Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE HEALTH RESOURCES AND SERVICES ADMINISTRATION SHOULD IMPROVE PREVENTIVE AND DETECTIVE CONTROLS TO MORE EFFECTIVELY MITIGATE THE RISK OF COMPROMISE

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

February 2023
A-18-20-08200

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 audits 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 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: February 2023
Report No. A-18-20-08200

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

The Health Resources and Services Administration Should Improve Preventive and Detective Controls To More Effectively Mitigate the Risk of Compromise

Why OIG Did This Audit

We conducted a cyber threat hunt assessment of the Health Resources and Services Administration's (HRSA's) information systems to independently assess the effectiveness of HRSA's cybersecurity defenses, conducted an intrusion analysis, and reviewed its incident response capabilities.

Our objectives were to determine whether: (1) HRSA's cybersecurity defenses were effective, (2) there was an active threat on the HRSA network or whether there had been a past cyber breach, and (3) HRSA was able to detect breaches and respond appropriately.

How OIG Did This Audit

We performed the cyber threat hunt of HRSA's endpoints between June and July 2020. We conducted the assessment on approximately 3,858 endpoints that HRSA manages. We contracted with Accenture Federal Services (AFS) to provide subject matter experts to conduct the cyber threat hunt on OIG's behalf. We closely oversaw the work performed by AFS, and the assessment was performed in accordance with generally accepted government auditing standards and agreed-upon Rules of Engagement among OIG, AFS, and HRSA.

What OIG Found

Although HRSA had implemented some security controls for detecting and preventing threats on its network, HRSA's cybersecurity controls needed improvements to better detect and prevent cyber threats on its network. We found multiple security controls at HRSA that were not operating effectively, including controls related to malicious code protection and protection against unauthorized installation of software by users. Although we did not identify evidence of a past breach, we found three active threats on the HRSA network. We promptly shared these significant findings with HRSA during our audit period. Lastly, we concluded that HRSA was able to detect certain breaches and respond appropriately. We based this conclusion on the fact that HRSA was already in the process of investigating two of the three active threats that we had identified before we notified it of our findings.

The security control failures that we identified occurred because HRSA had not updated security configurations to align with the most current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls and had not implemented procedures to assess and monitor the NIST controls on its endpoints. As a result of HRSA not correctly implementing these controls, these threats could increase the endpoint or network attack surfaces, or bypass current organizational security policies and controls. The likelihood of successful cyberattacks and unauthorized access to sensitive data is greater in environments where these types of security controls are not enforced.

What OIG Recommends and HRSA Comments

We recommend that HRSA: (1) remediate the nine security control findings we identified, (2) update security configurations to align with the most current NIST SP 800-53 security controls, and (3) implement policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 and remediate weak controls timely.

In written comments on our draft report, HRSA concurred with our findings and recommendations and described the actions it has taken or plans to take to address them.

TABLE OF CONTENTS

INTRODUCTION 1

Why We Did This Audit 1

Objectives 1

Background 1

Health Resources and Services Administration 2

How We Conducted This Audit 2

FINDINGS 4

RECOMMENDATIONS 7

HRSA COMMENTS 7

APPENDICES

A: Audit Scope and Methodology 8

B: Tools We Used to Conduct the Audit 14

C: Federal Requirements 15

D: HRSA Comments 20

INTRODUCTION

WHY WE DID THIS AUDIT

The Department of Health and Human Services (HHS), Office of Inspector General (OIG), Office of Audit Services (OAS), Cybersecurity and Information Technology Audit Division (CITAD), recently conducted a series of penetration test audits to evaluate the effectiveness of security controls at eight HHS operating divisions (OpDivs). These audits provided a snapshot of HHS's cyber defenses at all eight OpDivs and identified almost 200 vulnerabilities across HHS.[1]

Based on the results from the penetration test audits, we initiated a series of cyber threat hunts on a subset of HHS OpDivs' information systems to identify potential indicators of compromise (IOCs) on those systems and to determine whether any breaches have gone undetected.[2] As part of this body of work, we conducted a cyber threat hunt of selected Health Resources and Services Administration (HRSA) information systems in accordance with guidance outlined by the National Institute of Standards and Technology (NIST).

