Department of Health and Human Services

Office of Inspector General

Office of Audit Services

November 2024 | A-18-24-11200

Review of the Department of Health and Human Services' Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024

The Department of Health and Human Service's FY 2024 Federal Information Security Modernization Act (FISMA) Report

November 14, 2024

Building a better working world

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

Tel: +1 703 747 1000
Fax: +1 703 747 0100
ey.com

Report of Independent Auditors on the Department of Health and Human Service's FY 2024 Federal Information Security Modernization Act (FISMA) Report Based on a Performance Audit Conducted in Accordance with *Government Auditing Standards*

To: Tamara Lilly
Assistant Inspector General for Audit Services

We have conducted a performance audit of the Department of Health and Human Services' (HHS) security program as of July 31, 2024, with the objective of assessing HHS's effectiveness and consistency with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA) as defined in the FY 2023 - 2024 Inspector General FISMA Reporting Metrics. HHS's management is responsible for defining the policies, procedures, and practices supporting the implementation of the HHS's Information Security Program in accordance with FISMA reporting metrics.

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. The nature, timing, and extent of the procedures selected depend on our judgment. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To audit HHS's effectiveness and consistency with the requirements of FISMA, we applied the Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2023 – 2024 FISMA Reporting Metrics. The specific scope and methodology are defined in Appendix A of this report.

This performance audit did not constitute an audit of the financial statements in accordance with auditing standard generally accepted in the United State of America or Government Auditing Standards.

The conclusions in Section II and our findings, recommendations, and proposed actions for the improvement of HHS' effectiveness and consistency with the requirements with FISMA in Section III, were noted as a result of our audit. Management's responses to our reported findings and recommendations are included in Appendix C of this report.

This report is intended solely for the information and use of HHS, the HHS Office of Inspector General (OIG), Department of Homeland Security (DHS), Office of Management and Budget (OMB), the appropriate committees of Congress, and the Comptroller General, and is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

November 14, 2024

REPORT HIGHLIGHTS

November 2024 | A-18-24-11200

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024

Why OIG Did This Audit

- The Federal Information Security Modernization Act of 2014 (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. OIG engaged Ernst & Young LLP (EY) to conduct this audit.
- EY conducted a performance audit of the HHS Chief Information Officer's (HHS's) compliance with FISMA as of July 31, 2024, based upon the 2024 FISMA reporting metrics.
- The audit examined whether HHS's overall information technology security program and practices were effective as they relate to Federal information security requirements.

What OIG Found

Overall, through the evaluation of FISMA metrics, it was determined that HHS's information security program rated "Not Effective" for FY 2024, which is the same as the "Not Effective" program rating from FY 2023.

The determination that HHS's information security program was "Not Effective" was made based on HHS's inability to meet the "Managed and Measurable" maturity level for the Core and Supplemental Inspector General metrics in the function areas of Identify, Protect, Detect, Respond, and Recover.

What OIG Recommends

We made a series of six recommendations to HHS to strengthen its information security program through improved oversight and information security controls implementation.

HHS concurred with five of our recommendations. HHS did not concur with the recommendation to complete implementation of a cybersecurity risk management strategy, because it believes its current strategy is sufficient.

Table of Contents

Abbreviations

ATO	Authorization to Operate
BIA	Business Impact Assessments
CISO	Chief Information Security Officer
CCP	Common Control Providers
CMDB	Configuration Management Database
CDM	Continuous Diagnostic and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSRM	Cybersecurity Risk Management Strategy
DHS	Department of Homeland Security
EY	Ernst & Young LLP
EO	Executive Order
CIO	Chief Information Officer
FCEB	Federal Civilian Executive Branch
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
HHS	Health and Human Services
IG	Inspector General
IC	Intelligence Community
NIST	National Institute of Standards and Technology
NFR	Notice of Findings and Recommendation
OIG	Office of Inspector General
OMB	Office of Management and Budget
PHI	Personal Health Information
PIV	Personal Identity Verification
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PIA	Privacy Impact Assessments
SCRM	Supply Chain Risk Management
SSP	System Security Plans

Section 1
Overview

Section 1: Overview

1.1 Objective

We have conducted a performance audit (also referred to as an audit herein) on the Department of Health and Human Services' (HHS) (the Agency) information security program and practices (the Program) to determine whether they were effective and consistent with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), as defined in the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*[1] (IG FISMA Reporting Metrics) as of July 31, 2024.

