Department of Health and Human Services
Office of Inspector General

Office of Audit Services

December 2024 | A-18-22-07002

Summary Report of Prior Office of Inspector General Cyber Threat Hunt Audits of Eight HHS Operating Division Networks

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

Summary Report of Prior Office of Inspector General Cyber Threat Hunt Audits of Eight HHS Operating Division Networks

Report No. A-18-22-07002

December 2024

Table of Contents

- Why We Performed These Audits
- Overview and Background
- Audit Objectives
- How We Did These Audits
- HHS's Comments on Interim Summary Report
- What We Found
- Common Root Causes
- Potential Effects of Ineffective Controls
- OpDiv Responses to OIG Recommendations
- Implementation of Recommendations
- Recommendations to HHS's OCIO
- HHS OCIO's Comments and OIG Response
- Appendix: Scope, Methodology, Applicable Criteria, and HHS OCIO Comments

Why We Performed The Prior Audits

- Prior to our Cyber Threat Hunt (CTH) audits, we conducted a series of penetration test audits to evaluate the effectiveness of security controls at eight HHS operating divisions (OpDivs). The results of the penetration test audits provided a snapshot of HHS's cyber defenses at the eight OpDivs and identified almost 200 vulnerabilities across HHS.
- Based on the results from our penetration test audits, we initiated a series of CTH audits 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.

Overview

This summary report provides the Department of Health and Human Services (HHS) Office of Chief Information Officer (OCIO) with:

- actionable information regarding its cybersecurity posture,
- information on common vulnerabilities found at eight of its OpDivs,
- the implementation status of our recommendations previously made to the OpDivs, and
- recommendations to strengthen HHS's cybersecurity posture and mitigate weaknesses.

Background

- Government information systems, especially those managed by HHS, are under constant threat from cyberattacks such as denial of service, spear phishing, malware, and exploitation of software vulnerabilities. HHS cybersecurity teams must defend against these threats to mitigate risks posed by adversaries.
- Although cybersecurity defenses cannot prevent all breaches, agencies can minimize risks by effectively implementing controls in accordance with National Institute of Standards and Technology (NIST) cybersecurity requirements to detect a possible or actual cyberattack, investigate it timely, and respond appropriately to mitigate negative effects.
- Cyber threat hunt assessments are a way to assist information technology professionals in detecting cyber threats.

Audit Objectives

The objectives of the prior CTH audits performed at 8 HHS's OpDivs were to determine:

- whether there were active threats on the OpDiv's network or there had been past cyber breaches,
- whether the OpDiv's cybersecurity defenses were effective, and
- the OpDiv's ability to detect breaches and respond appropriately.

How We Did The Prior Audits

- We contracted with Accenture Federal Services (AFS) to assist with conducting our CTH audits.
- AFS provided subject matter experts during the initial planning, preparation, technology deployment, discovery phases, and analysis and reporting of the audits.
- We conducted the CTH audits at 8 HHS OpDivs from 2018 through 2020.
- Our audits were performed in accordance with agreed-upon rules of engagement between OIG, AFS, and the OpDivs.

OpDivs and Total Servers and Workstations Assessed

Food and Drug Administration	~27,000
HHS Office of the Secretary	~9,700
Indian Health Services	~18,000
National Institutes of Health	~61,000

OpDivs and Total Servers and Workstations Assessed

Administration for Children and Families	~80
Health Resources and Services Administration	~3,800
Substance Abuse and Mental Health Services Administration	6
Centers for Medicare and Medicaid Services	~8,400

HHS's Comments on Interim Summary Report

In March 2021, we issued an interim summary report to the HHS OCIO on the results of our first four CTH audits to ascertain any actions taken or planned in response to the threats and vulnerabilities we identified. In response to our interim summary report, OCIO informed us that it had no comments.

What We Found

Overall, the eight OpDivs lacked adequate preventative and detective controls to effectively mitigate the risk of compromise (i.e., threats that evade existing security solutions).

- We identified 19 active threats targeting some OpDivs' servers and workstations during our audits. We immediately communicated the discoveries to the OpDivs as part of our audit process.
- We identified a total of 138 vulnerabilities related to 19 NIST Special Publication (SP) 800-53, Revision 4, controls (NIST Controls) that were not effectively implemented.
- We did not identify any past breaches of the OpDivs' servers and workstations.

