Department of Health and Human Services

Office of Inspector General

Office of Audit Services

March 2026 | OAS-25-18-041

Review of the Department of Health and Human Services' Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025

The Department of Health and Human Services' FY 2025 Federal Information Security Modernization Act (FISMA) Report

March 2, 2026

Ernst & Young LLP Tel: +1 703 747 1000
1775 Tysons Blvd Fax: +1 703 747 0100
Tysons, VA 22102 ey.com

Shape the future with confidence

Report of Independent Auditors on the Department of Health and Human Services' FY 2025 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, 2025, 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 2025 Inspector General FISMA Reporting Metrics. HHS's management is responsible for defining the policies, procedures, and practices supporting the implementation of 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 the findings and conclusions based on the 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 the findings and conclusions based on the 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 2025 IG FISMA Reporting Metrics. The specific scope and methodology are defined in Appendix A of this report.

A workforce optimization initiative[1] starting on March 27, 2025, impacted HHS's ability to demonstrate that key cybersecurity functions for selected in-scope application systems had been performed. Specifically, the evaluation of the Govern, Identify, and Detect cybersecurity functions were impacted. Refer to Section 3 for additional comments regarding this effort.

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

Findings, Conclusions, and Recommendations

The conclusions in Section 2 and the findings and recommendations for the improvement of HHS's effectiveness and consistency with the requirements of FISMA in Section 3, were noted as a result of

[1] HHS Workforce Optimization Initiative | HHS.gov, https://www.hhs.gov/about/agencies/asa/workforce-optimization-initiative/index.html

Shape the future
with confidence

the 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

March 2, 2026

REPORT HIGHLIGHTS

March 2026 | OAS-25-18-041

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025

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 HHS's compliance with FISMA as of July 31, 2025, based upon the 2025 FISMA reporting metrics.
- The audit examined whether HHS's overall information security program and practices were effective as they relate to Federal information security requirements and included systems from five HHS divisions.

What OIG Found

For FY 2025, EY rated HHS's information security program "Not Effective" for the sixth consecutive year. To be considered "Effective," an agency must achieve at least a "Managed and Measurable" maturity level.

In FY 2025, HHS did not achieve a "Managed and Measurable" rating for either the Core or Supplemental Inspector General metrics in any of the six cybersecurity function areas: Govern, Identify, Protect, Detect, Respond, and Recover. Specifically, the overall maturity level for Core metrics was assessed as "Consistently Implemented," while the Supplemental metrics were rated "Ad Hoc." Together, these ratings fall below the "Managed and Measurable" level, resulting in an overall determination of "Not Effective."

What OIG Recommends

Based on the audit, EY made ten recommendations to HHS to strengthen its information security program through improved oversight of the Operating and Staff Divisions' (Divisions) implementation of Federal information security requirements for an effective FISMA program.

HHS concurred with seven recommendations and detailed steps it has taken and plans to take in response to the recommendations. HHS did not concur with three recommendations.

Table of contents

Abbreviations

ATO	Authorization to Operate
BIA	Business Impact Analysis
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
CP	Contingency Planning
CRMS	Cybersecurity Risk Management Strategy
CSF	Cybersecurity Framework
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
IDAM	Identity and Access Management
NIST	National Institute of Standards and Technology
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
RAM	Risk and Asset Management
SCRM	Supply Chain Risk Management
SSP	System Security Plans
ZTA	Zero-Trust Architecture

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) (also referred to as 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 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*[2] (IG FISMA Reporting Metrics) as of July 31, 2025.

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.[3]

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 to be based on the maturity model approach for all security domains and are fully aligned

[2]Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (https://www.cisa.gov/resources-tools/resources/fy-2025-ig-fisma-metrics)

[3] *Federal Information Security Modernization Act of 2014,* Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014)

with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0[4] function areas.

The IG FISMA Reporting Metrics are grouped into 10 domains and aligned to the six Cybersecurity Framework function areas:

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

Cybersecurity Framework Function Areas	FISMA Domains
Govern	Cybersecurity Governance
	Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset 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 twenty (20) Core and five (5) Supplemental IG Metrics. Determinations for each function were made based on the average score of the FY 2025 Core metrics and the FY 2025 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.
- Supplemental Metrics – Metrics that are not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. For FY 2025, the supplemental metrics comprised of five new metrics designed to gauge the maturity of agencies' cybersecurity

[4] NIST Cybersecurity Framework 2.0 (https://www.nist.gov/cyberframework)

governance practices and implementation of key components of Zero-Trust Architecture (ZTA).