1.2 Background

The FISMA was amended on December 18, 2014 (Public Law 113-283). The purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provide a mechanism for improved oversight of Federal agency information security programs. The amendment: (1) included the reestablishment of the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control.[2]

FISMA requires Inspectors General to perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of the information security program and practices of the agency. HHS's Office of the Inspector General (OIG) engaged us, Ernst & Young LLP, to assess the effectiveness of HHS's information security controls, including its policies, procedures, and practices on a representative subset of the Agency's information systems by leveraging work performed as part of the financial statement audit and performing necessary additional testing procedures, as applicable.

FISMA Domains, Metrics and Ratings

The IG FISMA Reporting Metrics were developed in a collaborative effort between (and the consensus opinion of) representatives from OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch (FCEB) Chief Information Security Officers (CISOs) and their staff, and the Intelligence Community (IC). The IG FISMA Reporting Metrics continued using the maturity model approach for all security domains and

[1]Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics ((https://www.cisa.gov/resources-tools/resources/fy23-24-ig-fisma-metrics))
[2] *Federal Information Security Management Act of 2014,* Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014)

are fully aligned with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[3] (Cybersecurity Framework) function areas.

The IG FISMA Reporting Metrics are grouped into nine domains and aligned to the five Cybersecurity Framework function areas:

Table 1: Alignment of the Cybersecurity Framework with the IG FISMA Domains

Cybersecurity Framework Function Areas	IG FISMA Domains
Identify	Risk Management
	Supply Chain Risk Management
Protect	Configuration Management
	Identity and Access Management
	Data Protection and Privacy
	Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Reporting Metrics

For the IG FISMA Metrics, the OMB, CIGIE, FCEB CISOs, and the IC defined the metrics into (20) Core and (37) Supplemental IG Metrics (Performance Metrics). The 37 supplemental IG Metrics were further split into two subcategories. For FY24, it includes the FY23 Supplemental Metrics, which consist of 20 previously scored metrics and FY24 Supplemental Metrics, which consist of 17 newly evaluated metrics. Determinations for each function were made based on the average score of the FY24 Core metrics, FY24 Supplemental metrics, and FY23 Supplemental metrics. Additional considerations were made on a case-by-case basis based on the issues identified during testing. Core and supplemental metrics were defined as follows:

- Core Metrics – Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.

[3] NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 (https://www.nist.gov/cyberframework)

- Supplemental Metrics – Metrics that are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

Maturity Level Scoring

OMB and DHS continued with a calculated scoring model for FY24. The maturity level scoring methodology was prepared by OMB and DHS and is divided into calculated scores for core and supplemental metrics. Level 1 (Ad-hoc) is the lowest maturity level and Level 5 (Optimized) is the highest maturity level. The details of the five maturity model levels are:

1. Level 1 (Ad-hoc): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.

2. Level 2 (Defined): Policies, procedures, and strategies are formalized and documented but not consistently implemented.

3. Level 3 (Consistently Implemented): Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

4. Level 4 (Managed and Measurable): Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.

5. Level 5 (Optimized): Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Within the context of the model, Level 4 (Managed and Measurable) represents an "effective" level of security as defined by the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*[4].

In FY24, based on OMB and DHS guidance, we performed procedures to assess HHS's information security program effectiveness required by FISMA. We tested HHS's information security controls at the Department, five operating divisions (OpDivs), and twenty-five systems (five at each OpDiv), that were representative of the broader IT environment implemented at HHS. Three of five operating divisions (OpDivs) evaluated in FY 2023 upon which the FY23 Supplemental Metrics scores were calculated and reported were replaced by three other OpDivs in FY24 as part of the audit methodology. The FY24 Supplemental Metrics scores were calculated using the FY24 OpDivs selected.

[4]Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (https://www.cisa.gov/resources-tools/resources/fy23-24-ig-fisma-metrics)

Based on the results of these tests, we determined whether HHS met the associated Metric maturity requirements. We then reviewed the results of the Core and Supplemental metrics to determine whether the Agency was at an overall effective level (Managed and Measurable) for the domain and corresponding function. We developed an Objective Attribute Recap Sheet (OARS) for each finding identified during testing and provided the OARS to HHS. Refer to Appendix A for further details on our scope and methodology.

Section 2
Conclusions and Enterprise-wide Recommendations

Section 2: Conclusion and Enterprise-wide Recommendations

2.1 Conclusion

We determined that HHS's cybersecurity program was "Not Effective." This determination was made based on HHS not meeting the 'Managed and Measurable' maturity level for all five function areas: Identify, Protect, Detect, Respond, and Recover. Individual domain and function effective or ineffective determinations were made by reviewing Core metric scores and the relevant risks identified by the evaluation of the supplemental metric areas or other risk factors identified during our audit period.

