Department of Health and Human Services

Office of Inspector General

Office of Audit Services

October 2026 | OAS-26-18-047

Review of the Department of Health and Human Services' Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2026

The Department of Health and Human Services' FY 2026 Federal Information Security Modernization Act (FISMA) Report

October 26, 2026



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

Shape the future with confidence

Report of Independent Auditors on the Department of Health and Human Services' FY 2026 Federal Information Security Modernization Act (FISMA) Report Based on a Performance Audit Conducted in Accordance with *Government Auditing Standards*

To: Charles Summers
Acting 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, 2026, 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 (IG) 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 Inspector General (IG) 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 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 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

October 26, 2026

Table of contents

Section 1: Overview 1
1.1 Objective 1
1.2 Background 1

Section 2: Conclusion and Enterprise-wide Recommendations 5
2.1 Conclusion 5
2.2 Recommendations 13

Section 3: Appendices 16
3.1 Appendix A: Scope and Methodology 16
3.2 Appendix B: Federal Requirements and Guidance 18
3.3 Appendix C: HHS Office of the Chief Information Officer Comments 20

Abbreviations

BIA	Business Impact Analysis
CISO	Chief Information Security Officer
CDM	Continuous Diagnostic and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CM	Configuration Management
CP	Contingency planning
CG	Cybersecurity Governance
CRMS	Cybersecurity Risk Management Strategy
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
EY	Ernst & Young LLP (EY US)
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
IR	Incident Response
ISCM	Information System Continuous Monitoring
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PHI	Protected Health Information
PII	Personally identifiable information
POA&M	Plan of Action and Milestones
RAM	Risk and Asset Management
SCRM	Supply Chain Risk Management
SSP	System Security Plans
ST	Security Training
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 Department) 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*[1] (IG FISMA Reporting Metrics) as of July 31, 2026.[2]

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 confirming 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 with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security 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 engaged us, Ernst & Young LLP (EY US), 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

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

[2] On March 17, 2026, DHS CISA issued a Joint Message from OMB and CIGIE establishing the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics as the FY 2026 criteria.

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

(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 with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0[4] function areas. To promote consistency in the annual FISMA evaluations, CIGIE, in coordination with OMB, DHS, and the Federal Chief Information Officers (CIO) and CISO councils developed the FY 2025 IG FISMA metrics Evaluator's Guide, issued May 5, 2025.[5]

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 core metrics and the 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.

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

[5] On March 17, 2026, DHS CISA issued a Joint Message from OMB and CIGIE establishing the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics as the FY 2026 criteria.

- 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 2026, the supplemental metrics comprised of five new metrics designed to gauge the maturity of agencies' cybersecurity 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 2026. 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*.[6, 7]

In FY 2026, 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.

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

[7] On March 17, 2026, DHS CISA issued a Joint Message from OMB and CIGIE establishing the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics as the FY 2026 criteria.

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 Department was at an overall effective level (Managed and Measurable) for the domain and corresponding function. We developed a Notice of Findings and Recommendations (NFR) for each finding identified during testing and provided the NFR 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 HHS's overall information security program was "Not Effective" based on our assessment at the "Consistently Implemented" maturity level. 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. The IG FISMA Reporting Metrics for FY2026 did not contain core or supplemental metrics to assess for certain domains 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 2026 IG assessment. The detailed list of findings for these domains was provided to HHS management outside of this report.

Table 2: 2026 HHS Maturity Levels Assessment Results

Cybersecurity Framework Function	FISMA Domain	Assessment Results for FY 2026 Core Metrics	Assessment Results for FY 2026 Supplemental Metrics	FY 2026 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*	Consistently Implemented	N/A	Not Effective
	Identity & Access Management	Consistently Implemented	N/A	Not Effective
	Data Protection & Privacy	Consistently Implemented	N/A	Not Effective
	Security Training	Ad Hoc	N/A	Not Effective
Detect	*Information Security Continuous Monitoring*	Consistently Implemented	Consistently Implemented	Not Effective
Respond	*Incident Response*	Consistently Implemented	N/A	Not Effective
Recover	*Contingency Planning*	Defined	N/A	Not Effective
Overall Maturity		Consistently Implemented	Ad Hoc	Not Effective

GOVERN

The goal of the Govern function is to confirm 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 2026 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 Department'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.
  - Two of the selected divisions had not fully implemented their processes for developing cybersecurity profiles, including assessing gaps and creating a prioritized action plan.
  - 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.
  - Three 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 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.