OBJECTIVES

Our objectives were to determine whether:

- HRSA's cybersecurity defenses were effective;
- there were any active threats on the HRSA network or whether there had been a past cyber breach; and
- HRSA was able to detect breaches and respond appropriately.[3]

BACKGROUND

Computer hackers use a variety of techniques in their persistent attempts to gain unauthorized access to sensitive Government information systems and data. Common attack methods include denial of service, spear phishing, unauthorized malicious software (malware), and

[1] Report in Brief for the *Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks* (A-18-18-08500), issued March 1, 2019.

[2] Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats.

[3] An active threat is an ongoing event or behavior with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.

Structured Query Language (SQL) Injection attacks against websites.[4, 5] HRSA's cybersecurity personnel must successfully defend against these attack methods while also addressing the risks presented by adversaries through the software supply chain and other attack vectors.

We recognize that cybersecurity defenses will not prevent all breaches from occurring. However, to reduce the likelihood of a breach, agencies must ensure that proper controls (such as effective patching, proper configuration management, access restrictions, and physical protections) are in place and operating effectively. Two of the best tactics to test the effectiveness of the control environment are penetration testing and cyber threat hunts that search for IOCs.

Health Resources and Services Administration

HRSA is the primary Federal agency for improving health care for people who are geographically isolated and those who are economically or medically vulnerable.[6] Tens of millions of Americans receive quality, affordable health care and other services through HRSA's 90-plus programs and more than 3,000 grantees. HRSA also supports the training of health professionals, the distribution of providers to areas where they are needed most, and improvements in health care delivery. In addition, HRSA oversees organ, bone marrow, and cord blood transplants. It compensates individuals harmed by vaccinations and maintains databases that flag providers with a record of health care malpractice, waste, fraud, and abuse that Federal, State, and local agencies use for their programs. Because of the importance of HRSA's mission and the value of sensitive patient information stored on its networks, HRSA could be a target for cybercrime and cyber espionage. Also, some grantees that interface with HRSA have limited cybersecurity resources to mitigate threats and therefore could introduce risk to HRSA's network.

HOW WE CONDUCTED THIS AUDIT

We performed the cyber threat hunt of the HRSA network in June and July 2020. To assist us with the cyber threat hunt, we relied on the work of specialists. OIG contracted with Accenture Federal Services (AFS) to perform a cyber threat hunt on a subset of HRSA's information systems. AFS provided subject matter expertise throughout the cyber threat hunt from March through August 2020. AFS performed the cyber threat hunt in accordance with the agreed-upon Rules of Engagement (ROE) document, signed and completed by OIG, AFS, and

[4] SQL Injection Attacks exploit websites that pass insufficiently processed user input to the database, allowing the attacker to read sensitive data from the database or perform other database functions through the website.

[5] Malware is any software program designed to damage or execute unauthorized actions on a computer system. Examples of malware include computer viruses, worms, and Trojan horses.

[6] HRSA Agency Overview. Available online at: https://www.hrsa.gov/sites/default/files/hrsa/about/hrsa-agency-overview.pdf. Accessed on October 18, 2022.

HRSA management in March 2020. To provide the most accurate results possible, we asked HRSA officials to not alert individual users about the cyber threat hunt while it was in progress.

Cyber threat hunts assist information technology (IT) professionals in detecting data breaches, malware infections, and other threatening activities. Our cyber threat hunts searched for IOCs, which are data that indicate potentially malicious activity on a system or network. For example, during the HRSA cyber threat hunt, we looked for unusual outbound network traffic or connections to foreign Internet Protocol (IP) addresses, abnormal user account activity, digital signatures of malware files, suspicious registry, or system file changes, and examined adversary tactics and techniques based on the MITRE ATT&CK framework.[7] We describe our cyber threat hunt methodology in Appendix A.