Maturity Level Scoring

OMB and DHS continued with a calculated average scoring model for FY 2025. 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 HHS 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 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.[5]

In FY 2025, 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 divisions, and 25 systems (five at each Division), that were representative of the broader IT environment implemented at HHS.

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.

[5]Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (https://www.cisa.gov/resources-tools/resources/fy-2025-ig-fisma-metrics)

Section 2
Conclusions and Enterprise-wide Recommendations

Section 2: Conclusion and Enterprise-wide Recommendations

2.1 Conclusion

We determined that HHS's information security program was "Not Effective." This determination was made based on HHS not meeting the 'Managed and Measurable' maturity level for all six (6) function areas: Govern, Identify, Protect, Detect, Respond, and Recover. Individual domain and function "Effective" or "Not Effective" 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. Certain domains lacked Core or Supplemental metrics and were consequently labeled as "N/A" in Table 2. In these instances, the domain was evaluated solely on the metrics selected for the FY 2025 IG assessment. The detailed list of findings for these domains was provided to HHS management outside of this report. Table 2 below provides the FY 2025 IG FISMA Maturity results and calculated scores.

Table 2: 2025 HHS Maturity Levels Assessment Results

Cybersecurity Framework Function	FISMA Domain	Assessment Results for FY 2025 Core Metrics	Assessment Results for FY 2025 Supplemental Metrics	FY 2025 IG Assessment by Domain
Govern	*Cybersecurity Governance*	N/A	Ad Hoc	Not Effective
	Cybersecurity Supply Chain Risk Management	Defined	N/A	Not Effective
Identify	*Risk and Asset Management*	Consistently Implemented	Ad Hoc	Not Effective
Protect	*Configuration Management*	Defined	N/A	Not Effective
	Identity & Access Management	Defined	N/A	Not Effective
	Data Protection & Privacy	Consistently Implemented	N/A	Not Effective
	Security Training	Defined	N/A	Not Effective
Detect	*Information Security Continuous Monitoring*	Consistently Implemented	Defined	Not Effective
Respond	*Incident Response*	Consistently Implemented	N/A	Not Effective

Cybersecurity Framework Function	FISMA Domain	Assessment Results for FY 2025 Core Metrics	Assessment Results for FY 2025 Supplemental Metrics	FY 2025 IG Assessment by Domain
Recover	*Contingency Planning*	Consistently Implemented	N/A	Not Effective
Overall Maturity		Consistently Implemented	Ad Hoc	Not Effective

GOVERN

The goal of the Govern function is to ensure HHS's cybersecurity risk management strategy, expectations, and policies are established, communicated, and monitored. Within this function, there are two domains: Cybersecurity Governance and Cybersecurity Supply Chain Risk Management. Cybersecurity Governance was at an "Ad Hoc" maturity level, and Cybersecurity Supply Chain Risk Management was at a "Defined" maturity level, and our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function	FISMA Domain	FY 2025 IG Assessment
Govern	Cybersecurity Governance	Ad Hoc
	Cybersecurity Supply Chain Risk Management	Defined

Cybersecurity Governance Findings

Cybersecurity Governance (CG) involves activities that pertain to maintaining comprehensive and effective oversight over HHS's cybersecurity posture, its risk management strategy, and its cybersecurity roles, responsibilities, and authorities.

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

- Metric: HHS should develop and maintain current and target cybersecurity profiles.
  - Three of the selected Divisions had not defined processes and procedures for developing and maintaining current and target cybersecurity profiles.
  - Cybersecurity profile requirements had not been defined by HHS policy and no formal guidance had been developed and disseminated to Divisions or other HHS organizations on the extent of profiles (entity level, division level, etc.) that need to be developed to design and measure an effective cybersecurity program.
- Metric: HHS should utilize a cybersecurity risk management strategy to support operational risk decisions.
  - Two of the selected Divisions had not defined processes and procedures for developing and maintaining cybersecurity risk management strategies to enable operational risk decisions.