- Three of the selected divisions were unable to demonstrate that cybersecurity duties were communicated, understood, and incorporated in relevant position 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 and failed to confirm that required policy approvals were obtained.

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 Department's SCRM program:

- Metric: documented policies and procedures should be implemented.
  - All 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 "Consistently Implemented" maturity level. Our overall assessment of this function was "Not Effective."

Cybersecurity Framework Function	FISMA Domain	FY 2026 IG Assessment
Identify	Risk and Asset Management	Consistently Implemented

Risk and Asset Management Findings

The risk management framework (RMF), developed by NIST,[8] 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, and prioritization of IT needs.

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

- Metric: Inventories of systems and applications, hardware, and software should be accurately maintained.

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

- All selected divisions had not fully implemented their SCRM policies and procedures.
- Three of the selected divisions had system inventories which could not be reconciled with the HHS enterprise listing. One of these three divisions failed to maintain a comprehensive and accurate system inventory by either omitting systems or failing to recognize the correct operational status of a system.
- 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.
- Three of the selected divisions did not have a hardware asset inventory that contained the standard data elements described in the policy.
- Three of the selected Divisions did not maintain an up-to-date inventory of software licenses.

- Metric: A data inventory should be accurately maintained.
  - All 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 and business process, and information system levels, and considered throughout the system lifecycle.
  - Three of the selected divisions had not consistently performed system risk or security control assessments in accordance with the timeline required by policy.
  - 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 confirm 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 was "Not Effective."

Cybersecurity Framework Function	FISMA Domain	FY 2026 IG Assessment
Protect	Configuration Management	Consistently Implemented
	Identity and Access Management	Consistently Implemented
	Data Protection and Privacy	Consistently Implemented
	Security Training	Ad Hoc

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 Department'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 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 implement phishing-resistant multifactor authentication to access Department's 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.
  - Three of the selected divisions did not implement processes for provisioning, managing, and reviewing privileged accounts consistently.

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[9] and BOD-

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

18-02[10] 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 Department's data protection and privacy program:

- Metric: Data should be protected throughout its entire lifecycle.
  - One of the selected divisions did not implement security controls to protect the confidentiality, integrity, and availability of PII and other sensitive data.
- Metric: Data transiting outside the network should be monitored.
  - One of the selected divisions had not defined its policies and procedures related to preventing data exfiltration and enhancing network defenses.
  - 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 Department's security training program:

- Metric: HHS should conduct a workforce skills assessment and gap analysis to provide specialized security training.
  - Three of the selected divisions had not defined processes and procedures for assessing the knowledge, skills, and abilities of their workforce to identify skill gaps and determine specialized training needs.
  - Workforce gap assessment requirements had not been defined by HHS policy. In addition, HHS had not completed or updated its workforce gap assessment to account for their current risk environment.

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

DETECT

The goal of the Detect function is to develop and implement 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 2026 IG Assessment
Detect	Information Security Continuous Monitoring	Consistently Implemented

Information Security 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 Department's Information Security Continuous Monitoring program:

- Metric: An ISCM strategy should be implemented at each organizational tier.
  - Two of the selected divisions did not consistently implement their ISCM policies and strategies.
- Metric: HHS should continuously monitor and measure the integrity and security posture of its owned and associated assets.
  - Three of the selected divisions have not linked security posture monitoring to hardware inventories or implemented enforcement mechanisms.

RESPOND

The goal of the Respond function is to develop and implement 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	FISMA Domain	FY 2026 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 Department's incident response program:

- Metric: Incidents should be detected, analyzed, and handled appropriately.
  - One of the selected Divisions had not consistently implemented incident notification and reporting requirements across its environment.

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

Cybersecurity Framework Function	FISMA Domain	FY 2026 IG Assessment
Recover	Contingency Planning	Defined

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 Department'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 enterprise level or confirmed all divisions are maintaining BIAs to guide contingency planning efforts.
  - Two of the selected divisions had not conducted a BIA at the organizational or system-level.
  - One of the selected Divisions had not consistently documented system-level BIAs to include key recovery metrics and priorities for system resources.
  - Four of the selected Divisions have not tested information system contingency plans periodically.