What We Found:
Examples of Significant Vulnerabilities

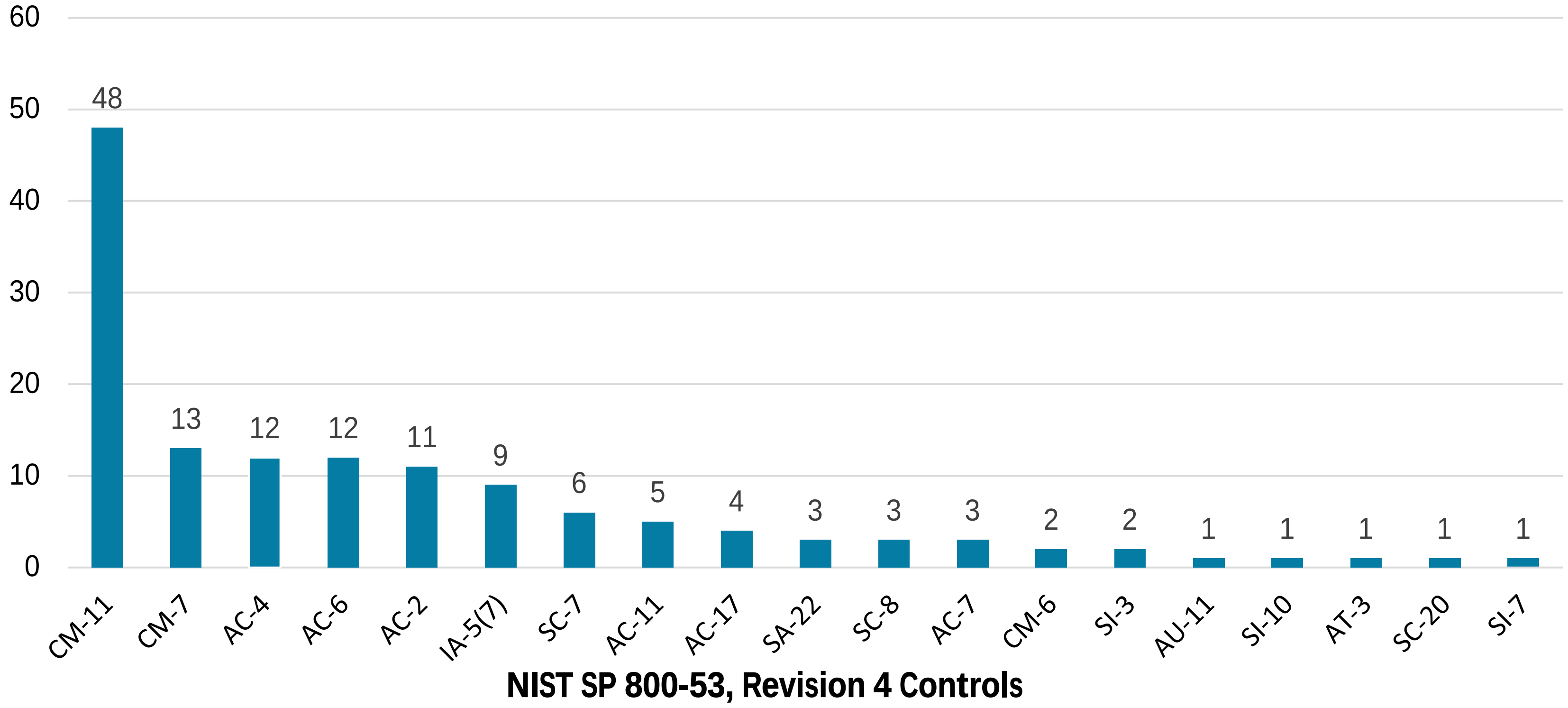
Significant Vulnerabilities	NIST SP 800-53 Controls, Revision 4
Data Loss Prevention controls did not block sensitive data transmission from leaking outside of the network.	AC-4 SC-7
Outbound web communications bypassed internet proxy controls.	AC-4
Unauthorized software and browser extensions were installed on various OpDivs' systems.	CM-11
Servers or workstations were sending traffic to suspicious domains via the Tor network, which is used to hide Internet activity.	CM-7
Servers or workstations were exhibiting indicators of compromise by malware that was not detected by security controls.	CM-11
Unapproved processes or applications were running from unauthorized portable drives.	CM-11