As outlined in the ROE, AFS reported any significant vulnerabilities and IOCs it identified during the cyber threat hunt to us. To verify that the reported vulnerabilities did not have national security implications or were related to an ongoing investigation, we referred those matters to our Office of Investigations (OI) Computer Crimes Unit (CCU) for further review. The OI CCU assessed the reported vulnerabilities and shared its recommendations with us. We then shared the vulnerabilities and the recommended actions with HRSA.

To begin the cyber threat hunt, we worked with HRSA to deploy an Endgame sensor package across endpoints in the HRSA network.[8, 9, 10] The sensor was configured to communicate with our Endgame server. We assisted HRSA in deploying the Endgame sensor package to approximately 3,858 endpoints identified by HRSA. HRSA officials informed us that they deployed the Endgame sensor to all endpoints in the HRSA network.

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.

[7] MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge. The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

[8] In October 2019, Elastic N.V. acquired Endgame becoming part of the Elastic Security Platform.

[9] Endgame is an application software tool used to identify IOCs on a system or network and to analyze systems for active threats. Threats are rated with a numerical malware score indicating the likelihood of malware.

[10] An endpoint is any device that is physically or virtually an end point on a network. Laptops, desktops, mobile phones, tablets, servers, and virtual environments can all be considered endpoints.

Appendix A contains the details of our audit scope and methodology, Appendix B contains the tools we used to conduct the audit, and Appendix C contains the Federal requirements we used to evaluate HRSA's controls.

FINDINGS

Although HRSA had implemented some security controls for detecting and preventing threats on its network, HRSA's cybersecurity controls needed improvements to better detect and prevent cyber threats on its network. We found multiple security controls that were not operating effectively. The most critical of which were related to malicious code protection and protection against unauthorized installation of software by users. Although we did not identify evidence of a past breach, we found three active threats on the HRSA network.[11] Specifically, we found software exfiltrating user data to an unapproved external non-HHS system; certain HRSA systems accessing the dark net; and a HRSA system communicating with an unknown web domain. We promptly shared these significant findings with HRSA during our audit period for immediate follow up. Lastly, we concluded that HRSA was able to detect certain breaches and respond appropriately. We based this conclusion on the fact that HRSA was already in the process of investigating two of the three active threats that we had identified before we notified HRSA of our findings.

The Federal Information Security Modernization Act (FISMA) of 2014, section 3554 (P.L. 113–283) directs agencies to comply with the policies, procedures, standards, and guidelines promulgated under section 11331 of title 40, which requires, in part, that Federal information systems meet the minimum information security system requirements described under section 20(b) of NIST (15 U.S.C. 278g-3). In response to FISMA, NIST developed the Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* as a mandatory Federal standard. To comply with the Federal standard, Federal agencies must meet the minimum security requirements using NIST Special Publication (SP) 800-53. HRSA did not correctly implement the NIST SP 800-53, Revision 4, security controls in the Table on the next page.

[11] An active threat is an ongoing cyber threat event or threat activity.

Table: Weak HRSA Systems Security Controls, Ordered by Risk Rating

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†
Malicious Code Protection	HRSA did not adequately employ malicious code protection mechanisms at the entry and exit points on certain information systems to detect and eradicate malicious code attacks.	SI-3	Critical
User Installed Software	HRSA did not adequately govern the installation of software by users and enforce and monitor software installation policies in its network.	CM-11	Critical
Least Privilege	HRSA did not adequately employ the principle of least privilege to provide users only with the access needed to accomplish assigned tasks based on their organizational missions and business functions.	AC-6	High
Unsuccessful Logon Attempts	Certain HRSA systems did not adequately enforce limits for consecutive invalid logon attempts by a user and did not lock the accounts when a user exceeded the maximum number of unsuccessful attempts.	AC-7	High
Session Lock	HRSA's information system did not adequately prevent further access to the system by initiating a session lock after a period of inactivity or upon receiving a request from a user. In addition, HRSA's information system did not effectively implement session lock controls.	AC-11	High
Information Flow Enforcement	HRSA did not enforce approved authorizations for controlling the flow of information within the information system and between interconnected systems.	AC-4	High