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 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 confirm 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. Develop policies, procedures, and guidance for assessing the skills, knowledge, and abilities of HHS's workforce. 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 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 confirm 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 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.
11. Require Divisions to implement information system contingency plan testing and exercises according to Division standards or standards approved by HHS for the Division. Divisions should confirm that contingency plans are tested regularly for all systems within their environment. HHS should confirm that Divisions are meeting the established standards.

HHS OCIO COMMENTS AND OFFICE OF THE INSPECTOR GENERAL RESPONSE

HHS concurred with seven (7) of our 11 recommendations, did not concur with our fourth recommendation, and partially concurred with three (3) of our 11 recommendations.

HHS stated that it did not concur with our fourth recommendation because it believes the recommendation does not accurately reflect the development of cybersecurity roles and responsibilities within the IS2P. At the time of the conclusion of our fieldwork, management had not yet fully completed the policy rewrites related to the IS2P nor had it published the final policy for system teams and divisions to follow. We made certain elements of this recommendation because management was in the process of updating the roles and responsibilities within the IS2P. Management acknowledges these ongoing efforts in its response; therefore, we maintain the validity of our recommendation.

HHS stated that it did not fully concur with our sixth recommendation because it believes the recommendation does not accurately reflect the current state of implementation. We made certain elements of this recommendation based on our observation that Department's existing process to collect asset information has consistently resulted in inaccurate inventories within the Department's CDM program. HHS has been in the process of implementing various CDM tools over the last 5 years, and our observation identified a lack of enforcement on existing implementation requirements which has resulted in incomplete inventories. The lack of enforcement against policies does not require the implementation of a new toolset; therefore, we maintain the validity of our recommendation.

HHS stated that it did not fully concur with our eighth recommendation because it believes the recommendation does not accurately reflect the current state of implementation. We made this recommendation in part due to the observation that Divisions and the selected systems were not consistently implementing secure configuration requirements or complying with Department policies for addressing the remediation of vulnerabilities. Management acknowledges in its response that it has ongoing activities to improve upon the Departments visibility into Division-level compliance; therefore, we maintain the validity of our recommendation.

HHS stated that it did not fully concur with our tenth recommendation because responsibility for conducting and updating BIAs appropriately resides with each Division under HHS's federated operating model. We agree that the responsibility for conducting and updating BIAs resides with each Division. However, we made this recommendation because the Departments' oversight responsibilities include confirming implementation of HHS's policy to conduct a BIA. In this instance, we found BIAs were not being done despite the requirement in existing policy. Management acknowledges in its response that it concurs with strengthening Department-level procedures and oversight to promote consistent implementation of implementation across Divisions. Therefore, we maintain the validity of our recommendation.

HHS's 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 EY US'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*[11] (IG FISMA Reporting Metrics) as of July 31, 2026.[12]

The FY 2026 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 2026, we tested HHS's information security controls across five (5) Divisions: Centers for Medicare & Medicaid Services (CMS), the Office of the Secretary (OS), Administration for Strategic Preparedness and Response (ASPR), National Institutes of Health (NIH), and Substance Abuse and Mental Health Services Administration (SAMHSA). We mapped the current year NFRs to prior year findings for the two (2) Divisions that were tested in both FY 2025 and FY 2026.

Methodology

We mapped HHS's key information security controls to the metrics in the FY 2026 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 Publication 800-53, Revision 5,[13] *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.

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

[12] On March 17, 2026, DHS CISA issued a Joint Message from OMB and CIGIE establishing the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics as the FY 2026 criteria.

[13] 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[14] (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 2026 IG FISMA Reporting Metrics. Incorporated the results as part of the FY 2026 IG FISMA Reporting 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.