What We Found: NIST SP 800-53 Controls Not Effectively Implemented by OpDivs

User-Installed Software	CM-11
Least Functionality	CM-7
Information Flow Enforcement	AC-4
Least Privilege	AC-6
Account Management	AC-2
Authenticator Management	IA-5(7)
Boundary Protection	SC-7
Session Lock	AC-11
Remote Access	AC-17
Transmission Confidentiality and Integrity	SC-8

Unsuccessful Logon Attempts	AC-7
System and Services Acquisition	SA-22
Configuration Settings	CM-6
Malicious Code Protection	SI-3
Audit Record Retention	AU-11
Information Input Validation	SI-10
Role-Based Security Training	AT-3
Secure Name / Address Resolution Service (Authoritative Source)	SC-20
Software, firmware, and information integrity	SI-7

What We Found:
138 Vulnerabilities by NIST Control



What We Found: Breakdown by OpDiv

Controls Not Effectively Implemented by OpDiv*	FDA	OS	IHS	NIH	CMS	HRSA	SAMHSA	ACF
User-Installed Software (CM-11)	þ	þ	þ	þ	þ	þ		þ
Least Functionality (CM-7)	þ	þ			þ			þ
Information Flow Enforcement (AC-4)	þ	þ	þ	þ	þ	þ		
Least Privilege (AC-6)	þ			þ		þ	þ	þ
Account Management (AC-2)	þ		þ	þ		þ	þ	þ
Authenticator Management (IA-5(7))	þ	þ	þ	þ	þ	þ		þ
Boundary Protection (SC-7)				þ	þ			þ
Session Lock (AC-11)	þ	þ	þ	þ		þ		
Remote Access (AC-17)			þ	þ				
System and Services Acquisition (SA-22)			þ	þ				þ

*Check mark indicates one or more vulnerabilities identified for the control

What We Found: Breakdown by OpDiv-Cont.

Controls Not Effectively Implemented by OpDiv*	FDA	OS	IHS	NIH	CMS	HRSA	SAMHSA	ACF
Transmission Confidentiality and Integrity (SC-8)								þ
Unsuccessful Logon Attempts (AC-7)				þ	þ	þ		
Configuration Settings (CM-6)	þ							
Malicious Code Protection (SI-3)			þ			þ		
Audit Record Retention (AU-11)				þ				
Information Input Validation (SI-10)				þ				
Role-Based Security Training (AT-3)				þ				
Secure Name / Address Resolution Service (Authoritative Source) (SC-20)						þ		
Software, firmware, and information integrity (SI-7)			þ					

*Check mark indicates one or more vulnerabilities identified for the control

Common Root Causes

These vulnerabilities occurred because some OpDivs did not:

- adequately implement HHS's and their own security policies,
- harden systems to allow only essential functions and services,
- implement effective controls to prevent end users from downloading and installing unauthorized applications from the internet or running unauthorized applications from unauthorized portable drives, and
- implement effective processes and technologies such as those for detecting unauthorized software and unauthorized or suspicious network connections.

Potential Effects of Ineffective Controls

Because OpDivs did not adequately implement certain controls, cyber threat actors could have launched cyberattacks or insiders could have bypassed OpDivs' security measures to potentially commit fraud, steal sensitive data, and evade detection while performing such attacks. When effective security controls are not enforced or adequately implemented, the chances of cyberattacks that exploit sensitive information increase.

