

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**HHS OFFICE OF THE SECRETARY
NEEDS TO IMPROVE KEY SECURITY
CONTROLS TO BETTER PROTECT
CERTAIN CLOUD INFORMATION
SYSTEMS**

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



**Amy J. Frontz
Deputy Inspector General
for Audit Services**

**July 2024
A-18-22-08018**

Office of Inspector General

<https://oig.hhs.gov>

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

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. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, the anti-kickback statute, and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at <https://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 website.

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.

Report in Brief

Date: July 2024

Report No. A-18-22-08018

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL



Why OIG Did This Audit

This audit is one in a series of audits that will examine whether HHS and its operating divisions (OpDivs) have implemented effective cybersecurity controls for cloud information systems owned, operated, or maintained by HHS or its contractors in accordance with Federal security requirements and guidelines.

Our objectives were to determine whether the HHS Office of the Secretary (HHS OS) (1) accurately identified and inventoried its cloud information systems and components and (2) implemented security controls in accordance with Federal requirements and guidelines.

How OIG Did This Audit

We reviewed HHS OS's cloud information system inventory and its policies and procedures. We also analyzed the configuration settings of HHS OS's cloud environment using both a network vulnerability scanner and a cloud security assessment tool. Also, we performed penetration testing of selected cloud information systems in June and July 2022. We also conducted two email phishing campaigns that included a limited number of HHS OS personnel and cloud component users during this period. We contracted with Breakpoint Labs, LLC (BPL), to conduct the penetration test of HHS OS. We closely oversaw the work performed by BPL, and the assessment was performed in accordance with the agreed-upon Rules of Engagement document.

HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems

What OIG Found

HHS OS accurately identified the components within the cloud systems we were able to assess. However, HHS OS did not accurately identify and inventory all of its cloud systems in accordance with HHS security requirements. Also, although HHS OS implemented some security controls to protect its cloud systems, several key security controls were not effectively implemented in accordance with Federal requirements and guidelines. This occurred because certain HHS OS system owners and System Security Officers did not identify some of their information systems as cloud systems in accordance with HHS requirements. Also, HHS OS System Security Officers—most often assigned by business or system owners—do not always have the skill sets or experience necessary to adequately perform the roles and responsibilities for the job function as defined by NIST. Although System Security Officer roles and responsibilities are defined in HHS security policies, there is no standardized process for ensuring qualified System Security Officers are selected. This adversely affects HHS OS's ability to ensure security controls are effectively implemented. As a result, HHS OS data stored in the cloud systems we examined may potentially be at a risk of compromise.

What OIG Recommends and HHS Office of the Secretary Comments

We made a series of recommendations for HHS OS to improve key security controls over cloud information systems, including that it implement a strategy that includes leveraging cloud security assessment tools that identify misconfigurations and other control weaknesses in its cloud services, and develop and implement a policy and process to ensure qualified staff are assigned as System Security Officers for its cloud systems.

In written comments on our draft report, HHS OS concurred with our recommendations and indicated that it would implement them.

TABLE OF CONTENTS

INTRODUCTION..... 1

 Why We Did This Audit..... 1

 Objectives..... 1

 Background 2

 HHS Office of the Secretary 2

 Cloud Computing 2

 How We Conducted This Audit..... 3

FINDINGS..... 4

 HHS Office of the Secretary Inventory of Its Cloud Systems Was Inaccurate 5

 Several HHS Office of the Secretary Security Controls Were Not Effectively
 Implemented..... 5

RECOMMENDATIONS 8

HHS OFFICE OF THE SECRETARY COMMENTS 8

APPENDICES

 A: Audit Scope and Methodology..... 9

 B: Tools We Used To Conduct the Audit..... 13

 C: HHS and Federal Requirements..... 15

 D: HHS Office of the Secretary Comments 20

INTRODUCTION

WHY WE DID THIS AUDIT

In June 2019, the Office of Management and Budget published its updated *Federal Cloud Computing Strategy* to accelerate information technology (IT) modernization through agency adoption of cloud-based solutions. Since then, Federal agencies are increasingly adopting cloud services to address their IT needs and potentially save money and time to meet their critical missions. In 2022, the Department of Health and Human Services (HHS) reported that more than 30 percent of its 1,555 systems were cloud-based.