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

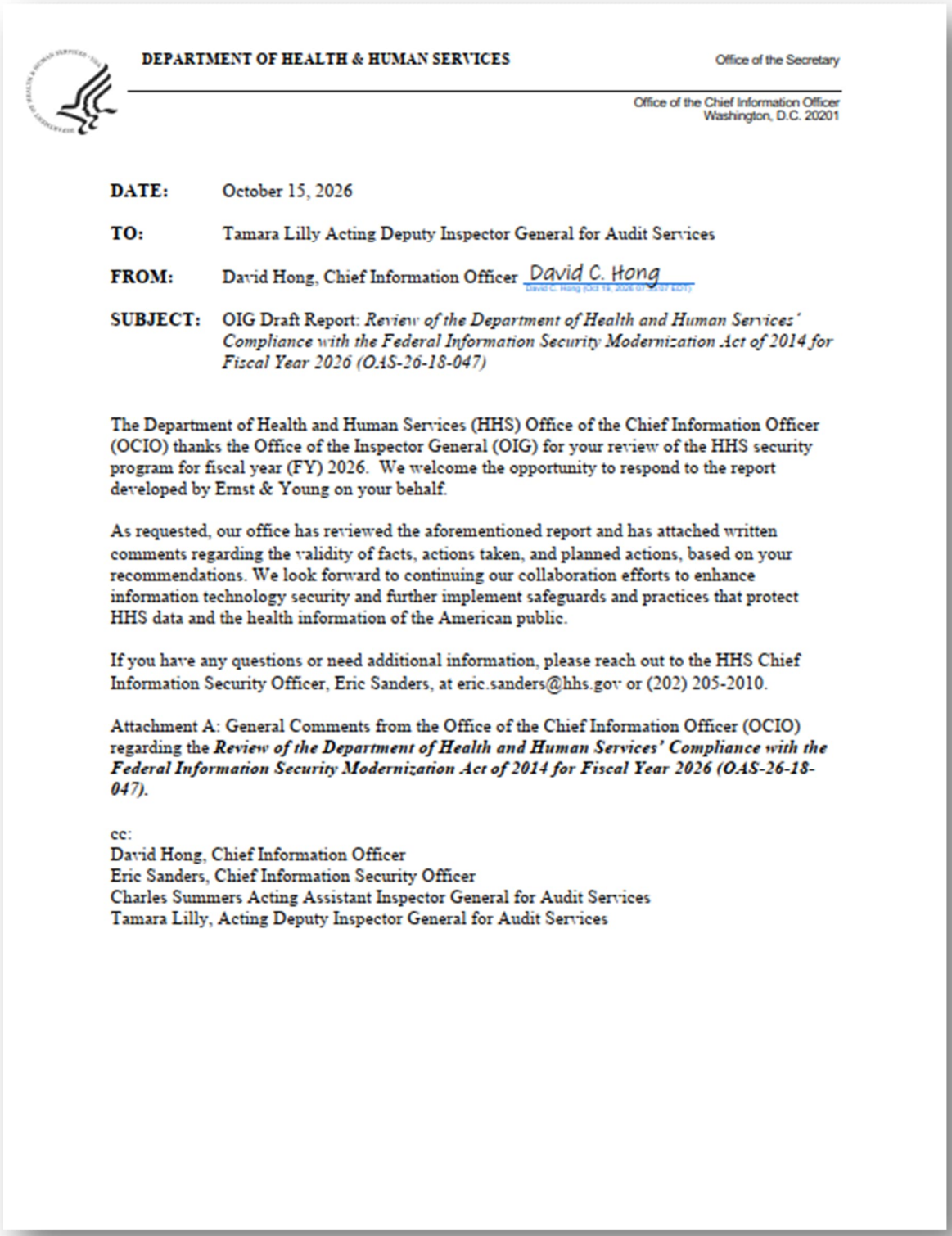
3.2 Appendix B: Federal Requirements and Guidance

The principal criteria used for this performance audit included:

- DHS Binding Operational Directive 18-02, Securing High Value Assets, (May 07, 2018)
- 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, Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile* (April 2025)
- NIST IR 8286, Revision 1, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (December 2025)
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011)
- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017)
- OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program* (December 10, 2018)
- OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 21, 2019)
- OMB Circular A-123, *Management's Responsibility for Internal Control* (March 10, 2026)
- OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures* (August 10, 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-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022)

- OMB M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* (January 15, 2025)
- OMB M-26-05, *Adopting a Risk-based Approach to Software and Hardware Security* (January 23, 2026)
- OMB M-26-14, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats* (May 22, 2026)

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: October 15, 2026

TO: Tamara Lilly Acting Deputy Inspector General for Audit Services

FROM: David Hong, Chief Information Officer David C. Hong

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 2026 (OAS-26-18-047)*

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) 2026. We welcome the opportunity to respond to the report developed by Ernst & 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, Eric Sanders, at eric.sanders@hhs.gov or (202) 205-2010.