  - Risks associated with recent reorganization efforts were not incorporated into existing risk management processes to provide for an adequate risk response or mitigation.
  - Roles and responsibilities within the Cybersecurity Risk Management Strategy (CRMS) were not reevaluated based on the reorganization plan put forward by Management.
- Metric: HHS should document and conduct evaluations of the performance of cybersecurity roles and responsibilities.
  - One of the selected Divisions was unable to demonstrate that cybersecurity duties were incorporated in relevant positions descriptions and cybersecurity risk management objectives were included within performance plans and assessments.
  - HHS had not maintained up-to-date policies and/or reviews of their governing documentation in accordance with their defined cadence.

Cybersecurity 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 finding was identified within the agency's SCRM program:

- Metric: Documented policies and procedures should be implemented.
  - Four of the selected Divisions had not fully implemented their SCRM policies and procedures.

IDENTIFY

The goal of the Identify function is to develop HHS's 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. There is one domain in this function: Risk and Asset Management, which was at a "Defined" maturity level. Our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function	FISMA Domain	FY 2025 IG Assessment
Identify	Risk and Asset Management	Defined

Risk and Asset Management Findings

The Risk Management Framework (RMF), 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:

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

an assessment of management's long-term plan for implementing risk management strategies, documented goals and objectives of the entity, and prioritization of IT needs.

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

- Metric: Inventories of systems and applications, hardware, and software should be accurately maintained.
  - One of the selected Divisions failed to maintain a comprehensive and accurate system inventory.
  - One of the selected Divisions was unable to determine if the systems within their inventory contained personally identifiable information (PII), interfaces, or whether the systems are public facing.
  - One of the selected Divisions did not have a hardware asset inventory that contained the standard data elements described in the policy.
  - One of the selected Divisions was unable to demonstrate the annual audit of the hardware asset inventory was performed as defined in the Standard Operating Procedure (SOP).
  - One of the selected Divisions did not maintain an up-to-date inventory of software licenses. Additionally, one of the selected Divisions did not have a process in place for tracking software asset and licenses.
- Metric: A data inventory should be accurately maintained.
  - Four of the selected Divisions did not maintain a comprehensive and accurate inventory of data and corresponding metadata for its data types. Department guidance on the extent to implement data architecture requirements to support zero trust implementation had not been developed. Further, there was limited guidance about role responsibilities in data governance and lack of formal zero-trust implementation strategy defined, inclusive of metadata tagging requirements to support implementation.
- Metric: System security risks should be adequately managed at HHS, mission/business process, and information system levels, and considered throughout the system lifecycle.
  - Two of the selected Divisions had not implemented an automated solution for a centralized, enterprise-wide view of cybersecurity risks across HHS.

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 was at "Defined" and our overall assessment of this function is "Not Effective."

Cybersecurity Framework Function	FISMA Domain	FY 2025 IG Assessment
Protect	Configuration Management	Defined
	Identity and Access Management	Defined
	Data Protection and Privacy	Consistently Implemented
	Security Training	Defined

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 and flaw remediation.

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

- Metric: Configuration settings should be utilized for systems and monitored for deviations from the baseline.
  - Two of the selected Divisions lacked common secure configurations for all their systems.
- Metric: Vulnerabilities identified on systems and assets should be remediated within the time frame specified by policy and procedure.
  - Four of the selected Divisions failed to consistently implement processes and procedures for flaw remediation. The Divisions were unable to provide artifacts to demonstrate that all sampled critical and high-risk vulnerabilities were tracked and remediated within 30 days.

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 Identity and Access Management program:

- Metric: Phishing-resistant multifactor authentication mechanisms should be implemented for non-privileged and privileged users.
  - One of the selected Divisions did not require phishing-resistant multifactor authentication to access agency facilities, systems, and networks for non-privileged and privileged users.
- Metric: Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties.
  - One of the selected Divisions was unable to demonstrate their processes for provisioning, managing, and reviewing privileged accounts. Additionally, one of the selected Divisions did not perform monitoring over privileged user activities.

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[7] and BOD-18-02[8] 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:

- Metric: Data transiting outside the network should be monitored.
  - One of the selected Divisions did not monitor inbound and outbound traffic using a web content filter and therefore did not block restricted and malicious web content.

Security Training Findings

An information 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.

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

- Metric: HHS should conduct a workforce skills assessment and gap analysis to provide specialized security training.
  - Although HHS had defined processes and procedures for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment, three of the selected Divisions had not consistently implemented its process.
  - HHS had not assessed the knowledge, skills, and abilities of its workforce to identify skill gaps.