Federal agencies are required to protect Federal information processed or stored in cloud systems to ensure the confidentiality, integrity, and availability of the information. Considering the potential wide-scale impact that a successful cyberattack against cloud information systems (systems) may have across HHS, we are performing a series of audits that will examine whether HHS and its operating divisions (OpDivs) have implemented effective cybersecurity controls for cloud systems owned, operated, or maintained by HHS or its managed service provider contractors in accordance with HHS policy and Federal requirements and guidelines.^{1, 2}

We conducted this audit to determine whether the HHS Office of the Secretary (HHS OS) is securing its cloud systems and computing components (components) in accordance with HHS policies and Federal requirements, including security controls outlined by the National Institute of Standards and Technology (NIST).³

OBJECTIVES

Our objectives were to determine whether HHS OS (1) accurately identified and inventoried its cloud information systems and components and (2) implemented security controls for their cloud information systems in accordance with Federal requirements and guidelines.

¹ An information system is defined by the National Institute of Standards and Technology as “A discrete set of information components organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.”

² A managed service provider is an outsourced third-party company that takes on the responsibility of managing services on behalf of an organization. In the context of this audit, a managed service provider manages cloud systems on behalf of HHS.

³ Cloud computing components include virtual networks, servers, storage, applications, services, accounts, etc., within cloud information systems. NIST SP 800-53, Revision 4. Available online at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. Accessed on Oct. 24, 2023.

BACKGROUND

HHS Office of the Secretary

HHS's mission is to enhance the health and well-being of Americans by providing effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services. The HHS OS administers and oversees the organization, its programs, and its activities. The HHS OS Office of the Chief Information Officer (OCIO) is responsible for leading the development and implementation of IT infrastructure across the agency and providing support for IT operations management and IT security and privacy.

Cloud Computing

NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable virtualized computing components (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction by an organization.⁴ The cloud computing model is composed of the following three service models:



- **Infrastructure-as-a-Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing components where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
- **Platform-as-a-Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Software-as-a-Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not

⁴ NIST definitions of cloud computing terms in this report are contained in NIST Special Publication (SP) 800-145, "The NIST Definition of Cloud Computing." Available online at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Accessed on Dec. 5, 2023.

manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

As displayed in Table 1, each service model involves different shared security responsibilities between the organization (e.g., HHS) and the cloud service provider.

Table 1 – Cloud Computing Shared Security Responsibilities Matrix

| IaaS Security | PaaS Security | SaaS Security |
|---|----------------|--|
| Data | Data | Data |
| Application | Application | Application |
| Platform | Platform | Platform |
| Infrastructure | Infrastructure | Infrastructure |
| Physical | Physical | Physical |
| Responsibility | | |
|  | Organization |  Cloud Service Provider |

HHS OS leverages these cloud service models to process, store, or transmit certain HHS OS mission-related information. During our audit, approximately 45 percent of HHS OS’s information systems were hosted by cloud service providers. Our audit focused on HHS OS’s security responsibilities.

With significant increases in cyberattacks against the Federal Government, such as email phishing and privilege escalation, HHS OS cloud systems are potential targets for hackers.⁵ HHS OS cloud systems host sensitive data, including information related to judicial hearings, legal investigations, healthcare delivery services, and emergency response. These data, if compromised, may be used by adversaries to sabotage the confidentiality, integrity, and availability of HHS OS data hosted within cloud systems.

HOW WE CONDUCTED THIS AUDIT

For our audit, we examined certain security controls that HHS OS is responsible for implementing. The scope of the audit included all cloud systems owned, operated, and maintained by HHS OS or its managed service provider contractors. We reviewed HHS OS’s cloud system policies and procedures and determined whether the cloud systems inventory

⁵ A privilege escalation attack is a cyberattack designed to gain unauthorized privileged access into a system.

was generated in compliance with them. We assessed the configuration settings of HHS OS's cloud environment using both a network vulnerability scanner and a cloud security assessment tool to identify vulnerabilities and misconfigurations. Also, we performed penetration testing of selected cloud systems in June and July 2022 to determine whether the controls in place would detect or prevent cyberattacks.⁶ We specified the systems that were to be tested within the Rules of Engagement (RoE) signed by the Office of Inspector General (OIG), an OIG contractor, and HHS OS.