Table 2 below provides the FY 2024 IG FISMA Maturity results and calculated score.

Table 2: 2024 HHS Maturity Levels

Cybersecurity Framework Function	IG FISMA Domain	Assessment Results for FY24 Core Metrics	Assessment Results for FY23 Supplemental Metrics[5]	Assessment Results for FY24 Supplemental Metrics	FY 2024 IG Assessment by Function
Identify	*Risk Management*	Consistently Implemented	Consistently Implemented	Managed and Measurable	Not Effective
	Supply Chain Risk Management	Defined	Defined	Ad hoc	
Protect	*Configuration Management*	Consistently Implemented	Consistently Implemented	Consistently Implemented	Not Effective
	Identity & Access Management	Consistently Implemented	Consistently Implemented	Defined	
	Data Protection & Privacy	Consistently Implemented	Consistently Implemented	Consistently Implemented	
	Security Training	Consistently Implemented	Consistently Implemented	Consistently Implemented	
Detect	*Information Security Continuous Monitoring*	Consistently Implemented	Managed and Measurable	Consistently Implemented	Not Effective
Respond	*Incident Response*	Consistently Implemented	Consistently Implemented	Consistently Implemented	Not Effective
Recover	*Contingency Planning*	Consistently Implemented	Consistently Implemented	Defined	Not Effective

[5] The scores in the column are repeated from our prior report "The Department of Health and Human Service's FY 2023 Federal Information Security Modernization Act (FISMA) Report." Per the FISMA Reporting Guidance, we did not perform additional procedures on the FY 2023 supplemental metrics.

Cybersecurity Framework Function	IG FISMA Domain	Assessment Results for FY24 Core Metrics	Assessment Results for FY23 Supplemental Metrics[5]	Assessment Results for FY24 Supplemental Metrics	FY 2024 IG Assessment by Function
Overall Maturity		Consistently Implemented	Consistently Implemented	Consistently Implemented	Not Effective

The detailed list of findings for these domains was provided to HHS management outside of this report.

IDENTIFY

The goal of the Identify function is to develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. This area is the foundation that allows an agency to focus and prioritize its efforts with its risk management strategy and business needs. Within this function, there are two domains, Risk Management and Supply Chain Risk Management. Risk Management is at a 'Consistently Implemented' maturity level and Supply Chain Risk Management is at a 'Defined' maturity level, therefore our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function	IG FISMA Domain	FY 2024 IG Assessment
Identify	Risk Management	Consistently Implemented
	Supply Chain Risk Management	Defined

Risk Management findings

The Risk Management Framework, developed by NIST,[6] provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. A risk management framework is the foundation on which an IT security program is developed and implemented by an entity. A risk management framework should include: an assessment of management's long-term plan for implementing risk management strategies, documented goals and objectives of the entity, clearly defined roles and responsibilities for security management personnel, and prioritization of IT needs.

The following findings were identified within the agency's risk management program:

- As part of the risk management domain, inventories of systems and applications, hardware, and software should be accurately maintained:

[6] NIST SP 800-137, ISCM for Federal Information Systems and Organizations (https://csrc.nist.gov/pubs/sp/800/137/final)

- Although HHS had defined a process to develop and maintain a comprehensive and accurate inventory of information systems and system interconnections, HHS did not consistently implement its processes to maintain a comprehensive and accurate inventory of its information systems. Specifically, the system inventories from three of five OpDivs did not reconcile to the system report collected by the Department. Further, we noted the Department did not verify the system inventory data reported by OpDivs were accurate and did not obtain assurance that system inventories are complete and accurate. Therefore, we could not conclude that the consolidated system reports or the OpDiv system repositories were complete and accurate.

- Although HHS had defined policy and procedures to maintain a hardware asset inventory, the policy and procedures were not fully implemented by two of five OpDivs. Specifically, hardware assets for one OpDiv did not include all hardware in accordance with HHS policy. In addition, one OpDiv did not implement the hardware taxonomy within its inventory that includes the specifications of each asset in accordance with HHS policy.

- As part of the risk management domain, system security risks should be adequately managed at the organizational, mission/business process, and information system levels, and considered throughout the system lifecycle:

  - Although HHS developed and published a cyber risk management strategy to assess risk at the organizational, mission/business process, and information system levels to support enterprise level risk-based decisions, one of five OpDivs did not perform an organizational level cybersecurity and privacy risk assessment.