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," and our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function	FISMA Domain	FY 2025 IG Assessment
Detect	ISCM	Consistently Implemented

[7] OMB M-22-09 Federal Zero Trust Strategy (whitehouse.gov)

[8] BOD 18-02: Securing High Value Assets | CISA

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 Plan of Action and Milestones (POA&Ms), which are the three principal documents in a security authorization package.

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

- Metric: An ISCM strategy should be implemented at each organizational tier.
  - One of the selected Divisions did not consistently implement these policies and strategies.
- Metric: HHS should continuously monitor and measure the integrity and security posture of its owned and associated assets.
  - One of the selected Divisions had not completely implemented event logging requirements per M-21-31 (Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents).
  - One of the selected Divisions did not deploy an ISCM monitoring tool in its environment.

RESPOND

The goal of the Respond function is to develop and implement the appropriate activities to respond to 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," and our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function Area	FISMA Domain	FY 2025 IG Assessment
Respond	Incident Response	Consistently Implemented

Incident Response Findings

Incident Response involves capturing general threats and incidents that occur in 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 finding was identified regarding the agency's incident response program:

- Metric: Incidents should be detected, analyzed, and handled appropriately.

- One of the selected Divisions had 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. The domain within this function is Contingency Planning, which was assessed at "Consistently Implemented," and our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function	FISMA Domain	FY 2025 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 findings were identified regarding the agency's contingency planning program:

- Metric: Business impact analyses (BIAs) are utilized to prioritize recovery, and contingency plans are developed and tested periodically.
  - HHS had not conducted a BIA at HHS level or ensured all Divisions are maintaining BIAs to guide contingency planning efforts.
  - One of the selected Divisions had not conducted a BIA at the organizational or system-level.

2.2 Recommendations

To strengthen HHS's enterprise-wide information security program, based on our reviews of the five selected Divisions in scope, we recommend that HHS focus on progressing towards an effective program. We recommend that HHS:

1. Develop a formal process for creating and maintaining cybersecurity profiles (current and target), including developing policies and procedures and implementing these policies and procedures at the Department level and at the Division level.

2. Implement the Cybersecurity Risk Management Strategy at the Department level and confirm implementation of the CRMS at the Division level. All Divisions should inherit the HHS Department enterprise-wide risk management strategy or develop and implement their own. Additionally, HHS should confirm that all risks, including those incurred during organizational restructuring, are documented, evaluated, and accounted for according to the CRMS.
3. Require and ensure Divisions implement SCRM policy and procedures.
4. Update the departmental policy to accurately define cybersecurity roles and responsibilities and define the processes to evaluate the performance of cybersecurity roles and responsibilities.
5. Conduct the workforce skills assessment/gap analysis timely and periodically update the assessment/gap analysis to account for changes in the risk environment across HHS and the Divisions.
6. Confirm that Divisions maintain comprehensive and accurate software and hardware asset and license inventories and employ the use of information system security continuous monitoring (ISCM) tools to monitor the security posture of assets in accordance with the defined standards across HHS. HHS should confirm that implementation of these inventories is consistent with established standards.
7. Develop policies, procedures, and guidance for the creation and maintenance of data and metadata inventories. These policies, procedures, and guidance should be implemented throughout HHS. HHS should establish a process to monitor Divisions' adherence to department-level policies, procedures, and guidance.
8. Require Divisions to implement common secure configurations and effective flaw remediation processes for all their systems according to Divisions standards or standards approved by HHS for the Division. Divisions should ensure that scanning for compliance and vulnerabilities is performed according to HHS policies and procedures and that all deviations and vulnerabilities are remediated within the defined timelines set by HHS. HHS should confirm that Divisions are meeting the established standards.
9. Enforce HHS policies and procedures for provisioning and monitoring access of all privileged users and confirm implementation aligns with the policies and procedures. Privileged user access requests with the required approval should be documented and retained.
10. Enforce policies and develop procedures for conducting and updating Business Impact Analyses (BIAs) and require implementation at the Department level and Division level. Divisions should implement as necessary and reference HHS policy as part of their contingency planning efforts to standardize the prioritization of business operations and functions.

HHS OCIO COMMENTS AND OFFICE OF THE INSPECTOR GENERAL RESPONSE

In written comments to the report, HHS OCIO concurred with seven of our ten recommendations and did not concur with three of the recommendations.