To assist us with the audit, we relied on the work of specialists. Specifically, we contracted with Breakpoint Labs, LLC (BPL), to conduct the penetration test of HHS OS. BPL provided subject matter expertise throughout the assessment of HHS OS's cloud systems. To simulate a real-world attack more closely, the penetration testing team was given no substantial information before the testing began. This scenario is known as a zero-knowledge, or Black Box, penetration test. The penetration testing team also completed two different email phishing campaigns during the audit period. We performed testing in accordance with the agreed-upon RoE document. We provided detailed documentation about our preliminary findings to HHS OS in advance of issuing our draft report.

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.

Appendix A contains the details of our audit scope and methodology, Appendix B describes the tools we used to conduct the audit, and Appendix C contains the Federal requirements.

FINDINGS

HHS OS accurately identified the components within the cloud systems we were able to assess. However, HHS OS did not accurately identify and inventory all of its cloud systems in accordance with HHS security requirements. Also, although HHS OS implemented some security controls to protect its cloud systems, several key security controls were not effectively implemented in accordance with Federal requirements and guidelines. As a result, HHS OS data stored in the cloud systems we examined may potentially be at a risk of compromise.

⁶ Penetration tests are intended to identify vulnerabilities and security flaws in systems, devices, and controls that are in place to protect customer information and components. This type of information security testing typically attempts to simulate attacks that are either internal to an organization's computer network (i.e., from employees or hired contractors) or outside an organization's network boundary (e.g., State sponsors and organized crime).

HHS OS INVENTORY OF ITS CLOUD SYSTEMS WAS INACCURATE

HHS requires all HHS entities to identify, register, and maintain a current and accurate inventory of cloud systems and its components. An accurate inventory provides an organization with the system information needed to effectively assess and manage risk. Specifically, an organization can more easily determine whether reported software vulnerabilities impact any of its systems if it can refer to an accurate inventory, and if so, timely apply patches. However, HHS OS's cloud systems inventory was inaccurate. We identified 13 HHS OS cloud systems not documented in HHS OS's inventory. We identified these systems through interviews with HHS OS IT personnel and cross-referencing the inventory list provided by HHS OS with its HHS Federal Information Security Modernization Act (FISMA) system list for FY 2022.⁷

According to HHS OS officials, HHS OS's inventory was inaccurate because certain HHS OS system owners and System Security Officers did not identify some of their information systems as cloud systems in accordance with HHS requirements. Additionally, HHS OS does not have any documented procedures to verify that its cloud system inventories are accurate and complete. As a result, HHS OS may not be effectively managing cybersecurity risks for all of its cloud systems. For example, HHS OS may be unaware that a misconfigured or unpatched cloud system susceptible to a cyberattack exists in its environment because the system was not inventoried, thereby making it unlikely that the system will be scheduled for patching to reduce the risk of a cyberattack.

SEVERAL HHS OS SECURITY CONTROLS WERE NOT EFFECTIVELY IMPLEMENTED

For the cloud systems we tested, we found several key security controls that were not effectively implemented and did not prevent our simulated cyberattacks during the "assumed breach" scenario we conducted as part of our penetration testing.⁸ Overall, we found 12 security controls that had not been implemented or did not comply with Federal requirements for the HHS OS cloud systems tested. During our testing, we were able to exploit some vulnerabilities to elevate our level of system privileges to access sensitive data (including personal identifiable information) and obtain unauthorized control of cloud computing components of 2 cloud systems. The most critical security control finding was related to multifactor authentication to privileged accounts. Table 2 (next page) lists the NIST SP 800-53,

⁷ FISMA requires Inspectors General to perform an annual independent evaluation of their agency's information security programs and practices to determine the effectiveness of those programs and practices. For FY 2022, HHS OIG conducted a performance audit of HHS's compliance with FISMA as of Sept. 30, 2022, based upon the FISMA reporting metrics defined by the Inspectors General. We received an inventory list as a part of this audit. See *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022* ([A-18-22-11200](#)), issued May 9, 2023.