  - Although HHS has defined the system development lifecycle process for the agency's systems, three of five OpDivs did not consistently perform a system impact analysis for a selection of changes.

  - Although HHS has developed a CSRM strategy and implementation plan, the strategy has not been implemented for one of five OpDivs to assess risks across the agency and facilitate enterprise level risk-based decisions, to include an aggregated enterprise risk register used to communicate risks with internal and external stakeholders.

Supply Chain Risk Management findings

Supply Chain Risk Management (SCRM) involves activities that pertain to managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risk presented by the supplier, the supplied products and services or the supply chain.

The following findings were identified within the agency's SCRM program:

- As part of the supply chain risk management domain, hardware received through the supply chain should be monitored for counterfeit components:
  - HHS has not fully defined procedures to detect and prevent counterfeit components from entering the system, to maintain configuration control over organizationally defined system components awaiting repair or being serviced, and requirements for reporting counterfeit system components.

PROTECT

The goal of the Protect function is to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event and incorporates the domains of Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. The Protect function is at 'Consistently Implemented' therefore, our overall assessment of this function of "Not Effective."

Cybersecurity Framework Function	IG FISMA Domain	FY 2024 IG Assessment
Protect	Configuration Management	Consistently Implemented
	Identity and Access Management	Defined[7]
	Data Protection and Privacy	Consistently Implemented
	Security Training	Consistently Implemented

Configuration Management findings

Configuration management involves activities that pertain to the operations, administration, maintenance and configuration of networked systems and their security posture. Areas of configuration management include standard baseline configurations, anti-virus management, and patch management.

The following findings were identified within the agency's configuration management program:

[7] Based on the average of the FY24 Core, FY24 Supplemental metrics, and FY23 Supplemental metrics, HHS received an average score of Consistently Implemented. However, based on testing, all OpDivs tested did not meet event logging requirements laid out in OMB M-21-31 which would allow the agency to log and review activities performed by privileged users. In addition, two of five OpDivs did not track background investigations and position risk designations for their employees. Due to the findings identified and their impact to the Identity and Access Management Domain, we rated this Domain at Defined.

- As part of change management domain, configuration settings should be utilized for systems and monitored for deviations from the baseline:

    - Although HHS established a policy and procedure to document and review secure configuration baselines, one of five OpDivs is still in the process of developing an enterprise-wide reporting process to monitor for misconfigurations.

    - Although HHS established a policy and procedure to utilize configuration settings for systems, one of five OpDivs did not consistently use standard configuration settings.

- As part of change management domain, vulnerabilities identified on systems and assets should be remediated within the timeframe specified by policy and procedure:

    - Although HHS has defined flaw remediation processes, including patch management, to manage software vulnerabilities, one of five OpDivs did not consistently utilize corrective actions for two of nine selected vulnerabilities that were not resolved within the timeline established by policy and procedure.

- As part of change management domain, configuration changes made to systems follow a documented approval, testing, and implementation process:

    - Although HHS has defined a configuration management process, two of five OpDivs did not consistently provide evidence that systems properly developed, tested, and approved selected changes. In addition, one of five OpDivs did not provide evidence of monitoring the effectiveness of the change management process.

Identity and Access Management findings

Federal agencies are required to establish policies and procedures to limit access to physical and logical assets and associated facilities to authorized users, processes, and devices. An appropriate monitoring process should also be implemented to validate that information system access is limited to authorized transactions and functions for each user based on the concept of least privilege.

The following findings were identified within HHS's IAM program:

- As part of identity and access management domain, personnel should undergo background screening and rescreening prior to accessing systems data:

    - Although HHS has defined a process for screening and assigning position risk designations for employee and contractor personnel, four of five OpDivs did not provide evidence that screening was performed, or a position risk designation was assigned to employees and contractors.

- As part of identity and access management domain, privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties:

    - Although HHS defined its processes for provisioning, managing, and reviewing privileged accounts, this process was not consistently implemented. Specifically, one of five OpDivs did not consistently perform access reviews of privileged users for access appropriateness.

Data Protection and Privacy findings

Federal agencies have unique access to personally identifiable information (PII) and personal health information (PHI) of U.S. citizens. Many of HHS's systems contain PII and PHI. The underlying principle of data privacy and protection controls is to protect the confidentiality of information stored on information systems. To protect this information, Federal regulations such as M-22-09[8] and BOD-18-02[9] require agencies to report when these types of information are stored, how they are protected, and when breaches occur that expose such information.