Attachment A: General Comments 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 2026 (OAS-26-18-047).***

cc:
David Hong, Chief Information Officer
Eric Sanders, Chief Information Security Officer
Charles Summers Acting Assistant Inspector General for Audit Services
Tamara Lilly, Acting Deputy Inspector General for Audit Services

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

ATTACHMENT A: General Comments 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 2026*** **(OAS-26-18-047)**

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***
   An agency-directed pause was placed on IT policy development and updating activities to support a Department-wide initiative addressing broader HHS policy challenges. The policy revision/review/development effort resumed in March 2026.

   Additional efforts remain underway to establish a centralized policy repository, update and consolidate existing policies, develop new policies where needed, and strengthen policy governance through organizational improvements. Overall responsibility for the Department-level risk profile rests with Assistant Secretary for Financial Resources (ASFR), the Office of the Secretary (including OIS), and Division Chief Operating Officers (COOs), with the HHS Enterprise Risk Management (ERM) Council coordinating Department-wide ERM activities. The ERM Council is responsible for overseeing development of the Department-level risk profile and must first establish or update the Department's cyber risk appetite before related cybersecurity profile activities can proceed. These activities are expected to be completed by the end of 2027.

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***
   An agency-directed pause was placed on IT policy development and updating activities to support a Department-wide initiative addressing broader HHS policy challenges. The policy revision/review/development effort resumed in March 2026. The OIS Risk Team began reviewing the Cybersecurity Risk Management

ATTACHMENT A: General Comments 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 2026*** **(OAS-26-18-047)**

Strategy (CRMS) in June 2026 and will work to ensure that the forthcoming update reflects organizational changes. To date, those organizational changes remain underway.

The CRMS update is dependent on updates to the Department-wide ERM risk profile and finalization of the OIS Strategy. Once these predecessor activities are completed, the CRMS can be updated to align with the Department's current organizational structure, risk posture, and strategic direction. The OIS Policy Team will lead development of applicable Department-level policies and guidance, while Divisions will be responsible for defining their implementing procedures. These activities are anticipated to be completed by the end of 2027. In the meantime, HHS will work with Divisions to confirm whether they have adopted the current Department CRMS or documented their own strategy, identify any gaps, and retain evidence of how their approaches address Department requirements. Once the CRMS update is complete, HHS will distribute the revised CRMS to the Divisions and confirm adoption or identify any Division-specific strategies established.

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

HHS Response: ***Concur***
As part of the ongoing IT and cybersecurity policy consolidation effort, Office of the Chief Information Officer (OCIO) will reinforce Supply Chain Risk Management (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 Enterprise-SCRM (ESCRM) Program Policy, OCIO will help strengthen oversight mechanisms to confirm Division-level implementation, clarify inherited versus Division-specific responsibilities, and improve enterprise visibility into SCRM risks.

In the interim, selected Divisions have been authorized to conduct independent Supply Chain Risk Assessments (SCRAs). Divisions will continue conducting SCRAs in accordance with existing SCRM procedures, under ONS leadership and with OCIO support. HHS will confirm Division-level implementation following policy finalization and provide updates to OIG as corrective actions progress. SCRAs have been conducted for system vendors within the following categories: High-Value Assets (HVAs), Critical Software, General Software, HHS sponsored FedRAMP associated vendors and FY26 Acquisitions. As of July 15, 2026, all planned SCRAs for these populations have been completed.

ATTACHMENT A: General Comments 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 2026*** **(OAS-26-18-047)**

The Cybersecurity Supply Chain Risk Management (C-SCRM) Working Group will also serve as a forum to communicate the outcomes of the targeted SCRAs and support implementation of the revised C-SCRM policy. Approval of the C-SCRM policy is expected by the end of the first quarter of FY27.

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***
   Cybersecurity roles and responsibilities are clearly defined in the Information Security and Privacy Policy (IS2P). The IS2P serves as the overarching policy that establishes HHS security requirements and assigns overall cybersecurity roles and responsibilities. The IS2P has undergone a thorough review and update process and was approved by the CISO, dated September 29, 2026. The IS2P is waiting to be published.

   In addition, the Office of Human Resources (OHR) Human Capital Accountability Directorate provides employee performance policy and guidance enterprise wide.