HHS OCIO stated that it did not concur with our fourth recommendation because they believe the recommendation does not accurately reflect the current state of implementation. We made this recommendation in part due to the number of policies that were out of date and not reviewed within the last three years in accordance with HHS policy. These policy failures have a correlation with implementation findings throughout the organization including but not limited to: Cyber Supply Chain Risk Management, Information Technology Asset Management, Vulnerability Management, and the Organization Continuity of Operations Plan. Additionally, management acknowledges these ongoing efforts in their response. Therefore, we maintain the validity of our recommendation.

HHS OCIO stated that it did not concur with our ninth recommendation because they believe it does not accurately reflect the current state of privileged access governance and enforcement. We made this recommendation to improve the OCIO's oversight responsibilities. Responsibilities should not only include policy development but also include validating implementation of the existing policies. Specifically, event logging and the monitoring of privileged user activity was a repeated challenge across HHS divisions during our testing even though existing policies and procedures have defined the requirement. Management acknowledges these challenges in their response. Therefore, we maintain the validity of our recommendation.

HHS OCIO stated that it did not concur with our tenth recommendation because responsibility for conducting and updating BIAs appropriately resides with each Operating Division under HHS's federated operating model. We agree that the responsibility for conducting and updating BIAs resides with each Operating Division. However, we made this recommendation because the Department's oversight responsibility includes confirming implementation of HHS policies for conducting BIAs. In this instance, we found BIAs not being completed despite existing policy in place. Therefore, we maintain the validity of our recommendation.

HHS OCIO'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 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*[9] (IG FISMA Reporting Metrics) as of August 1, 2025.

The FY 2025 IG FISMA reporting metrics were assessed at HHS and results were based on the aggregation of their results from the operating divisions selected for testing. In FY 2025, we tested HHS's information security controls across five (5) divisions: Centers for Medicare and Medicaid Services (CMS), the Office of the Secretary (OS), Agency for Healthcare Research and Quality (AHRQ), Indian Health Service (IHS), and Administration for Community Living (ACL). We mapped the current year OARS to prior year findings for the two (2) Divisions that were tested in both FY 2024 and FY 2025.

In March of 2025, HHS announced and initiated efforts to restructure the Department.[10] As a result of the restructuring that impacted one of the Divisions selected for testing, Administration for Community Living (ACL), we adjusted our audit plan for only ACL. The adjustments resulted in additional findings reported in the governance domain within Section II.

Methodology

We mapped HHS's key information security controls to the metrics in the FY 2025 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 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

[9]Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (https://www.cisa.gov/resources-tools/resources/fy-2025-ig-fisma-metrics)

[10] HHS Announces Transformation to Make America Healthy Again | HHS.gov (https://www.hhs.gov/press-room/hhs-restructuring-doge.html)

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.

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's security program against HHS information security 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 FY 2025 IG FISMA metrics. Incorporated the results as part of the FY 2025 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.

Additionally, we reviewed and responded to HHS management's comments on the reported findings and recommendations.

[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)

[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 (2025 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 Office of the Chief Information Officer Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

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

DATE: February 3, 2026

TO: John D. Hagg, Deputy Inspector General for Audit Services (Acting)

FROM: Clark Minor, Chief Information Officer CM

SUBJECT: OIG Draft Report: *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025 (OAS-25-18-041)*

The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) thanks the Office of the Inspector General (OIG) for your review of the HHS security program for fiscal year (FY) 2025. We welcome the opportunity to respond to the report developed by Ernest & Young on your behalf.

As requested, our office has reviewed the aforementioned report and has attached written comments regarding the validity of facts, actions taken, and planned actions, based on your recommendations. We look forward to continuing our collaboration efforts to enhance 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 reach out to the HHS Chief Information Security Officer (Acting), Christopher Bollerer, at Christopher.Bollerer@hhs.gov or 202-774-2121.

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 2025 (OAS-25-18-041)***

cc:
Clark Minor, Chief Information Officer
Christopher Bollerer, Chief Information Security Officer (Acting)
Charles Summers, Assistant Director, OIG Cybersecurity and IT Audit Division
Tamara Lilly, Assistant Inspector General, 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 2025*** **(OAS-25-18-041)**

Enterprise-wide Recommendations

To strengthen HHS's enterprise-wide cybersecurity program, based on our reviews of the five selected Divisions in scope, we recommend that HHS focus on progressing towards an effective program. We recommend that HHS:

1. Develop a formal process for creating and maintaining cybersecurity profiles (current and target), including developing policies and procedures and implementing these policies and procedures at the Department level and at the Division level.