The following findings were identified within the agency's data protection and privacy program:

- As part of the data protection and privacy domain, data transiting outside the network should be monitored and data privacy training should be provided to users with significant privacy roles:

    - HHS has defined a privacy program for the monitoring of data exfiltration; however, one of five OpDivs did not provide evidence of the implementation of a web content filter and email authentication security, which blocks restricted and malicious web content, and validates and manages e-mail traffic respectively.

    - Although HHS has implemented privacy awareness training for employees, one of five OpDivs did not measure the effectiveness of the training, such as the use of targeted phishing.

Security Training findings

An IT security program may not be effective without an established and maintained training program for its information system users. Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment and secured physical locations without providing their personnel role-based and security awareness training.

[8] OMB M-22-09 Federal Zero Trust Strategy (whitehouse.gov)
[9] BOD 18-02: Securing High Value Assets | CISA

- Although HHS has performed a workforce assessment to analyze the current skillset of the workforce, one of five OpDivs did not provide evidence of relevant training and/or hiring to address the skills gaps identified.

- Although HHS has implemented role-based awareness training for employees, one of five OpDivs did not measure the effectiveness of the training, such as the use of targeted phishing or monitoring of dashboards. In addition, one of five OpDivs did not ensure that all selected employees and contractors were assigned and completed the security awareness and role-based trainings.

DETECT

The goal of the Detect function is to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events. The domain within this function is Information Security Continuous Monitoring (ISCM), which was assessed at 'Consistently Implemented', therefore our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function	IG FISMA Domain	FY 2024 IG Assessment
Detect	ISCM	Consistently Implemented

Information System Continuous Monitoring findings

An ISCM program allows an organization to maintain the security authorization of an information system over time in a dynamic environment of operations with changing threats, vulnerabilities, technologies, and business processes. Per the Cybersecurity & Infrastructure Security Agency, implementation of a continuous diagnostic and mitigation (CDM) program results in an approach to fortifying the cybersecurity posture through ongoing updates to system security plans, a periodic security assessment and POA&Ms, which are the three principal documents in a security authorization package.

The following findings were identified within the agency's ISCM program:

- As part of the information system continuous monitoring domain, policies and procedures should be developed to continuously assess and maintain the security posture of the system:

    - Although HHS has defined and implemented an ISCM policy and strategy across the organization, performance measures have not been established to monitor the effectiveness of the policy.

- Although HHS has defined policies and procedures to be implemented organization-wide, several policies had not been updated or reviewed per the agency's three-year frequency.

RESPOND

The goal of the Respond function is to develop and implement the appropriate activities to act regarding a detected cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity event and is defined by the incident response program. The domain within this function is incident response, which was assessed at 'Consistently Implemented', therefore our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2024 IG Assessment
Respond	Incident Response	Consistently Implemented

Incident Response findings

Incident Response involves capturing general threats and incidents that occur in the HHS systems and physical environment. Incidents are captured by systematically scanning IT network assets for any potential threats, or they are reported by affected persons to the appropriate personnel.

The following findings were identified regarding the agency's incident response program:

- As part of the incident response domain, incidents should be detected, analyzed, and handled timely.
  - Although HHS has established an incident response process to detect and analyze incidents, two of five OpDivs did not manage and measure the effectiveness of the incident response process to identify areas of improvement.
  - Although HHS has implemented an incident detection and analysis process that uses lessons learned, threat vectors, precursors, and indicators, three of five OpDivs have not completely implemented Event Logging requirements per M-21-31 (Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents).

RECOVER

The goal of the Recover function is to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event or natural disaster. The Recover function supports timely recovery to

normal operations to reduce the impact from a cybersecurity event. The domain that was assessed within this function is Contingency Planning. Due to Contingency Planning being assessed at a maturity level of 'Consistently Implemented', our overall assessment of this function was "Not Effective".

Cybersecurity Framework Function	IG FISMA Domain	FY 2024 IG Assessment
Recover	Contingency planning	Consistently Implemented

Contingency Planning findings

Contingency planning refers to a coordinated strategy involving plans, procedures and technical measures that enable the recovery of business operations, information systems and data after a disruption.

Information system contingency planning is unique to each system. Each contingency plan should provide preventive measures, recovery strategies and technical considerations that are in accordance with the data and the system's confidentiality, integrity and availability requirements and the system impact level.