5. Develop policies, procedures, and guidance for assessing the skills, knowledge, and abilities of HHS's workforce. 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***
   The OHR, (HHS Workforce Planning Branch), in coordination with the OCIO and the HR Action Council on Workforce Planning, will establish and implement a Department-wide process to periodically aggregate and assess cybersecurity workforce skills data from HHS Components and Subcomponents using the NICE Workforce Framework. The process will include conducting recurring cybersecurity workforce skills gap analyses, validating identified gaps against the evolving cybersecurity risk environment, coordinating with Components to update workforce development and role-based training plans, as appropriate, and tracking progress through the HHS Cybersecurity Community of Practice. These activities will support enterprise-wide workforce planning and continuous improvement.

   In addition, HHS is implementing an enterprise-wide staffing plan to recruit and retain personnel with the cybersecurity skills and competencies needed to address identified workforce gaps.

ATTACHMENT A: General Comments 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 2026*** **(OAS-26-18-047)**

The OHR through the HR Action Council on Workforce Planning, will also review applicable cybersecurity position descriptions and employee performance plans to ensure that cybersecurity responsibilities are accurately documented and that cybersecurity risk management objectives are incorporated, as appropriate, in accordance with HHS policy and applicable Office of Personnel Management (OPM) guidance. Where deficiencies are identified, OHR will update position descriptions and performance plans and implement a periodic review process to ensure that cybersecurity roles and performance objectives remain current and aligned with organizational responsibilities.

Additionally, the Workforce Planning Cybersecurity Action Council is now fully established and includes new subject-matter experts representing key Components across the Department. The Council will resume and complete the cybersecurity workforce supply-and-demand skills gap assessment, incorporating updated workforce data, emerging cybersecurity requirements, and enterprise-wide expertise.

The revised target completion date for the assessment is the end of the first quarter of FY 2027.

6. Confirm that Divisions maintain comprehensive and accurate software and hardware asset and license inventories and employ the use of 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: ***Partially Concur***
   HHS plans to implement Xacta as its enterprise Governance, Risk, and Compliance (GRC) platform to strengthen cybersecurity governance, asset accountability, and Information Security Continuous Monitoring (ISCM) capabilities. The Department's Continuous Diagnostics and Mitigation (CDM) Program currently collects hardware and software asset information through integrated security tools across participating Divisions.

   HHS will evaluate opportunities to integrate CDM asset and security posture data with Xacta to support centralized reporting, inventory reconciliation, and continuous monitoring activities. This effort will include assessing existing data coverage, system boundary associations, and integration capabilities, while identifying gaps in software license tracking and authoritative inventory sources.

   Additionally, HHS will work toward establishing consistent ISCM monitoring and

ATTACHMENT A: General Comments 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 2026*** **(OAS-26-18-047)**

reporting requirements across Divisions, including defined reporting frequencies and minimum requirements aligned with departmental standards and each Division's security posture.

Acquisition and implementation of the enterprise GRC platform are targeted for completion by the end of the fourth quarter of FY 2027, subject to the established implementation schedule.

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 OCIO is in the process of recruiting and hiring a permanent Chief Data Officer (CDO) to build upon work done earlier this year under the Acting CDO and to work with OCIO to establish the path forward for the Office of the Chief Data Officer (OCDO) to address OIG Finding 26-A-18-055.07. In accordance with OMB Memorandum M-25-05 and the Foundations for Evidence-Based Policymaking Act of 2018, HHS published the Department-wide data inventory consistent with DCAT-US 3.0 metadata standard by September 30, 2026. Additionally, the Department is revising the underlying IT architecture to facilitate inventory development and maintenance. The OCDO is also developing policies, procedures, and guidance for HHS Divisions to provide metadata from their supporting inventories to the Department's centralized inventory.

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 confirm 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: ***Partially Concur***
   HHS will continue deploying Tenable One and integrating vulnerability data into the CDM Dashboard to improve enterprise visibility into vulnerability remediation. HHS will complete planned integrations with Armis, Axonius, and the Security Governance, Risk, and Compliance (SGRC) tool to improve asset ownership information, vulnerability reporting, and dashboard accuracy. HHS will also continue improving data quality and expanding vulnerability context

ATTACHMENT A: General Comments 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 2026*** **(OAS-26-18-047)**

fields to support risk-based remediation prioritization. These activities are estimated to be completed by the end of the fourth quarter of FY 2027.