⁸ "Assumed breach" is a scenario where a malicious threat actor compromises a legitimate user's account login credentials and uses them to access an information system.

Revision 4, security control findings that we identified. The findings are ordered by risk rating, as determined by OIG.

Table 2: HHS OS Cloud Systems Security Control Findings

| NIST SP 800-53, Revision 4, Security Control | Control No.* | Security Control Finding | Risk Rating |
|---|--------------|---|-------------|
| Multifactor Authentication to Privileged Accounts | IA-2(1) | HHS OS did not implement multifactor authentication for network access for three privileged accounts for one cloud system. | Critical |
| Information Flow Enforcement | AC-4 | HHS OS did not implement access controls on three cloud storage components to ensure sensitive data was not publicly accessible. | High |
| Least Privilege | AC-6 | HHS OS did not enforce access control policies for 27 cloud components to ensure authorized users were granted the minimum rights needed to perform their duties. | High |
| Flaw Remediation | SI-2 | HHS OS did not adequately identify, report, or correct system flaws in a timely manner for at least 25 cloud components. | High |
| Transmission Confidentiality and Integrity | SC-8(1) | HHS OS did not enforce web traffic encryption on one remote server. | High |
| Protection Of Information at Rest | SC-28 | HHS OS did not enforce cryptographic policies and procedures for one cloud system to protect data at rest. | Medium |
| Vulnerability Monitoring and Scanning | RA-5 | HHS OS did not adequately configure its vulnerability scanners to detect software flaws and improper configurations in one of its cloud systems. | Medium |

| NIST SP 800-53, Revision 4, Security Control | Control No.* | Security Control Finding | Risk Rating |
|---|--------------|---|-------------|
| Unsuccessful Logon Attempts | AC-7 | HHS OS did not configure two web applications hosted on one cloud system to limit the number of invalid logon attempts by a user. | Medium |
| Authenticator Management | IA-5 | HHS OS did not ensure access key rotation for four user accounts. Additionally, HHS OS did not protect authenticator content for at least 37 components from unauthorized disclosure. | Medium |
| Information Input Validation | SI-10 | HHS OS did not adequately verify information input for one public-facing web server hosted in the cloud. | Medium |
| Plan of Action and Milestones Process | PM-4 | HHS OS did not consistently implement a process to ensure that plans of action and milestone documentation meet HHS requirements. | Low |
| System Security Plan | PL-2 | HHS OS did not update its system security plans for eight cloud systems. | Low |
| *The Control No. is the abbreviation of the control family name and the number of the specific control within NIST SP 800-53, Revision 4. | | | |

The security control findings we identified occurred because HHS OS System Security Officers—most often assigned by business or system owners—do not always have the skill sets or experience necessary to adequately perform the roles and responsibilities for the job function, as defined by NIST. Although System Security Officer roles and responsibilities are defined in HHS security policies, there is no standardized process for ensuring qualified System Security Officers are assigned. This adversely affects HHS OS’s ability to ensure security controls are effectively implemented. In addition, HHS OS did not consistently confirm that required cloud security baselines were implemented and cloud services were secured in accordance with HHS security configuration guidance.

Failure to effectively implement required security controls places HHS OS cloud systems at potentially higher risk of malicious attacks by bad actors. The vulnerabilities we found may be

leveraged by adversaries who seek to steal or distort sensitive data, disrupt operations, and/or destroy the HHS OS cloud systems that support critical HHS programs. OIG has conducted multiple investigations involving Federal systems for which the principle of “least privilege” was not implemented, allowing individuals to access sensitive information beyond that which was needed to perform their job duties. This can result in criminals utilizing this information for personal financial gain.

Regarding our first phishing campaign, we sent a phishing email to 127 HHS OS employees with access to HHS OS cloud systems. The campaign did not reveal whether any of these emails were opened. This may have been due to email filtering technology or other defenses implemented by HHS OS that blocked our emails from being delivered. Regarding our second phishing campaign, we sent a different phishing email to 19 employees with access to a specific HHS OS cloud system. These emails were delivered to the target users’ email inboxes. Some employees clicked on a link directing them to our specially created website and others not only clicked on the link but also attempted to enter their credentials on the website. However, we were unable to obtain access to the targeted user accounts due to added security measures. The results of this phishing campaign were not considered systemic; therefore, we are not making a recommendation.