The following information security control deficiencies were identified within the agency's contingency planning program:

- As part of the contingency planning domain, business impact analyses are utilized to prioritize recovery and contingency plans are developed and tested periodically:
    - HHS consistently used a Business Impact Analysis (BIA) to guide contingency planning efforts; however, the required policies and procedures on performing BIAs to promote compliance and consistency were not defined.
    - Although HHS has defined information system contingency plans, one of five OpDivs did not consistently update or review the contingency plan for one of five systems.
    - HHS has implemented a program to perform test/exercises of its contingency planning process, however one of five OpDivs did not provide evidence that automation was used to test information system contingency plans as required.

2.2 Recommendations

To strengthen HHS's enterprise-wide cybersecurity program, based on our reviews of the five selected OpDivs in scope, we recommend that HHS focus on five areas related to the Identify, Protect, and Respond functions for an effective program. We recommend that HHS:

1. Update its enterprise architecture system inventory and software/hardware asset inventories to include the information systems and components that are active on the HHS network. HHS should utilize the inventories to continuously monitor assets and identify and remediate vulnerabilities timely to better manage the risks to these assets.

2. Complete implementation of a cybersecurity risk management strategy to assess and respond to identified risks within the agency and identified across OpDivs, watch for new risks, and monitor risks and confirm implementation. The strategy should define a standardized process to accept and monitor risks that cannot be adequately mitigated.

3. Require OpDivs incorporate analyses of security impacts of significant changes prior to implementation to measure its impacts to the organizations' security and enterprise architecture and confirm implementation.

4. Require OpDivs to implement an effective SCRM program that meets the defined standards across HHS and confirm implementation is consistent with established standard. This should include requiring OpDivs to assess vendors and submit said monitoring results to HHS to assist with tracking and monitoring components on the network.

5. Require OpDivs to establish oversight of background investigations performed for employees and contractors with logical access across the agency and perform continuous monitoring for new and existing users to ensure OpDivs are aware of the investigation status of their users.

6. Confirm that OpDivs' policies require monitoring of privileged user accounts for both logging and activity reviews, in an automated manner.

HHS OCIO COMMENTS AND OFFICE OF THE INSPECTOR GENERAL RESPONSE

HHS concurred with five of our six recommendations and did not concur with our second recommendation.

HHS stated that it did not concur with our second recommendation because OpDiv Chief Information Officers (CIOs) are responsible for implementing their own cybersecurity risk management strategies. We made the recommendation to HHS because it is responsible for the information security and privacy program of the agency which includes the OpDivs. To fulfill its oversight responsibility, HHS should monitor and confirm that the OpDivs have implemented a cybersecurity risk management strategy. Therefore, we maintain the validity of our recommendation.

HHS's full comments are provided in Appendix C.

Section 3
Appendices

Section 3: Appendices

3.1 Appendix A: Scope and Methodology

Scope

The Federal Information Security Modernization Act of 2014 (FISMA) directs each agency's Inspector General (IG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security programs and practices as well as a review of an appropriate subset of agency systems. The objective of Ernst & Young LLP's performance audit was to determine whether HHS's overall information security program and practices were effective and consistent with FISMA requirements, as defined in the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*[10] (IG FISMA Reporting Metrics) as of July 31, 2024.

The FY24 IG FISMA reporting metrics were assessed at HHS and results were based on the aggregation of their results from the operating divisions (OpDivs) selected for testing. In FY24, we tested HHS's information security controls across five (5) operating divisions: Centers for Medicare and Medicaid Services (CMS), Office of the Secretary (OS), Administration for Children and Families (ACF), Centers for Disease Control and Prevention (CDC), and Health Resources and Services Administration (HRSA). Three of five operating divisions (OpDivs) evaluated in FY 2023 upon which the FY23 Supplemental Metrics scores were calculated and reported were replaced by three other OpDivs in FY24 as part of the audit methodology. The FY24 Supplemental Metrics scores were calculated using the FY24 OpDivs selected. We also mapped the current year OARs to prior year findings.

Methodology

We mapped HHS's key information security controls to the metrics in the FY24 FISMA domains. For each metric question, we tested the design of the control through inquiry with management and inspection of management policies and procedures. For controls we determined HHS defined adequately, we performed tests to determine whether they were effectively and consistently implemented. Depending on the control, we performed procedures for our 15 in scope systems, random sampling, or inspection of system settings. For specific controls identified for testing we considered suggested controls outlined in the cybersecurity and privacy framework profile of the NIST Special Publication 800-53, Revision 5,[11] *Security and Privacy Controls for Information Systems and Organizations* along with the security and privacy control baselines identified in NIST for the Federal Government and tailored this guidance to assist in the control selection process.