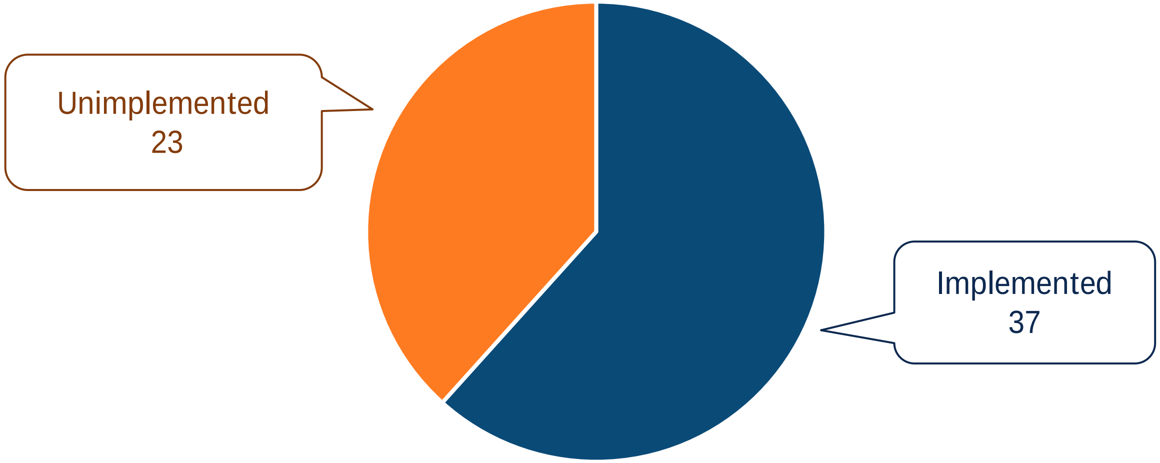
OpDiv Responses to OIG Recommendations

Overall, our recommendations to the OpDivs were aimed at improving cybersecurity controls and threat detection measures.

- OpDivs concurred with 59 of our 60 recommendations.
- One OpDiv did not concur with 1 recommendation to assess and implement authentication security controls in accordance with NIST SP 800-53, Revision 4, to ensure that privileged users use multifactor authentication for both local and network access; however, it provided corrective actions to resolve the vulnerability.

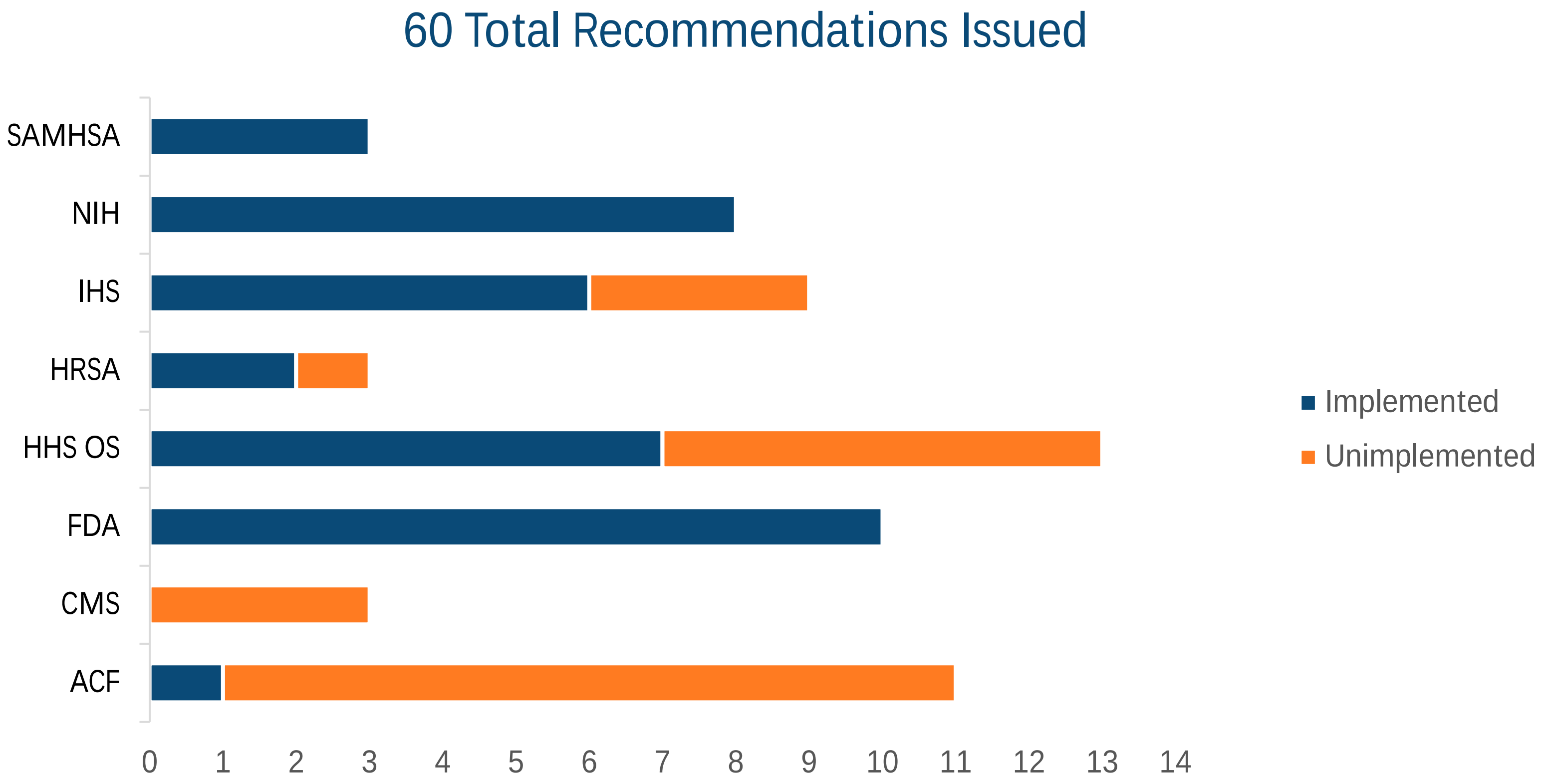
Implementation of Recommendations by Status (as of October 2024)