RECOMMENDATIONS

We recommend that the HHS Office of the Secretary:

- develop a procedure to ensure cloud system inventories are accurate and completed in accordance with HHS security requirements;
- remediate the 12 control findings in accordance with NIST SP 800-53;
- implement a strategy that includes leveraging cloud security assessment tools that identify misconfigurations and other control weaknesses in its cloud services, and remediate weak controls in a timely manner; and
- develop and implement a policy and process to ensure qualified staff are assigned as System Security Officers for its cloud systems.

HHS OFFICE OF THE SECRETARY COMMENTS

In written comments on our draft report, HHS OS concurred with our recommendations and indicated that it would implement them. HHS OS’s comments are included in their entirety as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The scope of this audit was all cloud systems identified in the agreed-upon RoE document. All tested systems are owned, operated, and maintained by HHS OS, HHS OS managed service provider contractors, or both. We focused the penetration test on public IP addresses and domain names, web applications, and cloud systems owned or operated by HHS OS or its managed service provider contractors. We audited the security controls for which HHS OS or its managed service provider contractors are responsible and did not audit the underlying infrastructure security controls that the cloud service provider is responsible for managing.

We performed our work remotely. Testing began June 15, 2022, and concluded July 18, 2022. During testing, we were not able to fully test some cloud systems because HHS OS did not provide the required access. In addition, the penetration testing team completed two phishing campaigns between June 15 and July 18, 2022. Our first campaign targeted 127 HHS OS cloud users. The second campaign targeted 19 HHS OS employees.

METHODOLOGY

We reviewed HHS OS policies and procedures related to the inventory of cloud systems and assessed whether required systems controls were in place and operating effectively in accordance with FedRAMP and NIST SP 800-53, Revision 4. We cross-referenced the inventory list that we received from HHS OS with the HHS FISMA system inventory list for FY 2022 to confirm completeness. We relied on the work of specialists to assist with utilizing network and web application penetration testing and social-engineering techniques. OAS contracted with BPL to conduct the penetration test of the HHS OS cloud systems. BPL provided subject matter experts who conducted the penetration test of systems identified in the RoE document for which we were provided access. In addition, BPL planned and executed two simulated email phishing campaigns against a subset of the HHS OS cloud users. OAS oversaw the work to ensure that all objectives were met, and testing was performed in accordance with generally accepted government auditing standards and the RoE document.

Our testing focused on HHS OS cloud systems. It included web application penetration testing to assess the security controls for target web applications. The intent was to find errors in the source code, produce unintended responses from the application, and identify any flaws in the application that can be used to access components or circumvent security controls. In addition, it included testing the HHS OS cloud systems from a Black Box and Gray Box perspective, along with two social engineering campaigns we launched within the testing timeline.⁹

⁹ Black Box Testing is a test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Gray Box Testing is a test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object.

To accomplish our objectives, OIG prepared the RoE document that outlined the general rules, logistics, and expectations for the penetration test.

In June 2022, we began reconnaissance and scope verification of cloud components owned, operated, and maintained by HHS OS. We then performed cloud penetration testing to determine whether internet-facing cloud systems were susceptible to exploits by an external attacker. We also tested to identify gaps in HHS OS's cloud defense mechanisms, cloud component configurations, and data exfiltration prevention and detection controls.

The penetration testing team performed procedures and testing activities specified in Table 3.

Table 3: Penetration Testing Methodology

| Infrastructure Testing | Description | Tools or Methods |
|---------------------------------|--|--|
| Enumeration | Activity aimed at identifying devices and components within the customer network and cross-referencing with provided inventory lists. | Testers utilized automated reconnaissance scanners and other analysis tools. |
| Vulnerability Assessment | Perform network-based vulnerability assessment of servers, workstations, and any other network device or appliance included in our scope. The assessment identifies vulnerabilities associated with network services, operating systems, and software. | Testers utilized automated vulnerability scanners and other analysis tools. |
| Penetration Testing | Attempt to exploit vulnerabilities identified from vulnerability scanning to determine the extent of the vulnerability and potential remediation steps that may be taken. | Testers utilized penetration testing tools and manual techniques. |

Web application penetration testing assesses the effectiveness of security controls of target web applications. The tests we performed were intended to find errors in the source code, produce unintended responses from the application, and identify any flaws in the application that can be used to exploit vulnerabilities identified because of weak controls. Table 4 (next page) describes our web application testing techniques.