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†
Account Management	HRSA did not adequately implement controls to create, enable, modify, disable, and remove information system accounts. In addition, HRSA did not adequately review accounts for compliance with account management requirements or establish a process for reissuing shared/group account credentials (if deployed) when individuals were removed from the group.	AC-2	Moderate
Authenticator Management	HRSA did not effectively manage information system authenticators (e.g., passwords) by ensuring that unencrypted static authenticators were not embedded in applications or access scripts or stored on function keys.	IA-5(7)	Moderate
Secure Name / Address Resolution Service (Authoritative Source)	HRSA did not implement authentication and integrity verification processes for host and service name resolution.	SC-20	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.

† NIST SP 800-53, Revision 4, Security Control Risk Rating as determined by CITAD.

The security controls were not correctly implemented because HRSA had not established policies and procedures to periodically assess whether controls were in place and operating effectively in accordance with NIST SP 800-53 or did not remediate known weak controls in a timely manner.

As a result of HRSA not correctly implementing these controls, cyber threat actors may be able to successfully carry out a cyberattack or insiders may be able to bypass HRSA security policies and controls that could allow them to connect to illegal websites, access the dark net, or exfiltrate sensitive data and go undetected. The likelihood of successful cyberattacks and unauthorized access to sensitive data is greater in environments where these types of security controls are not enforced.

RECOMMENDATIONS

We recommend that the Health Resources and Services Administration:

- remediate the nine security control findings we identified,

- update security configurations to align with the most current NIST SP 800-53 security controls, and

- implement policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 and remediate weak controls timely.

HRSA COMMENTS

In written comments on our draft report, HRSA concurred with all of our findings and recommendations and described actions it has taken or plans to take to address them. HRSA's comments are included in their entirety as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

To assist us with the OIG cyber threat hunt, we relied on the work of specialists. OAS contracted with AFS to conduct the cyber threat hunt of HRSA. AFS provided subject matter experts throughout the assessment. We performed the cyber threat hunt of HRSA's network in June and July 2020. Before the start of the assessment, HRSA completed a Network Environment Survey document. As requested in the Network Environmental Survey, HRSA provided us with a list of public-facing network subnets. We provided to HRSA an Endgame sensor software package that HRSA deployed to systems authorized by HRSA leadership.

Regarding the testing of internal controls during our audit, we identified the component "Control Activities" as significant to our audit objectives.[12] We reviewed various NIST SP 800-53, revision 4, security controls including, but not limited to:

- AC-2 Account Management
- AC-4 Information Flow Enforcement
- AC-6 Least Privilege
- AC-7 Unsuccessful Logon Attempts
- AC-11 Session Lock
- CM-11 User Installed Software
- IA-5(7) Authenticator Management
- SC-20 Secure Name / Address Resolution Service (Authoritative Source)
- SI-3 Malicious Code Protection

Based on our cyber threat hunt, we assessed the operating effectiveness of these internal controls and identified deficiencies that we believe could affect HRSA's ability to detect, or effectively prevent, certain cyberattacks. The internal control deficiencies we identified are listed as security control findings in the Findings section of this report. However, the cyber threat hunt we performed may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

[12] *Standards for Internal Control in the Federal Government, GAO-14-704G.*

We conducted the assessment on approximately 3,858 endpoints with varying operating systems. Over the course of the cyber threat hunt assessment, we received more than 6,600 individual alerts through the Endgame platform.

METHODOLOGY

To accomplish our objectives, OIG and HRSA prepared the ROE document that outlined the general rules, logistics, and expectations for the cyber threat hunt assessment. We obtained signatures from HRSA and AFS management indicating that they agreed with the ROE.

OAS contracted with AFS to perform a cyber threat hunt on a subset of HRSA's information systems. AFS provided subject matter expertise throughout the cyber threat hunt. AFS performed the cyber threat hunt in accordance with the agreed-upon in the ROE document. We conducted our cyber threat hunt from the OIG/OAS Cyber Range.