60 Total Recommendations Issued



Note: Newly issued recommendations begin as **Unimplemented**. Once the OpDiv concurs or partially concurs with the recommendation and provides evidence that the recommendation was implemented, the recommendation moves to **Implemented**.

Implementation of Recommendations by OpDivs (as of October 2024)



Recommendations to HHS's OCIO

We recommend that the Department of Health and Human Services Office of the Chief Information Officer:

1. Enforce existing information security continuous monitoring (ISCM) requirements for detecting, preventing, and reporting the installation of unauthorized software across OpDivs referenced in HHS Policy for Information Security and Privacy Protection (IS2P) and enforce the new ISCM policy once approved.
2. Enforce HHS's continuous monitoring policy for detecting, preventing, and reporting unauthorized or suspicious network activity across OpDivs.
3. Update the HHS IS2P to require OpDivs to implement NIST 800-53, Revision 5, CA-8 (2) Red Team Exercises at least every 2 years and RA-10 Threat Hunting yearly for high and moderate Federal Information Processing Standards Publication 199 impact systems.

HHS OCIO’s Comments and OIG Responses

- OCIO concurred with two of our three recommendations in our draft report. Although OCIO concurred with our first recommendation, it stated that it does not currently have an HHS Continuous Monitoring Policy. However, OCIO’s goal is to redo its outdated Information Security Continuous Monitoring (ISCM) Strategy and develop an HHS ISCM policy. The projected approval date of the strategy is late 2024 and policy is Quarter 2 FY 2026. Although we identified continuous monitoring requirements in the *HHS Policy for Information Security and Privacy Protection* that should be currently enforced, we are encouraged that HHS plans to update its ISCM strategy and develop a specific ISCM policy. We maintain the validity of our recommendation, but revised it based on the additional information provided by OCIO.
- OCIO also concurred with our third recommendation. Although NIST does not require CA-8(2) Red Team Exercises and RA-10 Threat Hunting for high and moderate Federal Information Processing Standards Publication 199 impact systems, OCIO agreed to update its HHS security control catalog to make both mandatory requirements for all moderate and high systems. We are encouraged by OCIO’s planned actions.

HHS OCIO's Comments and OIG Responses – Cont.

- OCIO did not concur with our second recommendation because it did not believe that our findings (19 active threats targeting some OpDivs' servers and workstations and 138 vulnerabilities out of 127,000 servers and workstations reviewed) supported the claim that HHS does not enforce a continuous monitoring policy for detecting, preventing, and reporting unauthorized or suspicious network activity across OpDivs. We believe that our findings demonstrate a systemic weakness in enforcing continuous monitoring within HHS and maintain our recommendation.

- HHS full comments can be found in the Appendix.