   HHS Response: ***Concur***

   While HHS fully understands the condition in this OARS that "the organization has not defined policies and procedures for requiring, developing, and maintaining current and target cybersecurity profiles", the reality of significant organizational changes implemented during this audit and their impact on existing policies must be highlighted as having a direct impact on the development of this condition.

   During this same time frame, there was an agency-directed stop on all related policy development and update activities due to the kickoff of an HHS effort to address various policy challenges. Resultantly, in late July 2025, OCIO embarked on a complete review of department IT policy and guidance.

   The ultimate goal is to complete the implementation of a new and consolidated set of IT polices by the end of July 2026 for HHS to be able to begin the process to remediate not having defined policies and procedures for requiring, developing, and maintaining current and target cybersecurity profiles.

2. Implement the Cybersecurity Risk Management Strategy at the Department level and confirm implementation of the CRMS at the Division level. All Divisions should inherit the HHS Department enterprise-wide risk management strategy or develop and implement their own. Additionally, HHS should confirm that all risks, including those incurred during organizational restructuring, are documented, evaluated, and accounted for according to the CRMS.

   HHS Response: ***Concur***

   While HHS fully understands the condition in this OARS that "the HHS Cybersecurity Risk Management Strategy (CRMS) had not been fully

implemented", and that "(1) Risks associated with recent reorganization efforts were not incorporated into existing risk management processes to provide for an adequate risk response or mitigation AND (2) Roles and responsibilities within the CRMS were not re-evaluated based on the reorganization plan put forward by Management".

It is unrealistic to expect reorganization efforts or reorganization plans to impact the CRMS while HHS continues to experience significant ongoing organizational changes implemented during this audit. This impact on existing policies and strategies must be highlighted as having a direct impact on the development of the overall condition and sub-conditions.

Additionally, during this same time frame, there was an agency-directed stop on all related policy development and update activities due to the kickoff of an HHS effort to address various policy challenges. Resultantly, in late July 2025, OCIO embarked on a complete review of department IT policy and guidance.

The HHS Cybersecurity Risk Management Strategy (CRMS) will be impacted in this overall effort, as it serves as the framework for our agency's existing Risk Management approach and will need to be re-examined to ensure it reflects the bandwidth needed for operating divisions to meet their mission needs.

The ultimate goal is to complete the implementation of a new and consolidated set of IT polices by the end of July 2026 for HHS to be able to begin the process to remediate not having defined policies and procedures for requiring, developing, and maintaining current and target cybersecurity profiles.

3. Require and ensure Divisions implement SCRM policy and procedures.

HHS Response: ***Concur***

HHS concurs with the recommendation to require and ensure Division implementation of Supply Chain Risk Management (SCRM) policies and procedures. While HHS has established SCRM-related policies and programs, including the HHS Cyber Supply Chain Risk Management (C-SCRM) Program Policy and the CRMS, the Department acknowledges gaps in consistent Division-level implementation and enterprise visibility.

HHS operates within a federated environment in which Divisions are responsible for implementing SCRM controls in accordance with Department policy and NIST guidance. During the audit period, implementation and oversight were affected by

organizational changes and a Department-wide effort to consolidate and modernize IT and cybersecurity policies.

As part of the ongoing IT and cybersecurity policy consolidation effort, OCIO will reinforce SCRM requirements through consolidated policy and supporting guidance to clarify implementation expectations, roles, and accountability. In coordination with the Office of National Security (ONS), which manages the E-SCRM Program Policy, OCIO will support strengthening oversight mechanisms to confirm Division implementation, clarify inheritance versus Division-specific responsibilities, and improve enterprise visibility into SCRM risks.

In the interim, Divisions will continue to conduct supply chain risk assessments in accordance with existing SCRM procedures under ONS leadership with OCIO support. HHS will confirm Division-level implementation following policy finalization and provide updates to the OIG as corrective actions progress.

4. Update the departmental policy to accurately define cybersecurity roles and responsibilities and define the processes to evaluate the performance of cybersecurity roles and responsibilities.

HHS Response: ***Non – Concur***

HHS respectfully non-concurs with this recommendation. The Department has already established cybersecurity roles and responsibilities, as well as mechanisms to evaluate performance, through existing policies, governance structures, and operational processes.

