systems. HHS and its OPDIVs use a variety of tools to monitor and detect exfiltration and other threats. All entities, including contractors that provide services to HHS, are required to follow HHS information security management practices for all covered systems.

[13] Many OPDIVs have a 3-year training schedule for personnel with significant security responsibilities. This completion percentage is reflective of those employees who were required to complete the training during the year. According to the HHS CIO, many employees fulfilled the requirement during previous years.