Table 4: Web Application Testing Techniques

| Web Application Test Techniques | Description |
|---|--|
| Visible Code Review | Reviewed the available source of pages to identify code and/or comments that may provide useful information, hidden form variables, and directory names. |
| Role Function Testing or Role-Based Access Control | Verified that role-based access controls properly restrict or provide access to data within the application as defined by the business logic. |
| Error Handling | Analyzed error, debug, and exception messages originated from the web server or database that may reveal any information that may be useful to an attacker. |
| Forceful Browsing / Directory Brute Forcing | Attempted to discover directories and files by appending known or standard names to the URL. Based on information gathered, attempted to find sensitive information, debug, or log files. |
| Administration Interfaces | Attempted to locate known administration interfaces based on known information, and manually enter the directory and port of default administrative sites. Exploitation of the manufacturer default credentials, common credentials, and previously discovered credentials all may be attempted when testing these interfaces. |
| Parameter Tampering | Attempted parameter tampering, which is a technique that takes advantage of a lack of input validation on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL). Modifications to these parameters can be used to bypass the security mechanisms of the application. |
| SQL Injection | Attempted SQL injection, which is a technique used to take advantage of a lack of input validation on user-submitted data that are passed from the web application to a backend database. The user-submitted data are then executed by the database and can be used to bypass authentication or gain access to unauthorized information. |
| Session Management / Hijacking | Attempted session hijacking, which is a technique used to take control of a user's session after obtaining the authentication ID. The authentication ID can be obtained by brute force, reverse engineering, or captured through methods such as cross-site scripting (XSS). Once the authentication ID is obtained, a user's session can be hijacked. |
| Cross-Site Request Forgery (CSRF or XSRF) | Attempted CSRF, which is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. |

| Web Application Test Techniques | Description |
|-----------------------------------|--|
| Cross-Site Scripting (XSS) | Attempted XSS, which is a common vulnerability discovered in web applications that enables attackers to inject client-side scripts into web application pages that are processed by the server. XSS vulnerabilities vary in risk depending on the circumstances under which the vulnerability can be exploited and the presence of the exploits. |
| Directory Traversal | Attempted directory traversal (or path traversal), which is when vulnerabilities can be the result of poor security validation, sanitization, or both, of user-supplied inputs. Successful exploitation may allow the attacker to determine, read, or edit files and file structures on the remote server. |
| Command Injection | Attempted malicious code injection, which can be the result of poorly configured or coded applications. It can be used to run operating system commands on a vulnerable server, which can lead to a complete compromise of confidentiality, integrity, and availability. |

In June 2022, BPL conducted two different simulated phishing campaigns to determine whether HHS OS implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether HHS OS personnel were adequately trained to recognize and appropriately respond to such malicious emails. HHS OS provided a list to OIG of the employees who would be subject to BPL’s simulated phishing campaigns. The first campaign was designed to gather information about the user’s browser and computer operating systems, which could then be used as reconnaissance. The second campaign was designed for users to open emails and click on a link to a webpage to download a utility zip file containing our malicious executable.

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 meets the required standards based on our audit objectives.

APPENDIX B: TOOLS WE USED TO CONDUCT THE AUDIT

Droopescan

Droopescan is a plugin-based scanner that is used to identify any issues in Drupal-based content management systems. Droopescan is similar to network scanners like Network Mapper (Nmap) but is used to scan Drupal-based systems instead. Drupal is an open-source content management framework and is often used to manage and administer websites. Droopescan is often used to spot bugs and issues with the Drupal script, and can, potentially, be used to highlight any exploitable issues.