To accomplish our objectives, we:

- reviewed Federal and HRSA policies and procedures;
- interviewed cybersecurity personnel;
- assisted HRSA in deploying the Endgame sensor software to HRSA endpoints;
- executed the Cyber Hunt Methodology;
- assessed HRSA systems for anomalies that posed a significant risk to the HRSA enterprise network;
- responded to Endgame-generated alerts and hunted across the HRSA environment for anomalies among processes, persistence mechanisms, and user log-ons; [13] and
- shared significant findings with HRSA during the audit and provided detailed documentation about our findings in advance of issuing our draft report.

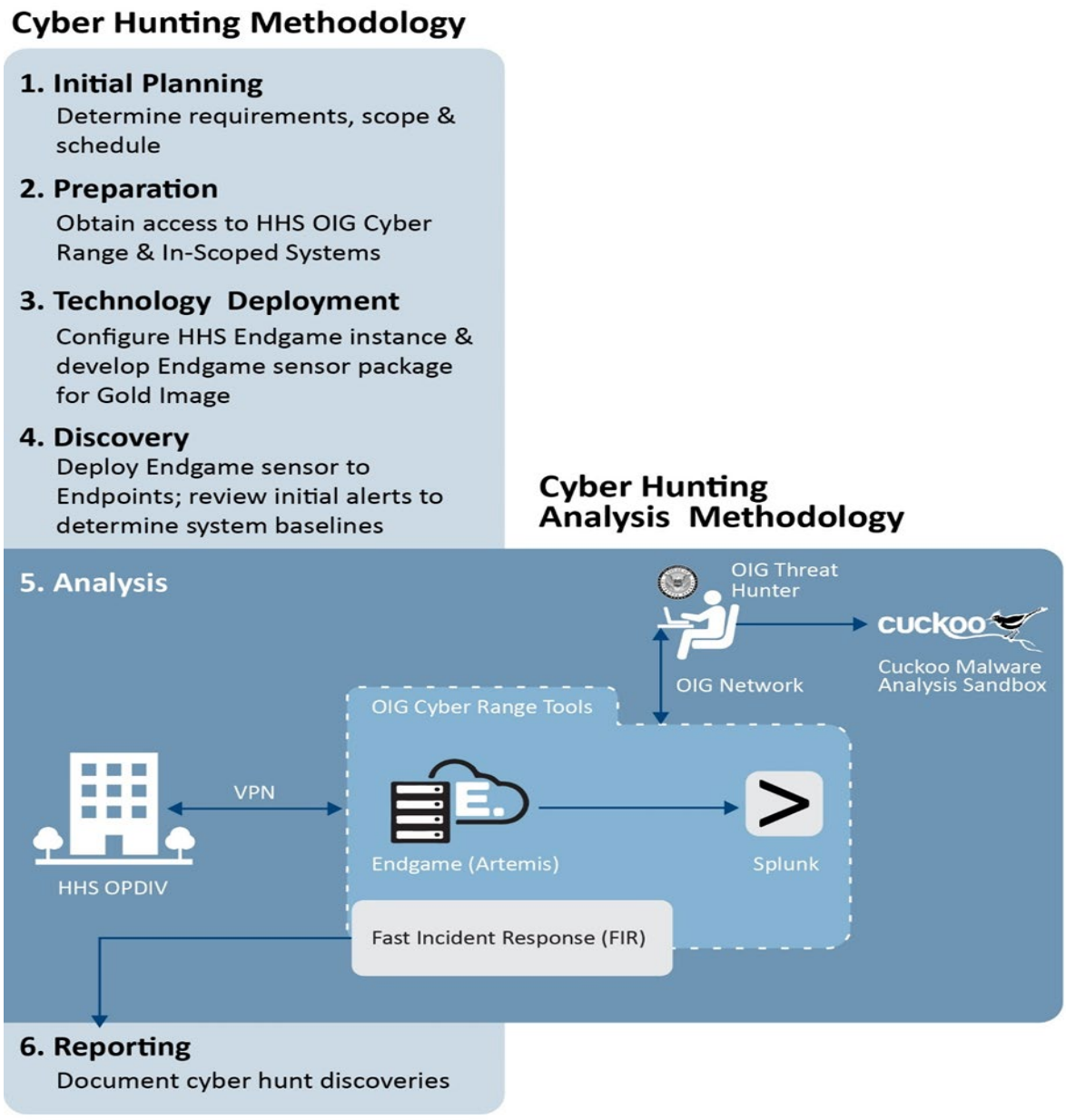
We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[13] Persistence Mechanisms are techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