Daily work supporting BOD 26-04 and Cyber Hygiene (CYHY) includes coordinating with Divisions on vulnerability reporting and remediation status, distributing CISA findings in CYHY reports, collecting, and consolidating Division responses, and following up on outstanding submissions and identified vulnerabilities. Leadership dashboards and vulnerability trend reports provide visibility into findings requiring attention and support reporting updates to CISA.

These activities support this recommendation by providing ongoing monitoring and follow-up to help HHS confirm that Divisions are addressing identified vulnerabilities within required timelines. They support the vulnerability remediation portion of the recommendation; confirmation of secure configuration compliance requires additional scanning and supporting evidence.

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.

   HHS Response: ***Concur***
   The Department continues to strengthen its enterprise Privileged Access Management (PAM) capabilities to promote consistent implementation across Divisions. HHS will continue expanding its enterprise PAM capabilities, issuing supplemental guidance to support consistent implementation of existing Department policies, and integrating privileged account monitoring into ISCM activities to improve Department-wide visibility. HHS will also continue to ensure Divisions are implementing and enforcing PAM policies, reinforcing compliance with privileged access requirements established in Department policy. These efforts are intended to strengthen implementation and oversight while reinforcing compliance with privileged access requirements established in Department policy.

   Integration of privileged account monitoring into Department ISCM activities and issuance of supplemental implementation guidance to the Divisions are estimated to be completed by the end of the fourth quarter of FY 2027.

10. Enforce policies and develop procedures for conducting and updating 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: ***Partially Concur***
HHS previously non-concurred with this recommendation based on the Department's established Business Impact Analysis (BIA) policies, standards, and delegated responsibilities under its federated operating model. Based on subsequent actions to strengthen Department-level standardization and oversight of BIA activities, HHS is revising its position to partially concur with the recommendation.

The Department has established policies, standards, and oversight mechanisms governing the development, maintenance, and use of BIAs. Consistent with HHS's federated operating model, responsibility for conducting, validating, and maintaining BIAs resides with each Division.

In accordance with the HHS Policy for IS2P and the HHS Control Catalog, including control CP-2 (Contingency Plan) and related enhancements, Divisions 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 HHS does not concur with the recommendation's emphasis on Department-level execution of BIAs, HHS concurs with strengthening Department-level procedures and oversight to promote consistent implementation across Divisions. HHS is engaging Division Continuity Managers and developing a sample Business Process Analysis (BPA) to support a more standardized approach while awaiting updated FEMA guidance. Existing HHS requirements remain in effect during this period.

Upon issuance of updated FEMA guidance, HHS will assess any necessary changes, reengage Divisions, and establish a standardized Department-wide approach for BIA methodology, documentation, review, and oversight, including a process for monitoring Division implementation. Overall completion is projected by the end of Q2 FY2028, contingent upon FEMA's issuance of updated requirements.

11. Require Divisions to implement information system contingency plan testing and exercises according to Division standards or standards approved by HHS for the Division. Divisions should confirm that contingency plans are tested regularly for

ATTACHMENT A: General Comments 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 2026*** **(OAS-26-18-047)**

all systems within their environment. HHS should confirm that Divisions are meeting the established standards.

HHS Response: ***Concur***

HHS will restart its department-wide Business Process Analysis (BPA) in October 2026 to identify critical functions and their dependencies. The subsequent BIA will assess disruption impacts and establish recovery priorities. Divisions will validate the information for their operations, incorporate applicable results into system contingency plans, and continue required plan testing, while HHS will provide common direction and monitor Division implementation. Together, the following strategies describe how HHS will guide and oversee this work, how Divisions will validate and apply the results, and how both will use those results to strengthen contingency planning and testing.

Divisions will continue to test applicable system contingency plans at the frequency required by HHS standards and document the results, deficiencies, and corrective actions. HHS will monitor Division testing records and track unresolved findings against established requirements. As the restarted BPA and subsequent BIA identify and validate critical functions, system dependencies, and recovery priorities, Divisions will incorporate those results into their contingency plans and future test scenarios. The test results will show whether recovery procedures can meet the documented needs and identify where plans or corrective actions require updating.

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