[10]Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (https://www.cisa.gov/resources-tools/resources/fy23-24-ig-fisma-metrics)
11 NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations (https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)

To accomplish our objectives, we performed the procedures outlined in our Statement of Work[12] (SOW)'s Planned Scope and Methodology section. This included using federal guidance as we:

- Reviewed applicable Federal laws, regulations, and guidance.
- Gained an understanding of the current security program at HHS.
- Inquired of HHS OCIO personnel their self-assessment for each FISMA reporting metric.
- Assessed the status of HHS' security program against HHS cybersecurity program policies, other standards and guidance issued by HHS management, and reporting metrics.
- Inspected and analyzed selected artifacts including but not limited to system security plans, evidence to support testing of security controls, POA&M records, security training records, asset compliance reports, system inventory reports and account management documentation.
- Inspected internal and third-party assessments performed on behalf of HHS management that had a similar scope to the FY24 IG FISMA metrics. Incorporated the results as part of the FY 2024 IG FISMA metrics.
- Inspected artifacts provided by HHS related to prior year ineffective areas to determine the extent to which testing of corrective actions was applicable to our current audit objectives.

[12] Contract Number: GS-00F-290CA, Task Order Number 47QFDA24F0002

3.2 Appendix B: Federal Requirements and Guidance

The principal criteria used for this performance audit included:

- DHS Binding Operational Directive 18-02, Securing High Value Assets, (May 07, 2018)
- DHS Binding Operational Directive 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems, (April 29, 2019)
- DHS Binding Operational Directive 22-01, Reducing Significant Risk of Known Exploited Vulnerabilities, (November 03, 2021)
- Executive Order on Improving the Nation's Cybersecurity (EO 14028) (May 12, 2021)
- IG FISMA Metrics Evaluation Guide (2023 Publication)
- Federal Information Security Modernization Act of 2014 (December 2014)
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (February 2004).
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006).
- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems (May 2010).
- NIST SP 800-37, revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (December 2018).
- NIST SP 800-53, revision 5, Security and Privacy Controls for Federal Information Systems and Organizations (September 2020).
- NIST SP 800-61, Computer Security Incident Handling Guide (August 2012).
- NIST IR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM) (October 2020)
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (September 2011).
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).
- OMB M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program (December 10, 2018)

- OMB M-19-07, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019)
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
- OMB M-21-30, Protecting Critical Software Through Enhanced Security Measures (August 10, 2021)
- OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (August 27, 2021)
- OMB M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (October 08, 2021)
- OMB M-22-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements (December 2, 2021)
- OMB M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (December 6, 2021)
- OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022)
- OMB M-24-04 Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements (December 4, 2023)

3.3 Appendix C: HHS Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

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

DATE: October 23, 2024

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

FROM: Jennifer Wendel, Acting Chief Information Officer JW

SUBJECT: *Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024 (A-18-24-11200)*

The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) deeply appreciates the Office of the Inspector General (OIG) for their comprehensive review of the HHS security program for fiscal year (FY) 2024. We value the insights provided in the report developed by Ernest & Young on your behalf and welcome the opportunity to respond.

As requested, our office has reviewed the report and attached written comments. We are committed to our collaboration efforts and look forward to working with you to enhance information technology 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 contact the HHS Chief Information Security Officer, La Monte Yarborough, at Lamonte.Yarborough@hhs.gov or 202-774-2446.

Attachment A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024 (A-18-24-11200)***

cc:
La Monte Yarborough, Acting Deputy Chief Information Officer (Acting)
Christopher Bollerer, Deputy Chief Information Security Officer
Charles Summers, Assistant Director, OIG Cybersecurity and IT Audit Division
Jarvis Rodgers, Director, OIG Cybersecurity & IT Audit Division

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*** **(A-18-24-11200)**

Enterprise-wide Recommendations

To strengthen HHS' enterprise-wide cybersecurity program, based on our reviews across the Department, we recommend that HHS:

1. Update its enterprise architecture system inventory and software/hardware asset inventories to include the information systems and components that are active on the HHS network. HHS should utilize the inventories to continuously monitor assets and identify and remediate vulnerabilities timely to better manage the risks to these assets.

   HHS Response: Concur

   The HHS Information System Inventory is the system of record (SoR) for all systems on the HHS network. Operating Divisions (OpDivs) play a crucial role in providing system updates to the Department to maintain accurate reporting and tracking. The Department will continue to foster this collaborative relationship with the OpDivs through monthly reviews to ensure the information remains accurate and up-to-date.