CYBER HUNT METHODOLOGY

The Cyber Hunt methodology consisted of six core phases: Initial Planning, Preparation, Technology Deployment, Discovery, Analysis, and Reporting. (See the figure below).

Figure: Cyber Hunt Methodology Overview



Initial Planning

We worked with HRSA to determine the requirements of the Cyber Hunt, defined the scope of IT assets on which to deploy tools for hunting, and developed the schedule for all phases of the Cyber Hunt.

Preparation

We obtained the necessary access to the OIG Cyber Range and to the systems identified as in-scope by HRSA during the Initial Planning Phase.

Technology Deployment

We configured the Endgame instance in the OIG Cyber Range and developed the Endgame sensor package deployed by HRSA to their endpoints (workstations and servers).[14]

Discovery

HRSA deployed the Endgame sensors to the endpoints. Once deployed, the endpoints began to report data back to the Endgame instance in the form of alerts. We reviewed these alerts to understand the system baselines and to remove any false positive data.

Analysis

The Cyber Hunt Analysis phase focused on searching for threat actor activity using known indicators of compromise and determining the impact of these threats on HRSA systems and the network. We focused on analyzing anomalies in the HRSA infrastructure and determining whether these anomalies were valid threats to the HRSA infrastructure. These anomalies were identified by feeding Endgame data into Splunk, which is used to analyze the data for any malicious or suspicious activity.[15] Endgame allowed us to analyze system activity and to identify and triage security concerns.

Reporting

This phase involved documenting the Cyber Hunt discoveries. This included disclosing affected systems and providing recommendations on how to improve the security posture of the HRSA network environment and systems contained therein.

[14] An "instance" is a virtual server in the Amazon Web Services cloud environment.

[15] Splunk is a software platform to search, analyze, and visualize the machine-generated data gathered from the websites, applications, sensors, devices, etc.

CYBER HUNT ANALYSIS METHODOLOGY

While conducting the Analysis phase, we used the following methodology to determine the validity of an alert. We first reviewed the alert to determine whether it was a type that warranted further analysis. If further analysis was needed, we then began full analysis of the alert utilizing tools such as Artemis and the Cuckoo Sandbox.[16, 17]

Alerts

The Cyber Hunt began by addressing Endgame alerts, which are system-generated notifications that detect potentially malicious activity on monitored endpoints. This type of activity may include but is not limited to ransomware, process injection, or permission theft.[18, 19] We used the alerts to help identify abnormal behavioral patterns that might require analysis. Alerts are the result of previously configured tradecraft protections, which are enabled when a sensor is deployed to an endpoint.[20] They specify what endpoint activity the sensor monitors and the action the sensor should take if it detects potential malicious activity. In general terms, alerts were generated for any activity that was determined to be outside of the baseline for that system.

Manual Analysis

We created custom searches to collect and analyze targeted data across multiple endpoints. This was initiated by assigning one or more hunts to selected endpoints. These hunts then searched for specified artifact values in the target device(s) and reported findings back to us.[21] Some of the items we searched for were IOCs that we had already found in Endgame alerts during the Cyber Hunt. We also searched for specific registry values, process trees, specific binaries, user account activity, and network connections that we had identified as a possible

[16] Artemis is Endgame's natural language interface to facilitate queries and expedite detection and responses.

[17] Cuckoo Sandbox is an open-source automated malware analysis system.

[18] Process injection is a defense evasion technique employed often within malware, which runs custom code within the address space of another process.