Cybersecurity roles and responsibilities are defined and implemented through authoritative sources, including the HHS Delegation of Authority, the HHS Policy for Information Security and Privacy Protection (IS2P), governance charters, role-based position descriptions, and Division-level implementation consistent with HHS's federated operating model. Performance and accountability are evaluated through management controls, operational reporting, risk management activities, and established oversight forums.

While HHS acknowledges that recent organizational changes and the ongoing IT policy consolidation effort may require alignment and streamlining of how roles and responsibilities are documented across policy artifacts, this does not indicate that roles, responsibilities, or performance evaluation processes are undefined or lacking. Accordingly, HHS believes the recommendation does not accurately

reflect the current state of implementation, and no separate corrective action is required beyond the ongoing policy consolidation effort.

5. Conduct the workforce skills assessment/gap analysis timely and periodically update the assessment/gap analysis to account for changes in the risk environment across HHS and the Divisions.

   HHS Response: ***Concur***

   HHS concurs with the recommendation to conduct workforce skills assessments and periodically update gap analyses to reflect changes in the risk environment. Consistent with HHS's federated operating model and Delegation of Authority, OpDivs are responsible for assessing cybersecurity workforce gaps and ensuring completion of role-based training in accordance with IS2P, the HHS Control Catalog (including AT-3), and Department training requirements.

   At the Department level, HHS OCIO supports and coordinates workforce development efforts to improve enterprise visibility into cybersecurity skill gaps. While a formal Department-wide workforce skills assessment has not yet been conducted on a recurring cadence, the HHS Cybersecurity Community of Practice has completed a supply-and-demand analysis aligned to the NICE Workforce Framework and identified key cybersecurity skill gaps.

   In November 2024, the Cybersecurity Community of Practice completed a Department-level analysis identifying priority cybersecurity skill gaps and associated action plans. HHS will build on this effort to mature a more structured and repeatable approach for aggregating Division-level gap information and periodically revalidating skill gaps based on evolving risk conditions. HHS OCIO will continue coordinating with OpDivs to support workforce planning, update gap analyses and role-based training as appropriate and provide updates to the OIG as these efforts progress.

6. Confirm that Divisions maintain comprehensive and accurate software and hardware asset and license inventories and employ the use of information system security continuous monitoring (ISCM) tools to monitor the security posture of assets in accordance with the defined standards across HHS. HHS should confirm that implementation of these inventories is consistent with established standards.

   HHS Response: ***Concur***

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 2025*** **(OAS-25-18-041)**

HHS concurs with the recommendation to confirm that OpDivs maintain accurate software, hardware, and license inventories and employ ISCM capabilities in accordance with HHS standards. Consistent with the Department's federated operating model, OpDivs are responsible for asset inventory management and ISCM implementation in accordance with IS2P, the HHS System Inventory Management Standard, and applicable NIST guidance.

HHS has made progress in strengthening its ISCM program, including approval of the ISCM Working Group charter in December 2023 and the ISCM Strategy in November 2024. However, a formal ISCM policy has not yet been finalized due to the ongoing IT and cybersecurity policy consolidation effort. While enterprise ISCM standards exist, Divisions are not required to adopt uniform ISCM or CDM tools, as ISCM encompasses broader processes and governance beyond specific tooling.

HHS will advance the ISCM policy through the Policy Tiger Team process and incorporate it into the consolidated HHS cybersecurity directive to formalize requirements, clarify expectations for asset inventory accuracy and monitoring practices, and strengthen Department-level visibility into Division implementation. HHS and the ISCM Program will provide updates to the OIG as milestones and corrective actions progress.

7. Develop policies, procedures, and guidance for the creation and maintenance of data and metadata inventories. These policies, procedures, and guidance should be implemented throughout HHS. HHS should establish a process to monitor Divisions' adherence to department-level policies, procedures, and guidance.

   HHS Response: ***Concur***

   HHS concurs with this recommendation. The Department recognizes the importance of establishing consistent, Department-wide policies, procedures, and guidance for the creation, maintenance, and management of data and metadata inventories to support effective data governance, risk management, and Zero Trust objectives.