   Despite some challenges faced by OpDivs, particularly during server migrations and hardware asset data collection, HHS is making significant progress in managing its enterprise-level software and hardware assets through the CDM dashboard. With most OpDivs exceeding the 80% compliance requirement, HHS is steadfast in its commitment to achieving full compliance by April 2025.

2. Complete implementation of a cybersecurity risk management strategy to assess and respond to identified risks within the agency and identified across OpDivs, watch for new risks, and monitor risks and confirm implementation. The strategy should define a standardized process to accept and monitor risks that cannot be adequately mitigated.

   HHS Response: Non-Concur

   HHS has already established a comprehensive Cybersecurity Risk Management Strategy (CRMS), developed in collaboration with the OpDivs, which they can leverage to meet their specific needs and effectively respond to identified risks. Sections 1.10 through 1.16 of the CRMS specifically support the definition of a standard process to accept and monitor risks that cannot be adequately mitigated.

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*** **(A-18-24-11200)**

Due to HHS's federated environment, Delegation of Authority to HHS OpDiv CIOs, and the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control RA-3 risk assessment, OpDivs are responsible for implementing a cybersecurity risk management strategy to assess and respond to identified risks within the agency, watch for new risks, monitor risks, and confirm implementation.

As such, HHS believes no further action is required for this recommendation, as our existing CRMS framework sufficiently addresses the audit recommendation.

3. Require OpDivs incorporate analyses of security impacts of significant changes prior to implementation to measure its impacts to the organizations' security and enterprise architecture and confirm implementation.

HHS Response: Concur

HHS has received a copy of the OpDiv OARS and will work with the OpDivs in scope who are associated with this recommendation to confirm its remediation.

Due to HHS' federated environment, Delegation of Authority to HHS OpDiv CIOs, and according to the HHS IS2P, and Control Catalog, specifically control, CM-4 Impact Analyses and its enhancements, OpDivs are responsible for monitoring, analyzing, and reporting qualitative and quantitative performance measures on the effectiveness of their change control activities to ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

4. Require OpDivs to implement an effective SCRM program that meets the defined standards across HHS and confirm implementation is consistent with established standard. This should include requiring OpDivs to assess vendors and submit said monitoring results to HHS to assist with tracking and monitoring components on the network.

HHS Response: Concur

HHS has established a C-SCRM office and revised the current operational C-SCRM Policy. The Policy also incorporates the National Institute of Standards and Technology (NIST) 800-53 Revision 5 SCRM security controls into its Cybersecurity

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*** **(A-18-24-11200)**

Standard. It defines the minimum-security control baseline and assessment objectives necessary to detect counterfeit and compromised ICT products.

Although the agency's SCRM program is in its early stages of maturity, a plan is being developed to ensure that the OpDivs have implemented the program according to the agency's standards.

5. Require OpDivs to establish oversight of background investigations performed for employees and contractors with logical access across the agency and perform continuous monitoring for new and existing users to ensure OpDivs are aware of the investigation status of their users.

   HHS Response: Concur

   HHS has received a copy of the OpDiv OARS and will work with the OpDivs in scope who are associated with this recommendation to confirm its remediation.

   HSPD-12 and FIPS 201 mandate that a non-sensitive, low-risk background investigation must be favorably initiated before issuing compliant credentials, enabling access to resources like email and network drives. If different investigations are required for access or elevated privilege accounts (e.g., Alternate Login Token (ALT) cards), the OpDiv and system owner must validate compliance. Access provisioning occurs separately across OpDiv CIO offices, and while there's no automation in the smartcard management system for logical access, proper alignment with HSPD-12 adjudication is necessary to ensure security protocols are followed.

6. Confirm that OpDivs' policies require monitoring of privileged user accounts for both logging and activity reviews, in an automated manner.

   HHS Response: Concur

   HHS has received a copy of the OpDiv OARS and will work with the OpDivs in scope who are associated with this recommendation to confirm its remediation.

   Due to HHS' federated environment, Delegation of Authority to HHS OpDiv CIOs, and according to the HHS IS2P and Control Catalog, specifically Control AC-6(7) Review of User Privileges, the OpDivs are responsible for ensuring that privileged users and privileged user activities are periodically logged and reviewed regularly as defined by the OpDivs.

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*** **(A-18-24-11200)**

Additionally, NIST 800-53 Rev. 5 control AC-6(7), Review of User Privileges, does not require monitoring of privileged user accounts for both logging and activity reviews to be automated. As such, HHS believes no further action is explicitly needed to automate privileged user account logging and activity reviews.

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