[19] Permission theft is the unauthorized theft of identity or permissions.

[20] Endgame's tradecraft protections monitor system activity in real-time and alert on techniques and tactics defined in the MITRE ATT&CK framework.

[21] An artifact value is a piece of data that may or may not be relevant to an investigation/response.

threat.[22, 23, 24] We then filtered the data by tailored analytics and distinguished actual incidents from false positives.

The main goal of this phase was to identify suspicious activity and report it to HRSA so that it could take remedial action.

[22] A registry value is an actual entry within the Microsoft's Windows Registry that contains specific instructions that Windows and applications look for to perform its functions.

[23] A binary describes a numbering scheme in which there are only two possible values for each digit: 0 and 1. The term also refers to any digital encoding/decoding system.

[24] A process tree is a tool for visualizing and archiving the processes of planning and development projects in chronological order. It brings several types of information together in one place, thus creating a general picture of the matter at hand.

APPENDIX B: TOOLS WE USED TO CONDUCT THE AUDIT

Endgame

Endgame is a centralized software application that monitors endpoints (e.g., workstations or servers). An endpoint is a remote computing device that communicates with a network to which it is connected. Endgame sensors collect data and perform active queries on individual endpoints across the OpDiv network. Endgame also collects data to feed Splunk.

Splunk

Splunk is a robust analytical tool used to collect and visualize data. Splunk, designed to be highly scalable and customizable, was used to review and parse data in bulk. Splunk's data search allows for a comparison of historical data across all endpoints. Splunk's ability to exclude known good artifacts was leveraged to search for an entire list of IOCs across Endgame collection results.

Artemis

We used Endgame's artificial intelligence assistant, Artemis, to combine hunts for both current and historical process data across one or more specified endpoints. Artemis allowed limited historical data queries, which allowed us to search for and analyze events over time.

Cuckoo Sandbox

An OIG internal Cuckoo Sandbox environment is used to analyze and reverse engineer binary files. Cuckoo Sandbox reports provided us with additional IOCs, such as malicious websites, initiated network connections, malware classifications, and other relevant details to triage suspicious binary files. This information was then used to tailor additional manual analysis against the OpDiv environment.

Fast Incident Response

Fast Incident Response (FIR) is a cybersecurity incident management platform designed for agility and speed. It allows for easy creation, tracking, and reporting of cybersecurity incidents. FIR was used in the reporting phase to document potential incidents.

APPENDIX C: FEDERAL REQUIREMENTS

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

> AC-2 Account Management (page F-7)
>
> Control: The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both.
>
> 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 (pages F-18-19)
>
> 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. Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.
>
> Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least

privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

AC-7 Unsuccessful Logon Attempts (page 21)

Control: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

AC-11 Session Lock

Control: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.

CM-11 User-Installed Software (page F-76)

Control: The organization:

a. establishes policies governing the installation of software by users;

b. enforces software installation policies, and

c. monitors policy compliance.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed

software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

IA-5(7) Authenticator Management | No Embedded Unencrypted Static Authenticators (page F-97)

Control: The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Supplemental Guidance: Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

SC-20 Secure Name/Address Resolution Service (Authoritative Source) (page F-199)

Control: The information system:

a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SI-3 Malicious Code Protection (page F-217)

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

NIST SP 800-66, Revision 1, ***An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,*** *section 4.18, Transmission Security,* states that organizations should "[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops,* states:

> Detection and Analysis. Organizations should strive to detect and validate malware incidents rapidly to minimize the number of infected hosts and the amount of damage the organization sustains.
>
> Section 3.4.4 Content Filtering/Inspection (page 14): Organizations should also block undesired web browser popup windows, as a form of content filtering. Some popup windows are crafted to look like legitimate system message boxes or websites, and can trick users into going to phony websites, including sites used for phishing, or authorizing changes to their hosts, among other malicious actions. Most web browsers can block popup windows, and third-party popup blockers are also available.