Nmap

Nmap is a free and open-source utility for network discovery and security auditing. Nmap is also utilized by penetration testers to obtain network inventory, manage service upgrade schedules, and monitor host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and operating system versions) they are running, what type of packet filters, or firewalls, are in use, and dozens of other characteristics.

Pacu

Pacu is an open-source Amazon Web Services (AWS) exploitation framework, designed for offensive security testing against cloud systems. Created and maintained by Rhino Security Labs, Pacu allows penetration testers to exploit configuration flaws within an AWS account, using modules to easily expand its functionality. Current modules enable a range of attacks, including user privilege escalation, backdooring of Identity and Access Management users, attacking vulnerable AWS Lambda functions, and much more.¹⁰

CloudMapper

CloudMapper is an open-source AWS cloud visualization tool used to analyze AWS cloud systems. CloudMapper generates interactive network diagrams of AWS accounts allowing penetration testers to understand AWS systems included in the audit scope.

Scout Suite

Scout Suite is an open-source, multi-cloud security-auditing tool that enables security posture assessment of cloud systems. Using the Application Programming Interfaces (APIs) exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and highlights risk

¹⁰ AWS Lambda is a serverless, event-driven computer service that lets a person run code for virtually any type of application or backend service without provisioning or managing servers.

areas.¹¹ Scout Suite was designed by security consultants/auditors. It is meant to provide a point-in-time, security-oriented view of the cloud account it was run in. Once the data has been gathered, all analysis can be performed offline.

Nessus

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language, a simple language that describes individual threats and potential attacks.

Shodan

Shodan is a search engine that allows users to search for various types of servers (webcams, routers, etc.) connected to the Internet using a variety of filters. Shodan provides information about the server software, what options the service supports, a welcome message, or anything else that the client can find out before interacting with the server.

Censys.io

Censys.io is a web-based search platform for assessing an attack surface for Internet connected devices. The tool can be used not only to identify Internet-connected components and Internet of Things/Industrial Internet of Things, but also Internet-connected industrial control systems and platforms.

Domain Dossier

The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just better understand how things are configured. These reports include the owner's contact information, registrar information, and registry information.

¹¹ An API is a set of defined rules that enable different applications to communicate with each other.

APPENDIX C: HHS AND FEDERAL REQUIREMENTS

FEDERAL REGULATIONS

DHS Cybersecurity and Infrastructure Agency (CISA) Binding Operational Directive (BOD) 18-01: Enhance Email and Web Security

DHS Cybersecurity and Infrastructure Agency (CISA) Binding Operational Directive (BOD) 18-01 requires all agencies to enforce the use of Hypertext Transfer Protocol Secure (HTTPS), and to use HTTP Strict Transport Security (HSTS) on its publicly accessible websites and web services.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Information systems and Organizations*, states:

AC-4 INFORMATION FLOW ENFORCEMENT (page F-14)

Control:

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on *[Assignment: organization-defined information flow control policies]*.

AC-6 LEAST PRIVILEGE (page F-18)

Control:

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS (page F-21)

Control:

The information system:

- a. Enforce a limit of *[Assignment: organization-defined number]* consecutive invalid logon attempts by a user during a *[Assignment: organization-defined time period]*; and
- b. Automatically *[Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]]* when the maximum number of unsuccessful attempts is exceeded.

IA-2(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) (page F-90)

Control:

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

PM-4 PLAN OF ACTION AND MILESTONES PROCESS (page G-4)

Control:

- a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
 1. Are developed and maintained;
 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
 3. Are reported in accordance with OMB FISMA reporting requirements.
- b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PL-2 SYSTEM SECURITY AND PRIVACY PLANS (page F-139)

Control:

- a. Develop security and privacy plans for the system that:
 1. Is consistent with the organization's enterprise architecture;
 2. Explicitly defines the authorization boundary for the system;
 3. Describe the operational context of the system in terms of missions and business processes;
 4. Provides the security categorization of the information system including supporting rationale;
 5. Describes the operational environment for the information system and relationships with or connections to other information systems;
 6. Provides an overview of the security requirements for the system;
 7. Identifies any relevant overlays, if applicable;
 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
- b. Distributes copies of the security plan and communicates subsequent changes to the plan to *[Assignment: organization-defined personnel or roles]*;
- c. Reviews the security plan for the information system *[Assignment: organization-defined frequency]*;

- d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
- e. Protects the security plan from unauthorized disclosure and modification.