   In coordination with the HHS CIO, the Chief Data Officer (CDO) is responsible for developing and maintaining Department-wide policies, procedures, and guidance governing data and metadata inventories. These efforts are aligned with the FY 2025 HHS Open Data Plan and are being advanced through the OneHHS approach to promote consistent implementation across all HHS Divisions.

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 2025*** **(OAS-25-18-041)**

HHS will establish and maintain a monitoring process to assess Division-level adherence to Department-level data and metadata inventory requirements. This process will leverage existing governance, reporting, and oversight mechanisms to improve visibility into implementation status and support corrective actions where gaps are identified. HHS will provide updates to the HHS OIG as these activities progress and milestones are established.

8. Require Divisions to implement common secure configurations and effective flaw remediation processes for all their systems according to Division standards or standards approved by HHS for the Division. Divisions should ensure that scanning for compliance and vulnerabilities is performed according to HHS policies and procedures and that all deviations and vulnerabilities are remediated within the defined timelines set by HHS. HHS should confirm that Divisions are meeting the established standards.

   HHS Response: ***Concur***

   HHS concurs with the recommendation to require OpDivs to implement secure configuration settings and effective flaw remediation processes, perform vulnerability and configuration compliance scanning in accordance with HHS policies, and remediate identified vulnerabilities within established timelines.

   Consistent with HHS's federated operating model and Delegation of Authority to OpDiv CIOs, responsibility for implementing secure configurations, conducting vulnerability scanning, and remediating vulnerabilities resides with each OpDiv in accordance with IS2P, the HHS Control Catalog (including SI-2, Flaw Remediation), the HHS Policy for Vulnerability Management, and the Plan of Action and Milestones (POA&M) Standard.

   HHS is strengthening Department-wide visibility and oversight of vulnerability remediation through modernization of its vulnerability management and Continuous Diagnostics and Mitigation (CDM) capabilities. This includes deployment of Tenable One to provide centralized visibility into vulnerability and remediation metrics across OpDivs, with licensing expected in the first quarter of FY26 and OpDiv migration throughout FY26.

9. Enforce HHS policies and procedures for provisioning and monitoring access of all privileged users and confirm implementation aligns with the policies and procedures. Privileged user access requests with the required approval should be documented and retained.

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 2025*** **(OAS-25-18-041)**

HHS Response: ***Non – Concur***

HHS respectfully non-concurs with this recommendation. The Department has established and implemented policies, procedures, and controls governing the provisioning, monitoring, documentation, and review of privileged user access in accordance with HHS policy and NIST requirements.

Privileged access management requirements are defined in authoritative Department policies and standards, including IS2P and the HHS Control Catalog (e.g., AC-2, AC-6, IA-2). These policies require that privileged access requests be approved, documented, retained, and periodically reviewed, and that privileged user activity is logged and monitored.

While HHS acknowledges that consistent implementation across all Operating Divisions (OpDivs) can be challenging due to the Department's federated environment and diverse system architectures, these challenges reflect execution variability rather than a lack of policy, procedures, or enforcement mechanisms.

HHS is actively strengthening enterprise privileged access management through the expansion of Department-wide PAM capabilities, issuance of reinforcing guidance, and integration of privileged account monitoring into ISCM activities. These efforts are focused on improving consistency and maturity of execution across OpDivs, not establishing new policy requirements. Accordingly, HHS believes the recommendation does not accurately reflect the current state of privileged access governance and enforcement.

10. Enforce policies and develop procedures for conducting and updating Business Impact Analyses (BIAs) and require implementation at the Department level and Division level. Divisions should implement as necessary and reference HHS policy as part of their contingency planning efforts to standardize the prioritization of business operations and functions.

HHS Response: ***Non – Concur***

HHS does not concur with this recommendation. The Department has established policies, standards, and oversight mechanisms governing the development, maintenance, and use of Business Impact Analyses (BIAs), and responsibility for conducting and updating BIAs appropriately resides with each OpDiv under HHS's federated operating model.

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 2025*** **(OAS-25-18-041)**

In accordance with the HHS Policy for IS2P and the HHS Control Catalog, including control CP-2 (Contingency Plan) and related enhancements, OpDivs are responsible for ensuring that operational systems maintain complete and up-to-date BIAs and that BIA results are incorporated into system-level contingency planning activities.

While the Department agrees that BIAs are critical to effective contingency planning and prioritization of mission-essential functions, the recommendation's emphasis on Department-level enforcement and execution does not align with HHS's delegated authorities or federated structure.

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