HHS Information Systems Security and Privacy Policy, (page 40), states:

> The responsibilities of the Department's users and contractors operating on behalf of the Department include, but are not limited to:
>
> 31.1 Reading, acknowledging, signing, and complying with the HHS [Rules of Behavior] RoB, and/or the OpDiv- and system-specific RoB, before gaining access to the Department's systems and networks.

HHS Rules of Behavior, Version 2.1, Use of HHS Information and IT Resources Policy (page 9), states:

> [HHS users] must protect [their] password . . . .
>
> Not share passwords or provide passwords to anyone, including system administrators. I must protect my passwords, Personal Identity Verification (PIV) card, Personal Identification Numbers (PIN) and other access credentials from disclosure and compromise;
>
> Promptly change my password when required by HHS policy and if I suspect that it has been compromised;
>
> HHS expects personnel to conduct themselves professionally in the workplace and to refrain from using GFE, email, third-party websites and applications (TPWAs) (e.g., HHS social media sites and cloud services, etc.) and other HHS information resources for activities that are not related to any legitimate/officially-sanctioned HHS business purpose.

> All privileged users (e.g., network/system administrators, developers, etc.) shall read, acknowledge, and adhere to the HHS/OpDiv Privileged User RoB prior to obtaining a privileged user account and at least annually thereafter. The acknowledgment of the RoB, which affirms that privileged users have read and understand the HHS/OpDiv RoB for Privileged Users, may be obtained by either hardcopy written signature or by electronic acknowledgement or signature.

HHS's Rules of Behavior for General Users — Strictly Prohibited Activities, **section 1.5,** states that "sharing, storing, or disclosing sensitive information with third-party organizations and/or using third-party applications (e.g., DropBox, Evernote, iCloud, etc.) unless authorized in accordance with HHS policies."

HHS's Rules of Behavior for General Users — A. HHS Information Systems, states that "when using and accessing HHS information resources and systems . . .,[users] must [n]ot reconfigure systems and modify GFE, install/load unauthorized/unlicensed software or make configuration changes without proper official authorization."

APPENDIX D: HRSA COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Health Resources and Services Administration

Rockville, MD 20857

DATE: December 22, 2022

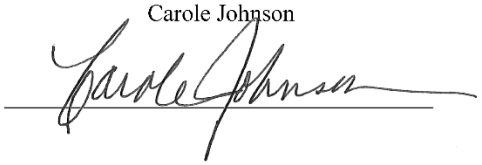
TO: Inspector General

FROM: Carole Johnson, Administrator

SUBJECT: OIG Draft Report: *The Health Resources and Services Administration Should Improve Preventive and Detective Controls to More Effectively Mitigate the Risk of Compromise* (A-18-20-08200)

Attached is the Health Resources and Services Administration's response to the above referenced report. If you have any questions, please contact Sandy Seaton in our Office of Federal Assistance Management at (301) 443-2432.

Carole Johnson



Attachment

Health Resources and Services Administration's Comments on the OIG DRAFT Report – "The Health Resources and Services Administration Should Improve Preventive and Detective Controls to More Effectively Mitigate the Risk of Compromise" (A-18-20-08200)

The Health Resources and Services Administration (HRSA) appreciates the opportunity to respond to the draft report referenced above. HRSA's responses to the Office of Inspector General (OIG) draft recommendations are as follows:

GENERAL COMMENTS

HRSA appreciates the opportunity to work with the OIG Team on this important issue. HRSA Security Program actions include strengthening our documented processes and procedures as detailed below.

OIG RECOMMENDATION #1

Remediate the nine security control findings OIG identified.

HRSA's RESPONSE

HRSA concurs. HRSA is working on addressing the finding.

OIG RECOMMENDATION #2

Update security configurations to align with the most current NIST SP 800-53 security controls.

HRSA RESPONSE

HRSA concurs. HRSA is working on addressing the finding.

OIG RECOMMENDATION #3

Implement policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with NIST SP 800-53 and remediate weak controls timely.

HRSA RESPONSE

HRSA concurs. HRSA addressed the finding.