RA-5 VULNERABILITY SCANNING (page F-153)

Control:

- a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - 1. Enumerating platforms, software flaws, and improper configurations;
 - 2. Formatting checklists and test procedures; and
 - 3. Measuring vulnerability impact;
- c. Analyzes vulnerability scan reports and results from security control assessments;
- d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and
- e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

SC-28 PROTECTION OF INFORMATION AT REST (page F-203)

Control:

The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].

SI-2 FLAW REMEDIATION (page F-215)

Control:

- a. Identify, report, and corrects information system flaws;
- b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
- d. Incorporate flaw remediation into the organizational configuration management process.

SI-10 INFORMATION INPUT VALIDATION (page F-229)

Control:

The information system checks the validity of [*Assignment: organization-defined information inputs*].

SC-8(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION (page F-193)

Control:

The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

HHS REQUIREMENTS

- HHS Policy for Information Security and Privacy Protection (IS2P).
- Minimum Security Configuration Standards Guidance.
- HHS Policy for IT System Inventory Management.
- HHS Standard for System Inventory Management.

APPENDIX D: HHS OFFICE OF THE SECRETARY COMMENTS



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the Chief Information Officer
Washington, D.C. 20201

DATE: June 3, 2024

TO: Amy J. Frontz, Deputy Inspector General for Audit Services

FROM: Jennifer Wendel, Chief Information Officer (Acting) Jennifer Wendel
Jennifer Wendel (Jun 3, 2024 10:55 EDT)

SUBJECT: *OIG Draft Report: HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems, A-18-22-08018*

The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) thanks the Office of the Inspector General (OIG) for your review of Security Controls for Certain Cloud Information Systems. We welcome the opportunity to respond to your report.

As requested, our office has reviewed the aforementioned report and has attached written comments regarding the validity of facts, actions taken and planned actions, based on your recommendations. We look forward to continuing our collaboration efforts to enhance cloud information system security and further implement safeguards and practices that protect HHS data and the health information of the American public.

If you have any questions or need additional information, please reach out to the OCIO Audit Liaison Lead, Christopher Reyes at Christopher.Reyes@hhs.gov or 202-923-9689.

Attachment A: Response from the Office of the Chief Information Officer (OCIO) regarding **HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems, A-18-22-08018**.

cc:

Jennifer Wendel, Chief Information Officer (Acting)
La Monte Yarborough, Deputy Chief Information Officer (Acting) & Chief Information Security Officer
Elizabeth Habib, Cybersecurity Director



ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding *HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems, A-18-22-08018*.

Recommendations

We recommend that the HHS Office of the Secretary:

1. Develop a procedure to ensure cloud system inventories are accurate and completed in accordance with HHS security requirements.

HHS Response: Concur

HHS OS provided an accurate inventory for SaaS systems as originally requested by OIG. HHS OS then provided an accurate inventory for public-facing IaaS systems when requested by OIG. HHS will develop a procedure to ensure that cloud system inventories are accurate and completed in accordance with HHS security requirements.

2. Remediate the 12 control findings in accordance with NIST SP 800-53.

HHS Response: Concur

HHS OS acknowledges this recommendation and will ensure that the 12 control findings are remediated in accordance with NIST SP 800-53.

3. Implement a strategy that includes leveraging cloud security assessment tools that identify misconfigurations and other control weaknesses in its cloud services, and remediate weak controls in a timely manner.

HHS Response: Concur

HHS OS currently assesses and remediates controls that are their responsibility. HHS OS will continue to implement a strategy that includes leveraging cloud security assessment tools that identify misconfigurations and other control weaknesses in its cloud services, and remediate weak controls in a timely manner.

4. Develop and implement a policy and process to ensure qualified staff are assigned as System Security Officers for its cloud systems.



ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding *HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems, A-18-22-08018*.

HHS Response: Concur

HHS OS will develop and implement a policy and process to ensure qualified staff are assigned as System Security Officers for its cloud systems.