Appendix

Scope, Methodology, Criteria, and HHS OCIO’s Comments

Scope

- We conducted a series of CTH audits at 8 HHS OpDivs from 2018 through 2020.
- We conducted our audit assessments on more than 127,000 servers and workstations with varying operating systems across the eight OpDivs.
- We excluded certain segments of network environments due to OpDivs' concerns about patient safety, business operation impact, or software compatibility issues.
- The CTH audits we performed may not have disclosed all threats or deficiencies that may have existed at the time of our audit.

Methodology: Adherence to GAGAS

- We conducted the eight performance audits in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audits 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 during those audits provided a reasonable basis for our findings and conclusions based on our audit objectives.

Methodology

- We analyzed servers and workstations data for:
  - unusual outbound network communications,
  - connections to foreign Internet Protocol (IP) addresses,
  - abnormal user account activity,
  - malicious activity,
  - hashes of known malware files, and
  - suspicious files, programs, or configuration changes.
- We scanned for adversary behavior and techniques used in cyberattacks based on the MITRE ATT&CK framework.*
- We also searched for known Indicators of Compromise (IoC) using cyber threat intelligence data feeds.

***MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.**

Methodology:
Use of Subject Matter Experts

- We relied on subject matter experts from AFS and from our OIG team to perform the CTH audits.
- We monitored AFS's work to ensure the audits followed GAGAS and agreed-upon Rules of Engagement between OIG, AFS, and the OpDivs.

Applicable Criteria

- HHS Policy for Information Security and Privacy Protection, version 1.1
- HHS Rules of Behavior, Version 2.1, Use of HHS Information and IT Resources Policy
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-66, Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- NIST SP 800-83, Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- Department of Homeland Security's Binding Operational Directive 17-01, *Removal of Kaspersky-branded Products*

HHS OCIO’s Comments

OFFICE OF THE
CHIEF INFORMATION OFFICER
DEPARTMENT OF HEALTH AND HUMAN SERVICES

August 2024
OCIO General Comments to Draft Report for "Summary Report for Office of Inspector General Cyber Threat Hunt Audits of Eight HHS Operating Division Networks" (Engagement Number: A-18-22-07002)

> **Recommendation**: Update the HHS Policy for Information Security and Privacy Protection to require OpDivs to implement NIST 800-53, Revision 5, CA-8 Red Team Exercises at least every 2 years and RA-10 Threat Hunting yearly for high and moderate Federal Information Processing Standards Publication 199 impact systems.

HHS Response: Concur.

CA-8 is not Red Team Exercises. CA-8 is Penetration Testing. Red Team Exercises is CA-8(2). HHS will update the IS2P Control Catalog according to OIG Audit recommendation although both CA-8(2) Red Team Exercises and RA-10 Threat Hunting are NIST Not Selected controls per NIST SP 800-53B. Since those controls are not required, currently HHS left those controls as options in the IS2P Control Catalog for the OpDivs to select those controls if they need additional protection based on their risk environment, system criticality, and business need. Per OIG recommendation, HHS will change these two controls from NIST Not Selected controls to HHS required controls to be implemented by all OpDivs for all Moderate and High systems and be implemented at least every two years for CA-8(2) and yearly for RA-10 control. Also, HHS will change the CA-8 control baseline from only High to Moderate and High. Currently, the draft updated IS2P Control Catalog is under review and the expected completion date is by the end of December 2024.

> **Recommendation:** Enforce HHS's continuous monitoring policy for detecting, preventing, and reporting unauthorized or suspicious network activity across OpDivs.

HHS Response: Non-concur.

The statement does not support the claim that the department does not currently enforce this policy. The auditors only identified 19 threats and 138 vulnerabilities out of the over 127,000 endpoints that were reviewed.

> **Recommendation:** Enforce HHS's continuous monitoring policy for detecting, preventing, and reporting the installation of unauthorized software across OpDivs.

HHS Response: Concur.

There is currently <u>no</u> HHS Continuous Monitoring Policy. There is an outdated Information Security Continuous Monitoring Strategy (2017) that is completely being redone and should be *approved by late 2024. It is the goal of the Information Security Continuous Monitoring (ISCM) Program to spearhead the development of an ISCM Policy, once the outdated ISCM Strategy is approved and signed. The anticipated timeline for approval of the ISCM Strategy is December 2024 and the projected approval date of an HHS ISCM Policy is Q2 FY26.*

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

OIGatHHS

HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov