Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Amy J. Frontz
Deputy Inspector General
for Audit Services

June 2024
A-18-23-11200

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

Office of Audit Services. OAS provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, the anti-kickback statute, and other OIG enforcement authorities.

Department of Health and Human Services

FY 2023 Federal Information Security Modernization Act (FISMA) Report

June 24, 2024

Building a better working world

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

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

Report of Independent Auditors on the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023 Based on a Performance Audit Conducted in Accordance with *Government Auditing Standards*

Ms. Tamara Lilly
Assistant Inspector General for Audit Services

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

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. The nature, timing, and extent of the procedures selected depend on our judgment. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To audit HHS' compliance with FISMA, we applied the *FY 2023 – 2024 Inspector General FISMA Reporting Metrics* to the information security program and practices of HHS to determine the effectiveness. The specific scope and methodology are defined in Appendix A of this report.

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

The conclusions in Section II and our findings and recommendations, as well as proposed actions for the improvement of HHS' compliance with FISMA in Section III, were noted based on our audit.

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; it is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

June 24, 2024

Report in Brief

Date: June 2024
Report No. A-18-23-11200

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

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023

Why We 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. HHS OIG engaged Ernst & Young LLP (EY) to conduct this audit.

EY conducted a performance audit of HHS' compliance with FISMA as of July 31, 2023, based upon the FISMA reporting metrics defined by the Inspectors General.

Our objective was to determine whether HHS' overall information technology security program and practices were effective as they relate to Federal information security requirements.

How We Did This Audit

We reviewed applicable Federal laws, regulations, and guidance; gained an understanding of the current security program at the Department level and the security programs at four (4) of the 12 Operating Divisions (OpDivs) and one (1) Staff Division (StaffDiv); assessed the status of HHS' security program against the Department and selected OpDivs' information security program policies, other standards and guidance issued by HHS management, and prescribed performance measures; inquired of personnel to gain an understanding of the FISMA reporting metric areas; inspected selected artifacts; and conducted procedures on prior-year issues.

What We Found

Overall, through the evaluation of FISMA metrics, it was determined that the HHS' information security program was "Not Effective." This determination was made based on HHS' inability to meet the "Managed and Measurable" maturity level for the Core and Supplemental Inspector General metrics in the function areas of Identify, Protect, Detect, Respond, and Recover. Overall, the HHS information security program rated ineffective for FY 2023, matching the evaluated program rating from FY 2022. HHS is a federated environment and large disparities continue to exist between the maturity levels at individual OpDivs and StaffDivs. While better performing OpDivs are approaching or at a Managed and Measurable maturity level, certain OpDivs and StaffDiv selected for the audit are either stagnant in their progress towards the Managed and Measurable maturity rating or are regressing and significantly below the Managed and Measurable maturity rating. The Department continues to define and update policies that are distributed to OpDivs and StaffDivs to assist with their own policy definitions or guide consistent implementation of a compliant cybersecurity strategy. However, the Department must go beyond defining and updating policies to achieve the Managed and Measurable level.

What We Recommend

We made recommendations to the Office of the Chief Information Officer to improve its oversight and to enforce accountability to further strengthen HHS's information security program and enhance information security controls at HHS. Recommendations specific to deficiencies found at the reviewed HHS OpDivs and StaffDiv were provided separately. HHS should commit to implementing recommendations identified within this report and incorporate enhancements into the overall formal cybersecurity maturity strategy that allows HHS to continue to advance its information security program from its current maturity state to Managed and Measurable. HHS should work to ensure that findings are communicated across the organization to increase awareness of identified gaps to help decrease disparity shown across OpDivs and StaffDivs.

In written comments to our report, HHS concurred with our Department and OpDiv recommendations, and enterprise-wide recommendation 3; while not concurring with enterprise-wide recommendations 1, 2, 4, 5, and 6. For two non-concur responses regarding duplicative recommendations, the recommendations are similar but not identical to address weaknesses at the Department and OpDiv levels. For one non-concur related to the repeat of a similar recommendation made in the FY2022 FISMA audit report. The recommendation was removed from this report and the FY2022 recommendation will remain open until addressed. For two non-concur responses, they were associated with the separation of responsibilities between the HHS OCIO and OpDivs. We maintain that our recommendations are valid.

Table of Contents

Section 1
Background

Section 1: Background

1.1 Introduction

We conducted a performance audit of the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of July 31, 2023, based upon the questions outlined in the *FY 2023 – 2024 Inspector General FISMA Reporting Metrics*.

1.2 Background

On December 17, 2002, the President signed the Federal Information Security Management Act into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). 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. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendment included the: (1) 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, including assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

To comply with FISMA, OMB, the Council of the Inspectors General on Integrity and Efficiency, Federal Civilian Executive Branch Chief Information Security Officers and their staff, and the Intelligence Community developed the FY 2023 IG FISMA reporting metrics, issued April 13, 2022. 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. The FY 2023 evaluation was completed by Ernst & Young LLP, under contract to the HHS Office of Inspector General, Office of Audit Services as a performance audit in accordance with the Government Accountability Office's *Government Auditing Standards*.

Cybersecurity Framework

The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. The FY 2023 IG Metrics mark a continuation of the work begun in FY 2016 when the IG metrics were aligned to the five function areas in the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity*: Identify, Protect, Detect, Respond, and Recover.

For FY 2023, updates were made to the IG FISMA metrics to align with Executive Order 14028 of May 12, 2021, "Improving the Nation's Cybersecurity," as well as OMB guidance M-22-09 "Federal Zero Trust", M-21-31 "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents", M-22-05 "Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements", and M-22-01 "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response" to agencies in furtherance of the modernization of federal cybersecurity. As a result, twenty (20) Core IG Metrics were selected for evaluation as to the effectiveness of the organization's information security program. In addition, twenty (20) rotating supplemental metrics were assessed to assist with maturity determination.

The FY 2023 IG FISMA Reporting Metrics are grouped into nine domains and aligned to the five Cybersecurity Framework function areas:

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

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

Reporting Metrics

For the FY 2023 IG FISMA Metrics, a series of metrics (or questions) were developed for each IG FISMA domain to assess the effectiveness of an agency's cybersecurity framework.

Maturity Level Scoring

The maturity level scoring was prepared by OMB and DHS. Level 1 (Ad-hoc) is the lowest maturity level and Level 5 (Optimized) is the highest maturity level. The details of the five maturity model levels are:

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

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

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

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

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

For FY 2023, further updates were made to the IG FISMA metrics to align with Executive Order 14028 of May 12, 2021, "Improving the Nation's Cybersecurity," as well as OMB guidance M-22-09, M-21-31, M-22-05, and M-22-01 to encourage agencies to shift toward a continuous assessment process. As a result, OMB implemented a new framework regarding the timing and focus of the assessments. The goal of this new framework was to provide a more flexible but continued focus on annual assessments for the federal community. This effort yielded two distinct groups of metrics: Core and Supplemental.

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

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

Further, OMB and DHS introduced a calculated average scoring model for FY 2023 and FY 2024. As part of this approach, Core metrics and Supplemental metrics will be averaged independently to determine a domain's maturity calculations and provide data points for the assessed program and function effectiveness. OMB and DHS further defined that scoring evaluations should be based on agencies' risk tolerance and threat models and that as a result, calculated averages should not be automatically rounded to a particular maturity level. In

determining maturity levels and the overall effectiveness of the agency's information security program, OMB and DHS encouraged a focus on the results of the Core metrics and usage of the calculated averages of the supplemental metrics as a data point to support their risk-based determination of overall program and function level effectiveness. Within the context of the maturity model, Level 4 (Managed and Measurable) represents an "effective" level of security. However, DHS allows OIG to deviate from the standard for determining the "effective" level of security when an agreed-upon methodology is determined.

HHS Shared Responsibility Model

The HHS information security program follows a shared responsibility model that recognizes that the Department, the HHS Operating Divisions (OpDivs), and contractors are critical to risk management. This model also recognizes that the responsibilities for certain aspects of risk management change between each stakeholder, depending upon the roles assigned to defining, implementing, and overseeing the operation of any given control. Assignments for those activities can and do change over time, often in conjunction with changes implemented to increase control maturity and especially where control implementation strategies change among centralized, federated and hybrid implementation strategies.

HHS Office of the Chief Information Officer Information Security and Privacy Program

The Office of the Chief Information Officer (OCIO) leads the development and implementation of enterprise information technology (IT) infrastructure across HHS. The office establishes and provides support for e-government initiatives, IT operations management, IT investment analysis, cybersecurity and privacy, performance measurement, policies to provide improved management of information resources and technology, strategic development and implementation of information systems and infrastructure, and technology-supported business process reengineering.

The HHS Chief Information Security Officer (CISO) is responsible for developing and maintaining the Department's information security and privacy program. This enterprise-wide program is designed to help protect HHS against cybersecurity threats. The OCIO information security and privacy program plays an important role in protecting HHS's ability to provide mission-critical operations by issuing security and privacy policies, standards, and guidance; overseeing the completion of privacy impact assessments; providing incident reporting policy and incident management guidelines; and promoting IT security awareness and training.

Due to Delegation of Authority to the OpDiv Chief Information Officers (CIOs), each OpDiv's CIO is responsible for establishing, implementing, and enforcing an OpDiv-wide framework to facilitate its information security program based on policies and standards provided by the HHS CIO and CISO. The OpDiv CISOs are responsible for implementing department and OpDiv cybersecurity policies and procedures. OpDiv personnel and contractors are responsible for executing the cybersecurity and privacy program as defined by HHS and each OpDiv on behalf of HHS.

Section 2
Conclusion and Enterprise-wide Recommendations

Section 2: Conclusion and Enterprise-wide Recommendations

2.1 Conclusion

Our specific conclusions related to HHS' information security program for each of the FISMA domains are based on the FISMA reporting metrics.

Based on the results of our performance audit of the FY 2023 IG FISMA Metrics, we determined that HHS' information security program was "Not Effective." This determination was made due to several factors including the fact that HHS has disparities within the ratings between OpDivs. Specifically, while some OpDivs are reaching a "Managed and Measurable" level, other OpDivs continue to operate with little to no advancements in maturity beyond "Defined". Additionally, the "Not Effective" rating was based on HHS not meeting the "Managed and Measurable" maturity level for five of the five function areas: Identify, Protect, Detect, Respond, and Recover.

Table 2 below provides the FY 2023 IG FISMA Maturity assessment results and comparison against FY 2022. In FY 2023, the maturity levels for all domains remained the same as FY 2022 outside of Information System Continuous Monitoring (ISCM), which increased. Areas where HHS' security program needed improvement are captured by our enterprise-wide recommendations and specific findings in Section 3.

Table 2: FY 2023 vs FY 2022 HHS Maturity Levels

Function	Domain	OIG Assessed Domain Maturity		OIG Assessed Function Maturity	
		FY22	FY23	FY22	FY23
Identify	***Risk Management***	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
	Supply Chain Risk Management	Defined (Level 2)	Defined (Level 2)		
Protect	***Configuration Management***	Consistently Implemented	Consistently Implemented	Consistently Implemented	Consistently Implemented

Function	Domain	OIG Assessed Domain Maturity		OIG Assessed Function Maturity	
		FY22	FY23	FY22	FY23
Detect	***Identity & Access Management***	(Level 3)	(Level 3)	(Level 3)	(Level 3)
	Data Protection & Privacy				
	Security Training				
	Information Security Continuous Monitoring	Defined (Level 2)	Consistently Implemented (Level 3)	Defined (Level 2)	Consistently Implemented (Level 3)
Respond	***Incident Response***	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Recover	***Contingency Planning***	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)

Progress in some function areas has not been achieved due to weaknesses identified across all domains as well as lack of implementation of HHS policy and processes at multiple OpDivs. Detailed findings for these domains have been provided, along with others as identified, in Section III of this report. The following outlines specific failures to meet effective maturity ratings in each domain:

Risk Management

In the area of Risk Management, we noted that the in-scope OpDivs lack inventory management at the system hardware and software levels as required by OMB guidance. In the absence of proper inventory management, HHS exposes itself to the risk of limited asset visibility into its information systems components, which could affect HHS's ability to properly oversee and manage its information resources. Ineffectiveness in maintaining an inventory could lead to difficulties in tracking configuration changes, version control, and ensuring consistency in system configurations. Finally, HHS risks a lack of ability to maintain and sustain the resources and infrastructure supporting the system. Additionally, in this domain, the OpDivs did not implement their risk management strategy using reports/dashboards showing automated tracking of cybersecurity risks, activities, and Plans of Action and Milestones (POA&Ms). Without the use of monitoring reports/dashboards, HHS may not resolve cybersecurity risks and issues timely possibly resulting in risk exposure exceeding predefined or accepted risk tolerances.

Supply Chain Risk Management

In the area of Supply Chain Risk Management (SCRM), we noted that in-scope OpDivs did not consistently document policies for SCRM. Some OpDivs were not performing procedures to correlate their policies and processes to ensure consistency in assessing and reviewing supply chain-related risks associated with systems, suppliers, or contractors. In the absence of implemented supply chain management policies and procedures at all OpDivs, HHS is at risk of acquiring supplier components that do not meet HHS's minimum-security requirements, which can lead to a lack of appropriately vetted assets, compromise, reputational harm, etc.

Configuration Management

In the area of Configuration Management, some OpDivs did not ensure that vulnerabilities were identified and remediated within the timeframe required by the organization's policy. In the absence of timely vulnerability identification and remediation, HHS exposes itself to the risk of exploitation of the vulnerability by a bad actor. Additionally, within this domain it was noted that OpDivs did not appropriately document baseline configurations. Without established baseline configurations, HHS exposes itself to the risk of not having an accurate foundation for future builds, releases, or changes to systems. In addition, future implementations may not include the proper security and privacy controls. In addition, operational systems without defined baseline configurations may lack sufficient operational procedures, information about system components, network topology, or knowledge regarding local placement of components in the system architecture. Lastly, in this domain area, one OpDiv did not ensure the implementation of the Trusted Internet Connection (TIC) 3.0 program. The TIC program is a federal initiative designed to consolidate and improve the security of network connections at a federal organization. In the absence of an implemented TIC 3.0 program, HHS is at risk of not effectively improving the organization's security posture and incident response capability of external connections.

Identity and Access Management

In the area of Identity and Access Management, at some OpDivs it was noted that there were several instances in which the system owner had not implemented multi-factor authentication or an approved alternative strong authentication mechanism for privileged and non-privileged users. In the absence of a strong authentication mechanism, HHS exposes itself to an increased risk of unauthorized access to the organization's systems. Furthermore, multiple OpDivs are still working towards the implementation of user access reviews and audit logging for privileged user accounts.

Data Protection and Privacy

In the area of Data Protection and Privacy, it was noted that multiple OpDivs did not ensure the safeguard of personally identifiable information (PII) by use of Federal Information Processing Standards (FIPS)-validated encryption of PII, conduct Privacy Impact Assessments (PIA)s within the time frame required by the organization's policy, and consistently monitor inbound and

outbound traffic. In the absence of PII safeguards, HHS exposes itself to an increased risk of a potential privacy breach.

Security Training

In the area of security training (ST), it was noted that some OpDivs have not implemented a process to assess the knowledge, skills, and abilities of its workforce, tailored its awareness and specialized training, and identified its skill gaps. In the absence of a workforce analysis process, HHS exposes itself to an increased risk that individuals are ill-equipped to perform assigned security tasks and that the organization is unable to recognize current gaps and appropriately remediate failings that are due to improper or insufficient human resources.

Information Security and Continuous Monitoring

In the area of ISCM, it was noted that some OpDivs did not ensure that system owners conducted Authorizations-to-Operate (ATOs) and Security Assessment Reports (SARs) within the timeframe required by the organization's policy. In the absence of timely ATOs and SARs being performed/conducted, HHS exposes itself to the risk of not ensuring its systems meet information security and privacy requirements. In addition, there is a risk of failure to identify weaknesses and deficiencies in the system. Without this knowledge, the organization may fail to make appropriate risk-based decisions or comply with vulnerability mitigation procedures.

Incident Response

In the area of Incident Response, it was noted that some OpDivs did not ensure the use of common threat vectors to identify incidents as established per the US-CERT Federal Incident Notification Guidelines. Without the use of common threat vectors to identify incidents, HHS increases its risk of failing to maintain their desired level of risk acceptance. Proper identification of incidents allows organizations to not only direct proper response actions but also correctly evaluate their posture post-incident.

Contingency Planning

In the area of Contingency Planning, we noted that OCIO performs monthly reconciliations for expired or soon to expire contingency plan testing with the OpDivs and implemented the OCIO Contingency Planning Oversight program. However, we also noted that some OpDivs we reviewed did not conduct a Business Impact Analysis or ensure that system owners performed testing of their Contingency Plans within the timeframe required by the organization's policy. Without the necessary Contingency Planning tests and Business Impact Analysis being performed, HHS exposes itself to the risk of not properly planning for the relevant contingencies to successful recover from them. In addition, system recovery objectives may not reflect the applicable controls and guidance as determined by NIST and OMB. Finally, it is important to complete the required analysis to obtain a top-down view of significant risk exposures that should be addressed. These measures will allow HHS to facilitate achieving the managed and measurable level maturity level. This is a repeat finding from the FY 2022 FISMA

audit report.[1] A recommendation to address this finding will not be made in this report because we made a recommendation in the FY 2022 FISMA audit report which will remain open until the Department implements the appropriate corrective actions. .

2.2 Enterprise-wide Recommendations

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

1. Refine their enterprise architecture system inventory and software/hardware asset inventories to ensure the inclusion of the information systems and components active on the HHS network. HHS should utilize these inventories to monitor assets continuously and identify and remediate vulnerabilities timely to better manage the risks to these assets.

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

3. Confirm that all organization-wide and system-level risk assessments have been completed in an accurate and timely manner and include data points such as the threat vectors, likelihood, and tolerance level. This will help with the ability to address risks at the organization consistently and promptly.

4. Require OpDivs to implement an effective SCRM program that meets the defined standards across HHS and confirm implementation is consistent with established standard. HHS should ensure that all OpDivs are appropriately assessing vendors and submitting data points to assist with tracking and monitoring components on the network.

5. Require OpDivs to assess and inventory privileged user accounts across the agency by an established due date and confirm completion. HHS should confirm that OpDivs policies are defined to require privileged user account monitoring in both logging and activity reviews, preferably at an automated level.

HHS OCIO COMMENTS AND OFFICE OF THE INSPECTOR GENERAL RESPONSE

HHS concurred with our enterprise-wide recommendation 3; while not concurring with enterprise-wide recommendations 1, 2, 4, 5, and 6.

HHS stated two non-concur responses due to the recommendations being duplicative. The recommendations are similar but not identical to address weaknesses at the Department and

[1] *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022* (A-18-22-11200), issued May 2023.

OpDiv levels. One recommendation was made to the OpDivs for them to appropriately track software license information and maintain an accessible, up-to-date inventory for all their respective software licenses. Conversely, we made another recommendation to the Department focused on its oversight responsibility to ensure that the Department's enterprise architecture system inventory and software/hardware asset inventories include the inventories from each OpDiv. Additionally, the Department as required by FISMA should utilize the Department level inventories to monitor assets continuously and ensure that vulnerabilities are identified and remediated timely to better manage risks across the Department.

HHS stated one non-concur because it was a repeat of a similar recommendation made in the FY2022 FISMA audit report. We confirmed that it had not been addressed and removed it from this report. The previously made recommendation will remain open until addressed by the Department. HHS stated two non-concur responses due to the recommendations were associated with the separation of responsibilities between the HHS OCIO and OpDivs.

HHS also stated that due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, controls referenced in recommendations 1, 2, 4, 5, and 6 identify the OpDivs are responsible for ensuring that processes are in place to evaluate their implementation in a timely manner. While HHS is a federated environment, the OCIO remains responsible for leading the development and implementation of the enterprise information technology (IT) infrastructure across HHS. This includes establishing and overseeing the Department's information security and privacy program. The Delegation of Authority to the OpDiv CIOs for establishing, implementing, and enforcing an OpDiv-wide framework to facilitate its information security program is based on policies and standards provided by the HHS CIO and CISO. The Delegation of Authority does not change the responsibility for the OCIO to provide oversight of the Department's information security and privacy program. To fulfill its oversight responsibility, the OCIO should monitor and confirm that the OpDivs have implemented the polices and standards it has provided. We maintain that our recommendations are still valid.

HHS OCIO's full comments are provided in Appendix D.

Section 3
Department and OpDiv Findings and Recommendations

Section 3: Department and OpDiv Findings and Recommendations

3.1 Summary

This section consolidates the findings at each of the OpDivs reviewed against the five function areas within the Cybersecurity Framework. We identified several findings in HHS' security program and consolidated them into each of the nine domains related to the five functions. We also included recommendations that should assist the Department as they focus on achieving a higher maturity level. Management responses to these findings and auditor response to disagreements are documented in Appendix D.

3.2 Identify

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

Risk Management

The Risk Management Framework, developed by NIST, 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, documented goals and objectives of the entity, clearly defined roles and responsibilities for security management personnel, and prioritization of IT needs.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2023 IG Assessment	Change from FY 2022 IG Assessment
Identify	Risk Management	Consistently Implemented (Level 3)	No Change

The OCIO is responsible for ensuring that the OpDivs report all systems to the OCIO, identify their high-value assets, and report their POA&Ms. OpDivs are responsible for the implementation of their risk management program, which includes the assessment of risk, monitoring of vulnerabilities, and the resolution of security weaknesses.

Risk Management Findings and Recommendations

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

- At one (1) OpDiv, for one (1) of five (5) selected systems, the system with a Moderate risk profile, did not provide the most recent risk assessment report performed of the system. At another one (1) OpDiv, for two (2) of five (5) selected systems, the systems with a Moderate risk profile, did not provide the most recent SAR.
- Three (3) OpDivs were unable to provide software licenses as part of their software inventory.
- One (1) OpDiv was unable to provide an accurate or comprehensive system inventory due to identifier issues.
- Two (2) OpDivs were unable to provide an accurate or comprehensive hardware inventory.
- At one (1) OpDiv, twelve (12) of sixty-eight (68) selected federal information systems did not perform the required annual SARs. At one (1) OpDiv, two (2) of five (5) selected systems failed to perform their SARs in a timely manner.
- At one (1) OpDiv, one (1) of the five (5) selected systems had an expired Authorization to Operate.
- At one (1) OpDiv, one (1) of the five (5) selected systems did not ensure that all operational systems utilize technology/automation to provide a centralized, enterprise-wide (portfolio) view of cybersecurity risk management activities.

Based on our findings at the OpDivs, we recommend that the HHS OCIO monitor and confirm that the OpDivs:

- Conduct an annual review of the System Security & Privacy Plan and annually perform risk assessments for all operational systems, according to organizational policy.
- Appropriately track software license information and maintain an accessible, up-to-date inventory for all its software licenses.
- Perform the SAR and ATO in accordance with the organization's policy.
- Utilize automated solutions to provide a portfolio view of cybersecurity risk at the organization is consistently implemented in accordance with NIST standards.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

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.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2023 IG Assessment	Change from FY 2022 IG Assessment
Identify	Supply Chain Risk Management	Defined (Level 2)	No Change

Supply Chain Risk Management Findings and Recommendations

The following findings were identified within the OpDivs' SCRM program:

- Two (2) OpDivs did not define or document an organization Supply Chain Risk Management policy in compliance with NIST 800-53 criteria.

Based on our findings at the OpDivs, we recommend that the HHS OCIO:

- Confirm OpDivs define and implement an OpDiv level supply chain risk management strategy based on HHS departmental policy and NIST standards.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

3.3 Protect

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

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2023 IG Assessment	Change from FY 2022 IG Assessment
Protect	Configuration Management	Consistently Implemented (Level 3)	No Change
	Identity and Access Management	Consistently Implemented (Level 3)	No Change
	Data Protection and Privacy	Consistently Implemented (Level 3)	No Change
	Security Training	Consistently Implemented (Level 3)	No Change

Configuration Management

Configuration management involves activities that pertain to the operations, administration, maintenance, and configuration of networked systems and their security posture. Areas of configuration management include standard baseline configurations, anti-virus management, and patch management. As systems change, adjustments are often made to the system configuration. Effective configuration management ensures that these adjustments do not adversely affect the security of the system.

Configuration Management Findings and Recommendations

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

- At one (1) OpDiv, for ten (10) of the ten (10) vulnerabilities that were selected, the OpDiv did not provide evidence of the remediation of the vulnerabilities. At another one (1) OpDiv, fifteen (15) of the fifteen (15) selected vulnerabilities were not remediated within a timely manner. At one (1) OpDiv, vulnerability reports were unavailable.
- At one (1) OpDiv, for one (1) of the five (5) selected systems, the OpDiv did not provide evidence of baseline configurations.

- At one (1) OpDiv, one (1) of five (5) selected systems did not have documented baseline configurations. At one (1) OpDiv, all five (5) selected systems did not have documented baseline configurations.

- One (1) OpDiv had not defined policies and procedures to adopt the TIC 3.0 program to assist in protecting its network.

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

- Ensure that OpDivs' vulnerabilities are tracked and remediated in a timely manner and create POA&Ms for any vulnerabilities in accordance with the organization's policy.

- Ensure that all OpDivs' baseline configurations are documented and tracked for each system in the OpDiv.

- Ensure that all OpDivs' TIC 3.0 program use cases are reviewed for relevance and capabilities that are new to the latest revision of the TIC guidance are consistently implemented in accordance with HHS Policy for the Implementation of TIC and OMB M-19-26.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

Identity and Access Management

Federal agencies are required to establish 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.

Identity and Access Management Findings and Recommendations

The following findings were identified within the OpDivs' identity and access management program:

- At two (2) OpDivs, multi-factor authentication (MFA) or an alternative strong authentication mechanism for privileged and non-privileged users had not been implemented for one (1) of the five (5) selected systems. At another one (1) OpDiv, MFA had not been implemented. At another one (1) OpDiv, all five (5) selected systems failed to implement MFA.

- At one (1) OpDiv, evidence of all privileged accounts being provisioned, managed, and reviewed had not been provided for one (1) of the five (5) selected systems. At another one (1) OpDiv, policy governing privileged user accounts has yet to be defined and privileged user accounts are not being managed in accordance with NIST standards. At another two (2) OpDivs, privileged user activities had not been reviewed for four (4) of the five (5) selected systems.

- At one (1) OpDiv, evidence of a remote session timeout configuration had not been provided for one (1) of the five (5) selected systems. At one (1) OpDiv, remote access connections are not properly governed for all five (5) selected systems.

- At one (1) OpDiv, access agreements for users are not being properly tracked and renewed for two (2) of the five (5) selected systems. At one (1) OpDiv, access agreement completions are not properly tracked for all five (5) selected systems. At another OpDiv, access agreement completions are not properly tracked for four (4) of five (5) selected systems.

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

- Ensure that all OpDivs acquire the resources to fully implement MFA or an alternative strong authentication and implement multi-factor authentication or an alternative strong authentication for both privileged and non-privileged users on all operational systems.

- Ensure that all OpDivs provision, manage, and review privileged user accounts for operational systems.

- Ensure that all OpDivs are properly implementing remote session timeouts of 30 minutes (or less) for operating systems.

- Ensure that all OpDivs consistently implement access policies and procedures in accordance with the organization's Risk Management Safeguards policy across the organization.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

Data Protection and Privacy

Federal agencies have unique access to PII and protected health information (PHI) of US citizens. Many of HHS's systems contain PII and PHI, including systems that support the Medicare program and its 64 million beneficiaries. 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 have been established requiring agencies to report when this information is stored, how it is protected, and when breaches occur.

Data Protection and Privacy Findings and Recommendations

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

- At one (1) OpDiv, for one (1) of the five (5) selected systems, the system failed to provide evidence of the most recently completed PIA. At another one (1) OpDiv, for two (2) of the five (5) selected systems, PIAs were not completely in a timely manner.
- At one OpDiv, one (1) of the five (5) selected systems, did not provide evidence of implemented security controls to protect its PII and other agency data, as appropriate, throughout the data lifecycle (encryption methods to protect data in transit and data at rest).
- At one OpDiv, the organization does not have a policy defined to govern data protection and privacy, including securing PII, protecting against data exfiltration, and appropriately assessing systems via privacy threshold analyses and/or PIAs as necessary.

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

- Ensure that all OpDivs' operational systems have an approved and up-to-date PIA in accordance with the HHS Policy of Privacy Impact Assessment.
- Ensure that all OpDivs implement data encryption methods to protect data determined to be PII or sensitive by the systems and enhanced network defenses in accordance with NIST standards.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

Security Training

An effective IT security program cannot be established and maintained without providing adequate training to its information system users. People are generally considered one of the weakest links when it pertains to securing systems and networks. An adequate training system allows people to understand their roles, how to properly protect IT resources, and the effective implementation of organizational policies.

HHS's information security training function has the following in place:

- Security awareness and training strategy that leverages an organizational skills assessment.

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

- At two (2) OpDivs, the organization does not have a policy or procedures in place to define the requirements of their security training program or their workforce analysis strategy.

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

- Require and confirm that all OpDivs have a process in place to evaluate their workforce gaps. Furthermore, confirm that all OpDivs are implementing a compliant security training strategy as defined by overarching HHS policy.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

3.4 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 ISCM. Due to ISCM being assessed at a maturity level of "Defined," our overall assessment of this function was "Not Effective."

Information Security Continuous Monitoring

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. The implementation of a continuous diagnostic and mitigation program results in an approach to fortifying the cybersecurity posture through ongoing updates to system security plans, periodic security assessments, and POA&Ms, which are the three principal documents in a security authorization package.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2023 IG Assessment	Change from FY 2022 IG Assessment
Detect	ISCM	Consistently Implemented (Level 3)	Increased

ISCM Findings and Recommendations

The following findings were identified within the OpDiv's information security continuous monitoring program:

- At two (2) OpDivs, the organization has yet to define the policy or procedures to implement their ISCM strategy.
- At one (1) OpDiv, the organization was unable to provide dashboards or scans showing tools in place to detect or address vulnerabilities in their systems.

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

- Ensure that all OpDivs are inheriting and consistently implementing policies and procedures defined by HHS department level policy.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

3.5 Respond

The goal of the Respond function is to develop and implement the appropriate actions to take regarding a detected cybersecurity event. These activities include response planning, event communication, event analysis, and incident mitigation. 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. Our overall assessment of this function was "Not Effective" due to the Incident Response domain not yet being assessed at a maturity level of "Managed and Measurable."

Incident Response

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

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2023 IG Assessment	Change from FY 2022 IG Assessment
Respond	Incident Response	Consistently Implemented (Level 3)	No Change

HHS' Incident Response function has the following in place:

- Established monitoring requirements for security incidents identified across the enterprise, which includes detection, analysis, and handling.

Incident Response Findings and Recommendations

The following findings were identified within the OpDiv's Incident Response program:

- At one (1) OpDiv, the organization has failed to define and implement policies or procedures to implement their incident response strategy. The OpDiv was unable to provide incident logs or a plan to identify incidents using common threat vectors.
- At one (1) OpDiv, the organization has yet to implement policies and procedures to define common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents across the organization.

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO continuously monitor to ensure that all OpDivs:

- Inherit and consistently implement policies or procedures to govern their incident response strategy.
- Define common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents in accordance with NIST standards, US-CERT Federal Incident Notification Guidelines and OMB guidance across the organization.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

3.6 Recover

The goal of the Recover function is to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event or natural disaster. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. The domain that was assessed within this function is Contingency Planning. Due to Contingency Planning being assessed at a maturity level of "Defined," our overall assessment of this function was "Not Effective."

Contingency Planning

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 system's information confidentiality, integrity and availability requirements and the system impact level.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2023 IG Assessment	Change from FY 2022 IG Assessment
Recover	Contingency Planning	Defined (Level 2)	No Change

Contingency Planning Findings and Recommendations

The following findings were identified within the OpDiv's Contingency Planning program:

- At two (2) OpDivs, evidence of a complete and up-to-date Business Impact Analysis was not completed for two (2) of the five (5) selected systems. At another one (1) OpDiv, a complete and up-to-date Business Impact Analysis was not available for three (3) out of five (5) selected systems.

- At one (1) OpDiv, an up-to-date tabletop or functional test of their Contingency Plan and after-action report as required by organizational policy was not provided for one (1) of the five (5) selected systems.

- At two (2) OpDivs, a Contingency Plan test was not performed for one (1) of the five (5) selected systems.

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

- Require and confirm that all OpDivs' operational systems have a complete and up-to-date BIA.

- Require and confirm that all OpDivs' operational systems conduct Contingency Plan testing and exercises as required by their risk rating. Any testing and exercises conducted should be followed with after-action reports as necessary.

- Confirm that all OpDivs' policies and procedures covering Contingency Plan testing are in accordance with policy requirements by Departmental policy, NIST standards, and OMB guidance.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS's comments, excluding technical comments, are included as Appendix D.

Section 4
Appendices

Appendix A
Audit Scope and Methodology

Section 4: Appendices

4.1 Appendix A: Audit Scope and Methodology

Scope

We performed procedures to assess, based on OMB and DHS guidance, HHS's compliance with FISMA. To assess HHS's FISMA compliance, we leveraged the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. We developed an Objective Attribute Recap Sheet (OARS) for each finding identified during testing and provided the OARS to each OpDiv and HHS OCIO after the OIG's review and concurrence.

The FY 2023 – FY 2024 IG FISMA reporting metrics were assessed at selected HHS OpDivs and based on the aggregation of their results. We performed our fieldwork at the HHS OCIO and four HHS OpDivs:

- Centers for Medicare & Medicaid Services
- Food and Drug Administration
- Office of the Inspector General
- Office of the Secretary
- Substance Abuse and Mental Health Administration

Methodology

To accomplish our objective, we:

- Reviewed applicable Federal laws, regulations, and guidance.
- Gained an understanding of the current security program at HHS and selected OpDivs.
- Inquired of HHS OCIO and OpDiv personnel their self-assessment for each FISMA reporting metric.
- Assessed the status of HHS's security program against HHS and selected OpDiv 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 any results from Government Accountability Office and OIG audits and reports that had a similar scope to the FY 2023 IG FISMA metrics; incorporated the results as part of the FY 2023 IG FISMA metrics where applicable.

- 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.

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

Appendix B
Federal Requirements and Guidance

4.2 Appendix B: Federal Requirements and Guidance

The principal criteria used for this audit included:

- Assistant Secretary for Administration Office of Security and Strategic Information, HSPD-12 Implementation Policy for the Use of the Personal Identity Verification Card for Strong Authentication (January 13, 2017)
- DHS Binding Operational Directive 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems, (April 29, 2019)
- FY 2023 IG FISMA Metrics Evaluation Guide
- FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
- 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)
- HHS Information Security Program, Standard for Encryption of Computing Devices and Information (December 14, 2016)
- HHS Policy for the High Value Asset Program (August 2019)
- HHS Policy for Information Systems Security and Privacy Protection (November 2021)
- HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (May 2020)
- HHS Policy for Privacy Impact Assessments (June 4, 2019)
- HHS System Inventory Management Standard (December 27, 2018)
- Minimum Security Configuration Standards Guidance (October 5, 2017)
- HHS Plan of Action and Milestones Standard Version 2 (June 2019)
- 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)
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
- OMB M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (December 6, 2021)
- US-CERT Federal Incident Notification Guidelines

Appendix C
FY 2023 Inspector General FISMA Reporting Metrics

4.3 Appendix C: FY 2023 Inspector General FISMA Reporting Metrics

Appendix C contains a system-generated report exported from the CyberScope FISMA Reporting Application. CyberScope is maintained by DHS and OMB. The HHS OIG entered its FY 2023 FISMA audit results and narrative comments into the CyberScope system. The report begins on the following page.

For Official Use Only

Inspector General
Section Report

2023

Department of Health and Human Services

Function 0: Overall

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Not Effective

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

To assess and determine the effectiveness of HHS's information security program, we executed an audit plan in order to assist with the determination of the maturity levels of the questions listed in the FISMA reporting metrics. Our audit included five functional areas: Identify, Protect, Detect, Respond, and Recover. The five functional areas spanned nine domains, which align to the function areas as follows: Identify covers domains risk management and supply chain risk management (SCRM). Protect covers domains configuration management, identity and access management, data protection and privacy, and security training. Detect covers domains information security continuous monitoring. Respond covers domain incident response and Recover contains domain contingency planning. In addition to the HHS Office of the Chief Information Officer, the following five HHS Operating Divisions (OpDivs) were in-scope for this assessment: Centers for Medicare and Medicaid Services, Food and Drug Administration, Office of the Inspector General, Substance Abuse and Mental Health Service Administration, and the Office of the Secretary. Through this evaluation, we determined that for FY23 HHS's information security program was Not Effective. HHS has received the assessment of Not Effective for the seventh consecutive year since the introduction of the current maturity model methodology in 2016. Four OpDivs rated between Consistently Implemented and Ad-Hoc with minimal advancement in maturity and no defined strategic plan to improve the OpDiv's maturity level. One OpDiv reached an "effective" Managed and Measurable level for the FY23 assessment. HHS's lack of progress in one significant area–Recovery–which has been assessed as Defined for the fifth consecutive years since 2019, is hindering its ability to achieve an overall assessment rating of effective. For the Recovery function, HHS had issues related to maintaining a current business impact analysis and consistently testing their established contingency plan at the system level. Additionally, issues were identified within the SCRM domain. These issues contributed to the Identify function being assessed at Ineffective with a rating Consistently Implemented. Many of the OpDivs reviewed, had processes for SCRM in the beginning stages with no clear implementations' strategy identified. While the Department has made strides in developing policies and processes for addressing the associated SCRM metrics, failures at the OCIO and OpDivs to have a consistently implemented program throughout limits full implementation.

Function 1A: Identify - Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. Three OpDivs were rated at Consistently Implemented, one OpDiv was rated as Defined, and one OpDiv was rated as Ad-Hoc. Three of the five OpDivs maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections. Two OpDivs rated as Defined and Ad-Hoc are still undergoing discovery of current systems and do not have a comprehensive system inventory at either the OpDiv or Department level. Variances still occur between Department held system listings and those produced at the OpDiv level.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is Managed and Measurable, two OpDivs are Consistently Implemented for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting. Two OpDivs are still defining appropriate procedures and processes for maintaining a hardware listing. One OpDiv rated as Managed and Measurable has provided evidence that mobile devices are denied access if they are non-compliant or unregistered.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. Two OpDivs are rated as Ad-Hoc, one OpDiv is rated Defined, one OpDiv is rated Consistently Implemented, and one OpDiv is rated as Managed and Measurable for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting. For two OpDivs rated Ad-Hoc, processes are still being developed to define procedures which allow for accurate tracking of software inventory. One OpDiv rated as Defined, the software inventory does not include data elements regarding the software details as required by organizational policies and procedures.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?

5 To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is at Optimized, one at Managed and Measurable, two OpDivs are Defined and one OpDiv is Ad-Hoc. Two OpDivs have effectively implemented a process for performing system risk assessments according to organizational defined time frame and have implemented the appropriate security controls to mitigate risks identified are implemented on a consistent basis. Three of the five OpDivs failed to maintain their risk assessments. In addition, one OpDiv failed to define and communicate their policies, procedures, and processes regarding cybersecurity risks.

6 To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?

7 To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level with two OpDivs rated at a Managed and Measurable level, one OpDiv rated at a Consistently Implemented level, one OpDiv at a Defined level and one at an Ad-Hoc level. Three OpDivs did not allocate resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively implement cybersecurity risk management activities and integrate those activities with enterprise risk management processes, as appropriate.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level with one OpDiv at a Managed and Measurable level, two OpDivs at Consistently Implemented, one Opdiv at Defined and one OpDiv at the Ad-Hoc level. For one OpDiv reviewed, management consistently utilized POA&Ms to effectively mitigate security weakness. Management is in the process of setting up procedures to utilize a prioritized and consistent approach to POA&Ms that considers items such as, but not limited to, security categorization, specific control deficiencies, and POA&M attributes captured in M-04-14.

9 To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level with two OpDivs rated at a Managed and Measurable level, two OpDivs rated at the Consistently Implemented level and one OpDiv rated at the Ad-Hoc level. One OpDiv did not consistently utilize a cybersecurity risk register, or other comparable mechanism to ensure that information about risks are communicated in a timely and effective manner to appropriate internal and external stakeholders with a need-to-know.

10 To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs are Managed and Measurable, one OpDiv is Consistently Implemented, one OpDiv is Defined, and one OpDiv is Ad-Hoc. Three OpDivs consistently implemented an automated solution across the enterprise that provides a centralized, enterprise wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. One OpDiv did not have the capability to provide a centralized, enterprise wide view of cybersecurity risks for management reporting.

11.1 Please provide the assessed maturity level for the agency's Identify - Risk Management program.

Consistently Implemented (Level 3)

11.2 Provide any additional information on the effectiveness (positive or negative) of the organizations risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

No further comment(s) to add.

Function 1B: Identify - Supply Chain Risk Management

12 To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. One OpDiv rated at Consistently Implemented, two OpDivs are at Defined and two OpDivs are rated at the Ad-Hoc level. Four OpDivs did not consistently implement a SCRM strategy across the organization and utilize the strategy to guide supply chain analyses, communication with internal and external partners and stakeholders, and in building consensus regarding the appropriate resources for SCRM.

13 To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. One OpDiv rated at Consistently Implemented, two OpDivs are at Defined and two OpDivs are rated at the Ad-Hoc level. Four OpDivs did not consistently implement a SCRM strategy across the organization and utilize the strategy to guide supply chain analyses, communication with internal and external partners and stakeholders, and in building consensus regarding the appropriate resources for SCRM.

14 To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. Two OpDivs are at a Defined maturity level, two OpDivs are rated at Ad-Hoc, and one is rated at Consistently Implemented. Four of five OpDivs did not ensure that policies, procedures, and processes were consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component.

15 To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?

16.1 Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.

Defined (Level 2)

16.2 Please provide the assessed maturity level for the agency's Identify Function.

Consistently Implemented (Level 3)

16.3 Provide any additional information on the effectiveness (positive or negative) of the organizations supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

No further comment(s) to add.

Function 2A: Protect - Configuration Management

17 To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

18 To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractoroperated systems?

19 To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Defined maturity level. One OpDiv is rated at a Managed and Measurable level, one OpDiv is rated Consistently Implemented, two OpDivs are rated Defined and on OpDiv is rated Ad-Hoc. Three OpDivs did not consistently record, implement, and maintain baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.

20 To what extent does the organization use configuration settings/common secure configurations for its information systems?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. One OpDiv is at Managed and Measurable, one OpDivs is rated as Consistently Implemented, two OpDivs are rated as Defined and one OpDiv is at Ad-Hoc. Two OpDivs consistently implement, assess, and maintain secure configuration settings for its information systems. Two OpDivs did not maintain sufficient secure configuration settings.

21 To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP- assets?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs reached a Consistently Implemented maturity level, one OpDiv is Defined and one OpDiv was evaluated at Ad-Hoc. Two OpDivs did not consistently record, implement, and maintain baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures. Two of the five OpDivs failed to provide evidence of vulnerability resolution or showed that they did not resolve critical vulnerabilities in a timely manner.

22 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented level, one OpDiv rated at the Managed and Measurable level, two OpDivs are rated at a Consistently Implemented level, one OpDiv is at a Defined level and one OpDiv is rated at the Ad-Hoc level. HHS has communicated appropriate TIC 3.0 guidance to OpDivs and four of five OpDivs were either considering TIC 3.0 use cases or had already considered use cases to meet mission need.

23 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, asappropriate?

24 To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet- accessible federal systems?

Managed and Measurable (Level 4)

Comments : Managed and Measurable (Level 4). Overall, HHS is at a Managed and Measurable level. Two OpDivs rated Managed and Measurable and three OpDivs rated Consistently Implemented related to VDP processes. HHS has established a public facing VDP program which contains relevant OpDivs and sites. HHS monitors VDP submissions and utilizes data received to assess and make changes as needed to their program as a whole.

25.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

Consistently Implemented (Level 3)

25.2 Provide any additional information on the effectiveness (positive or negative) of the organizations configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

No further comment(s) to add.

Function 2B: Protect - Identity and Access Management

26 To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv rated at the Optimized level, one OpDiv is at Managed and Measurable, and three OpDivs are Defined. Three OpDivs did not allocate resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively implement identity, credential and access management activities. Three OpDivs did not ensure that there was consistent coordination among organization leaders and mission owners to implement, manage, and maintain the organization's ICAM policy and strategy.

27 To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Defined maturity level. One OpDiv is Managed and Measurable, two OpDivs are Consistently Implemented, and two OpDivs are Defined. Two OpDivs did not consistently implement their ICAM policy, strategy, process, and technology solution road map.

28

To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?

29 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non- privileged users) that access its systems are completed and maintained?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. One OpDiv is rated at Consistently Implemented, and four OpDivs were Defined. Four OpDivs did not define or consistently ensure that access agreements for individuals are completed prior to assigning access.

30 To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for non- privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs rated as Consistently Implemented has implemented strong authentication mechanisms for non- privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets. Three OpDivs rated as Defined did not ensure that all non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and facilities.

31 To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented level. Two OpDivs are Managed and Measurable. Three OpDivs are Defined since they did not ensure that all privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and facilities.

32 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. Four of five OpDivs did not ensure that their processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization.

33 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote accesssessions?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is at a Optimized level, one OpDiv is at a Consistently Implemented level and three OpDivs are Defined. Three OpDivs did not ensure that FIPS 140-2 validated cryptographic modules were implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.

34.1 Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.

Consistently Implemented (Level 3)

34.2 Provide any additional information on the effectiveness (positive or negative) of the organizations identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

No further comment(s) to add.

Function 2C: Protect - Data Protection and Privacy

35 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv was assessed at an Ad Hoc level while another OpDiv was assessed at a Managed and Measurable level. Three OpDivs (two assessed at Defined and one assessed at Ad Hoc) failed to consistently implement their privacy program and regularly conduct privacy impact assessments as determined through privacy threshold analyses performed on the systems.

36 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?
 Encryption of data at rest
 Encryption of data in transit
 Limitation of transfer to removable media
 Sanitization of digital media prior to disposal or reuse

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. One OpDiv is Managed and Measurable, one OpDiv is Consistently Implemented, Two OpDivs are rated as Defined and one OpDiv is Ad-Hoc. For two OpDivs, the policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.

37 To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs reviewed for this metric consistently conduct exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses and were rated as Consistently Implemented. However, for two of these OpDivs, they did not analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. One OpDiv has not defined its policies and procedures related to data exfiltration, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering. This resulted in an assessment of one OpDiv as Optimized, two at Consistently Implemented, one as defined and one at Ad Hoc.

38 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?

39 To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?(Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of and E- Government Act of 20consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and userequirements)

40.1 Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Consistently Implemented (Level 3)

40.2 Provide any additional information on the effectiveness (positive or negative) of the organizations data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

No further comment(s) to add.

Function 2D: Protect - Security Training

41 To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?Note: This includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant securityresponsibilities.

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv has yet to define their security training program and policies and as such were assessed at an Ad Hoc level. Furthermore, two OpDivs were assessed at a defined level as they failed to show that their defined roles are being performed consistently in the area of their security training program. Two OpDivs demonstrated that they are holding individuals responsible and assigning resources in a risk-based manner in order to consistently implement their security training policy and as such have been assessed at a Managed and Measurable or Optimized level.

42 To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is Optimized, two OpDivs are Consistently Implemented, one OpDiv defined and one Ad-Hoc. Three of five Opdivs have assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and identified its skill gaps.

43 To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment?Note: The strategy/plan should include the following components:
 The structure of the awareness and training program
 Priorities
 Funding
 The goals of the program
 Target audiences
 Types of courses/ material for each audience
 Use of technologies (such as email advisories, intranet updates/wiki pages/social media, web- based training, phishing simulation tools)
 Frequency of training
 Deployment methods

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented level. One of the OpDivs have yet to define their security awareness strategy and assessed at the Ad Hoc level. Two OpDivs has yet to consistently implement their defined plan. Another OpDiv has been assessed at a Managed and Measurable level. Further, one OpDiv was assessed at an Optimized level as they demonstrated that their training activities were integrated across other domains.

44

To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?

45 To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization`s security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?

46.1 Please provide the assessed maturity level for the agency's Protect - Security Training program.

Consistently Implemented (Level 3)

46.2 Please provide the assessed maturity level for the agency's Protect Function.

Consistently Implemented (Level 3)

46.3 Provide any additional information on the effectiveness (positive or negative) of the organizations security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

No further comment(s) to add.

Function 3: Detect - ISCM

47 To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. For the two OpDivs rated as Managed and Measurable, a centralized tool is used to obtain qualitative and quantitative performance measures on the effectiveness of its ISCM to include activities performed across the organization in support of continuous monitoring. Additionally, the OpDivs has transitioned to ongoing control and system authorization in accordance with continuous monitoring policies. Two OpDivs rated as Defined did not consistently implement ISCM policies and strategies at the organization, business process, and information system levels. One OpDiv has not yet determined the policies and procedures which define their ISCM program.

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented level, two OpDivs rated at the Managed and Measurable level, one OpDiv is at the Consistently Implemented level, one OpDiv is at a Defined level and one OpDiv is rated at the Ad-Hoc level. HHS has defined and performs the roles as defined in the area of Information Security Continuous Monitoring. However, two OpDivs are lacking either definitions or consistent implementation while others strive to allocate resources in a risk-based manner to create and effective strategy that holds stakeholders accountable.

49 How mature are the organization`s processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. For the two OpDivs rated as Managed and Measurable, a centralized tool is used to obtain qualitative and quantitative performance measures on the effectiveness of its ISCM to include activities performed across the organization in support of continuous monitoring. Additionally, the OpDivs have transitioned to ongoing control and system authorization in accordance with continuous monitoring policies. Two OpDivs rated as Defined did not consistently implement ISCM policies and strategies at the organization, business process, and information system levels. One OpDiv has not yet determined the policies and procedures which define their ISCM program.

50 How mature is the organization`s process for collecting and analyzing ISCM performance measures and reporting findings?

51.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

Consistently Implemented (Level 3)

51.2 Provide any additional information on the effectiveness (positive or negative) of the organizations ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

No further comment(s) to add.

Function 4: Respond - Incident Response

52 To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

54 How mature are the organization`s processes for incident detection and analysis?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is rated as Managed and Measurable, two are rated as Consistently Implemented, one rated at Defined and the last at Ad-Hoc. While one OpDiv was rated as Managed and Measurable, three of five OpDivs utilized profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. HHS is still working on improving their Incident Response program in order to bring other OpDivs to a Managed and Measurable level.

55 How mature are the organization`s processes for incident handling?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented maturity level. One OpDiv was Optimized, one Managed and measurable, two OpDivs were Consistently Implemented and one Ad-Hoc. Two OpDivs managed and measured the impact of successful incidents and could quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability. Two OpDivs did not manage and measure the impact of successful incidents but still reached a Consistently Implemented level. One OpDiv is continuing to identify areas of improvement for their program and define policies and procedures for incident detection and handling.

56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?

57 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented level, as three OpDivs are assessed at a Managed and Measurable level while two OpDivs are assessed at a Consistently Implemented level. One OpDiv was assessed at an Ad Hoc level for failing to define how they collaborate with other parties to provide surge support or review their Einstein implementation or participation.

58 To what extent does the organization use the following technology to support its incident response program?
 Web application protections, such as web application firewalls
 Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
 Aggregation and analysis, such as security information and event management (SIEM) products
 Malware detection, such as antivirus and antispam software technologies
 Information management, such as data loss prevention
 File integrity and endpoint and serversecurity tools

Managed and Measurable (Level 4)

Comments : Managed and Measurable (Level 4). Overall, at HHS is at a Consistently Implemented level. One OpDiv was assessed at an Optimized level and another at a Mananged and Measurable level where they showed that their programs evaluate the effectiveness of their programs and make adjustments based on those evaluations. Two OpDivs, consistently implement their incident response plan. One OpDiv, has yet to implement their incident response plan and were assessed at Defined.

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Consistently Implemented (Level 3)

59.2 Provide any additional information on the effectiveness (positive or negative) of the organizations incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

No further comment(s) to add.

Function 5: Recover - Contingency Planning

60 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?

Consistently Implemented (Level 3)

Comments : Consistently Implemented (Level 3). Overall, HHS is at a Consistently Implemented level. One OpDiv has yet to define their roles and responsibilities with regards to contingency planning. Two OpDivs are assessed at a Defined level as they have not shown to perform the roles and responsibilities of their contingency planning strategy consistently. While one OpDiv is consistently implemented, another assessed at Optimized and incorporates simulated events into its contingency planning efforts.

61 To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. Four OpDivs did not consistently incorporate the results of organizational and system level BIAs into strategy and plan development efforts. One OpDiv successfully ensured that BIA's were completed timely and incorporated into an organizational strategy.

62 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?

63 To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined maturity level. One OpDiv is at the Consistently Implemented level. Four OpDivs did not consistently implement information system contingency plan testing and exercises and were rated Defined. One OpDiv rated as Consistently Implemented, information system contingency plan testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP. This OpDiv adequately determines if weaknesses are incorporated into the contingency plan process updates.

64 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?

65 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teamsand used to make risk- based decisions?

Defined (Level 2)

Comments : Defined (Level 2). Overall, HHS is at a Defined level. One OpDiv assessed at a Managed and Measurable level and has demonstrated that data supporting their contingency planning metrics are obtained accurately, consistently, and in a reproducible format. Three OpDivs have defined how their planning and recovery activities are communicated to stakeholders but have yet to consistently implement those activities. One OpDiv has yet to define how these efforts are communicated and has been assessed at an Ad Hoc level.

66.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Defined (Level 2)

66.2 Provide any additional information on the effectiveness (positive or negative) of the organizations contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

No further comment(s) to add.

APPENDIX A: Maturity Model Scoring

A.1 Please provide the assessed maturity level for the agency's Overall status.

Function	Core	FY23 Supplemental	FY24 Supplemental	FY23 Assessed Maturity	FY23 Effectivness	Explanation
Identify	2.50	2.60	N/A	Consistently Implemented (Level 3)	Not Effective	We have assessed the Identify function at the Consistently Implemented level. Issues were identified within the SCRM domain. Many of the OpDivs reviewed had processes for SCRM in the beginning stages with no clear implementations' strategy identified. While the Department has made strides in developing policies and processes for addressing the associated SCRM metrics, failures at the OCIO and OpDivs to have a consistently implemented program throughout, limits full implementation.

Protect	2.63	3.00	N/A	Consistently Implemented (Level 3)	Not Effective	We have assessed the Protect function at the Consistently Implemented level. Each domain of this function area was assessed at Consistently Implemented. We noted multiple findings, often with regards to vulnerability resolution and user access, across the domains of the function area that lead to the program being Ineffective for this area.
Detect	3.00	3.00	N/A	Consistently Implemented (Level 3)	Not Effective	We have assessed the Detect function at the Consistently Implemented level. Ratings for this domain were split between Consistently Implemented and Defined. The team noted multiple findings that often appear during the authorization, tracking, and assessment processes that prevent this domain from being able to be assessed at an Effective level.

Respond	3.00	3.50	N/A	Consistently Implemented (Level 3)	Not Effective	We have assessed the Respond function at the Consistently Implemented level. HHS has made strides to improve their incident response functions as a Department overall, but many smaller OpDivs lack the implementations found at more mature OpDivs. These pockets of failings prevent HHS from being assessed at an Effective level.
Recover	2.00	2.50	N/A	Defined (Level 2)	Not Effective	We have assessed the Recover function at the Defined level. HHS had issues related to maintaining a current business impact analysis and consistently testing their established contingency plans at the system level.

Overall	**Consistently**	**We have assessed the Overall Maturity at the Consistently Implemented level. We determined that for FY23 HHS's information security program was Not Effective. HHS has received the assessment of Not Effective for the seventh consecutive year since the introduction of the current maturity model methodology in 2016. Four OpDivs rated between Consistently Implemented and Ad-Hoc with minimal advancement in maturity and no defined strategic plan to improve the OpDiv's maturity level. One OpDiv reached an "effective" Managed and Measurable level for the FY23 assessment. In addition, one significant area preventing HHS from achieving an assessment of Effective is the Recovery functional area which was assessed as Defined for the fifth consecutive year since**

Maturity	**2.63**	**2.92**	**N/A**	**Implemented (Level 3)**	**Not Effective**	**2019. For the Recovery function, HHS had issues related to maintaining a current business impact analysis and consistently testing their established contingency plan at the system level. Additionally, issues were identified within the SCRM domain. These issues contributed to the Identify function being assessed at Ineffective with a rating Consistently Implemented. Many of the OpDivs reviewed had processes for SCRM in the beginning stages with no clear implementations' strategy identified. While the Department has made strides in developing policies and processes for addressing the associated SCRM metrics, failures at the OCIO and OpDivs to have a consistently implemented program throughout limits full implementation.**

Function 1A: Identify - Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	0
Consistently Implemented (Level 3)	3	3
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.60**	**3.00**

Function 1B: Identify - Supply Chain Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	2
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.00**

Function 2A: Protect - Configuration Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	0
Consistently Implemented (Level 3)	1	2
Managed and Measurable (Level 4)	0	1
Optimized (Level 5)	0	0
Calculated Rating:	**2.50**	**3.33**

Function 2B: Protect - Identity and Access Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	1
Consistently Implemented (Level 3)	2	3
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.67**	**2.75**

Function 2C: Protect - Data Protection and Privacy

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	0
Consistently Implemented (Level 3)	1	1
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.50**	**3.00**

Function 2D: Protect - Security Training

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	1	2
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**3.00**	**3.00**

Function 3: Detect - ISCM

Maturity Level	Core	Supplemental

Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	2	1
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**3.00**	**3.00**

Function 4: Respond - Incident Response

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	2	1
Managed and Measurable (Level 4)	0	1
Optimized (Level 5)	0	0
Calculated Rating:	**3.00**	**3.50**

Function 5: Recover - Contingency Planning

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0

Defined (Level 2)	2	1
Consistently Implemented (Level 3)	0	1
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.50**

Appendix D
HHS Comments

4.4 Appendix D: HHS Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

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

DATE: April 19, 2024

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

FROM: Jennifer Wendel, Chief Information Officer (Acting) Jennifer Wendel
Jennifer Wendel (Apr 22, 2024 13:25 EDT)

SUBJECT: Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023 (A-18-23-11200)

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) 2023. 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, La Monte Yarborough at Lamonte.Yarborough@hhs.gov or 202-774-2446.

Attachment A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023 (A-18-23-11200)***

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

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 2023*** **(A-18- 23-11200)**

Enterprise-wide Recommendations

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

1. Refine their enterprise architecture system inventory and software/hardware asset inventories to ensure the inclusion of the information systems and components active on the HHS network. HHS should utilize these inventories to monitor assets continuously and identify and remediate vulnerabilities timely to better manage the risks to these assets.

   HHS Response: Non-Concur

   Due to HHS' federated environment, delegation of authority to the HHS Operating Division (OpDiv) CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control PM-5 System Inventory and its enhancements, the HHS System Inventory Management Standard, and the HHS Policy for IT System Inventory Management, the OpDivs are responsible for ensuring that their information systems are reported to the HHS Security Data Warehouse (HSDW).

   HHS has Continuous Diagnostic and Mitigation (CDM) tools deployed across the enterprise to accomplish Software Asset Management (SWAM), Hardware Asset Management (HWAM), Vulnerability Management (VUL) and Configuration System Management (CSM). The tools used to accomplish this are Big Fix, ForeScout and Tenable. The information is automatically reported up to Splunk. Each OpDiv also has their own instance of Splunk.

   The sensors collect the data, aggregate the information, and report it through the CDM Elastic Dashboard. The assets are continuously monitored on a near real time basis. The data reported from the sensors is required to be updated every 72 hours.

   Additionally, OpDivs are responsible for maintaining their software and hardware asset inventories to ensure the inclusion of the information systems and components active on the HHS network. HHS non-concurs with this recommendation as it is a duplicate of recommendations issued to the OpDivs under Findings and Recommendations on page 5 of this document.

2. Require OpDivs to implement a cybersecurity risk management strategy to assess and respond to identified risks within the agency, watch for new risks, and

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 2023*** **(A-18- 23-11200)**

monitor risks and confirm implementation. The strategy should define a process to accept and monitor risks that cannot be adequately mitigated.

HHS Response: Non-Concur

After careful consideration, we must respectfully non-concur with this recommendation. HHS has a robust Cybersecurity Risk Management Strategy (CRMS) in place, developed in collaboration with OpDivs, which they can leverage and tailor to meet division needs and respond to identified risks effectively.

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

Therefore, we believe that no further action is required specifically for this recommendation, as the framework provided by our current CRMS adequately addresses the audit recommendation.

3. Confirm that all organization-wide and system-level risk assessments have been completed in an accurate and timely manner and include data points such as the threat vectors, likelihood, and tolerance level. This will help with the ability to address risks at the organization consistently and promptly.

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to HHS OpDiv CIOs, the HHS CRMS and associated policies such as the HHS IS2P and its associated control overlays help guide OpDiv processes and procedures to establish and manage an effective risk management program. HHS will work with the OpDivs to reiterate the importance of maintaining system-level risk assessments to include data points such as the threat vectors, likelihood, and tolerance level.

The HHS CRMS also links cybersecurity operations and assets to the overarching department mission, functions, and goals and incorporates cybersecurity risks into division-level Enterprise Risk Management (ERM) efforts which allows the HHS to manage risks and impacts of potential security breaches, compromises, and attacks.

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 2023*** **(A-18- 23-11200)**

HHS consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information system.

4. Require OpDivs to implement an effective SCRM program that meets the defined standards across HHS and confirm implementation is consistent with established standard. HHS should ensure that all OpDivs are appropriately assessing vendors and submitting data points to assist with tracking and monitoring components on the network.

HHS Response: Non-Concur

HHS non-concurs with this recommendation as it is a duplicate of the recommendation issued to the OpDivs under Identify - Supply Chain Risk Management domain area on page 6 of this document.

Due to HHS' federated environment, Delegation of Authority to HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically controls PM-30 Supply Chain Risk Management, the SR Supply Chain Risk Management controls and their enhancements; the Enterprise Supply Chain Risk Management Policy (E- SCRM); and the HHS Cyber Supply Chain Risk Management Program Policy (C-SCRM), the OpDivs are responsible for ensuring their SCRM policies and procedures are being consistently implemented as defined by policy and NIST standards.

5. Require OpDivs to assess and inventory privileged user accounts across the agency by an established due date and confirm completion. HHS should confirm that OpDivs policies are defined to require privileged user account monitoring in both logging and activity reviews, preferably at an automated level.

HHS Response: Non-Concur

Due to HHS' federated environment, Delegation of Authority to HHS OpDiv CIOs, and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically IA Controls and Control AC-6(7) Review of User Privilege, the OpDivs are responsible for ensuring that privileged users' logical access contains approved authentication mechanisms and privileged user activities are periodically logged and reviewed as required per OpDivs' defined frequency.

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 2023*** **(A-18- 23-11200)**

6. Require OpDivs to implement Contingency Plan testing and to perform Contingency Plan testing within the timeframe required by HHS policy.

HHS Response: Non-Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs, and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control, CP-4 Contingency Plan Testing, OpDivs are responsible for testing the contingency plan on at least an annual basis. HHS OCIO provides oversight regarding this as we perform monthly reconciliation activities with the OpDivs including providing awareness for expired or soon to expire Contingency Plan Testing dates. HHS has also implemented a Contingency Planning Oversight Program to ensure that plans are developed and tested in accordance with federal requirements.

Additionally, this is a repeat of a similar recommendation from the FY22 OIG FISMA Audit Final Report, recommendation number: 23-A-18-069.14 (Ensure that all OpDivs implement its policies and procedures to perform periodic BIAs and contingency plan testing within the timeframe required by HHS policy).

Department and OpDiv Findings and Recommendations

Identify - Risk Management

OIG Recommendations

Based on our findings at the OpDivs, we recommend that the HHS OCIO work with the OpDivs to:

1. Conduct an annual review of the System Security & Privacy Plan and annually perform risk assessments for all operational systems, according to organizational policy.

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs, and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls, PL-2 System

Security and Privacy Plans, and RA-3 risk assessment, the OpDivs are responsible for annually reviewing their System Security & Privacy Plan performing risk assessments for all operational systems.

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 2023*** **(A-18- 23-11200)**

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

2. Appropriately track software license information and maintain an accessible, up-to-date inventory for all its software licenses.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control PM-5 System Inventory and its enhancements, the HHS System Inventory Management Standard, and the HHS Policy for IT System Inventory Management, the OpDivs are responsible for completing discovery of all information systems and maintaining an up-to-date inventory of systems, software, and licenses.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

3. Perform the SAR and ATO in accordance with the organization's policy.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control CA-2 Control Assessments, the OpDivs are responsible for ensuring that SCAs and ATOs are conducted within the appropriate timeframe as defined by policy for all systems.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

4. Utilize automated solutions to provide a portfolio view of cybersecurity risk at the organization is consistently implemented in accordance with NIST standards.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control

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 2023*** **(A-18- 23-11200)**

Catalog, specifically controls RA-5 Vulnerability Monitoring and Scanning, and CA-7 Continuous Monitoring, the OpDivs are responsible for utilizing technology/automation to monitor and scan for vulnerabilities in the system and hosted applications.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

Identify - Supply Chain Risk Management

OIG Recommendations

Based on our findings at the OpDivs, we recommend that the HHS OCIO:

1. Confirm OpDivs define and implement an OpDiv level supply chain risk management strategy based on HHS departmental policy and NIST standards.

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically controls PM-30 Supply Chain Risk Management, the SR Supply Chain Risk Management controls and their enhancements, the Enterprise Supply Chain Risk Management Policy (E- SCRM) and the HHS Cyber Supply Chain Risk Management Program Policy (C-SCRM), the OpDivs are responsible for ensuring their SCRM policies and procedures are being consistently implemented as defined by policy and NIST standards.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

Protect – Configuration Management

OIG Recommendations

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

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 2023*** **(A-18- 23-11200)**

1. Ensure that OpDivs' vulnerabilities are tracked and remediated in a timely manner and create POA&Ms for any vulnerabilities in accordance with the organization's policy.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control SI-2 Flaw Remediation and its enhancements, the HHS Policy for Vulnerability Management, and the HHS Plan of Action and Milestones Standard, the OpDivs are responsible for ensuring that vulnerabilities are tracked and remediated in a timely manner and POA&Ms created for any vulnerabilities in accordance with the organization's policy.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

2. Ensure that all OpDivs' baseline configurations are documented and tracked for each system in the OpDiv.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically controls CM-2 Baseline configuration, CM-3 Configuration Change Control, and their enhancements, and the Minimum-Security Configuration Standards Guidance, the OpDivs
   are responsible for ensuring that baseline configurations are documented and tracked for each system.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

3. Ensure that all OpDivs' TIC 3.0 program use cases are reviewed for relevance and capabilities that are new to the latest revision of the TIC guidance are consistently implemented in accordance with HHS Policy for the Implementation of TIC and OMB M-19-26.

   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 2023*** **(A-18- 23-11200)**

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically control AC-17(3) Managed Access Control Points and the HHS Policy for the Implementation of Trusted Internet Connections (TIC), the OpDivs are responsible for identifying acceptable network access control points (e.g., connections standardized through the Trusted Internet Connection (TIC) initiative); and that the TIC guidance are consistently implemented in accordance with HHS Policy for the Implementation of TIC and OMB M-19-26.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

Protect - Identity and Access Management

OIG Recommendations

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

1. Ensure that all OpDivs acquire the resources to fully implement MFA or an alternative strong authentication and implement multi-factor authentication or an alternative strong authentication for both privileged and non-privileged users on all operational systems.

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control IA-2 Identification And Authentication (Organizational Users) and its enhancements, the E- Authentication Guidance and the E-Authentication RA Template, the OpDivs are responsible for ensuring that all operational systems have multifactor or an alternative strong authentication mechanism for both privileged and non- privileged users.

Additionally, HHS has given high priority to Multi-Factor Authentication (MFA) and Encryption requirements. The HHS OCIO collects additional data on a quarterly basis from OpDivs not 100% compliant. This data will help OpDivs to establish a baseline for their compliance with the MFA and Encryption metrics. Further, the data will provide quarterly status updates on their implementation of MFA and Encryption on non-compliant systems.

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 2023*** **(A-18- 23-11200)**

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

2. Ensure that all OpDivs provision, manage, and review privileged user accounts for operational systems.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, the AC controls specifically controls AC-6 Least Privilege, AU-6 Audit Record Review, Analysis, and Reporting and their enhancements, the OpDivs are responsible for provisioning, managing, and reviewing privileged user accounts for operational systems.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

3. Ensure that all OpDivs are properly implementing remote session timeouts of 30 minutes (or less) for operating systems.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically controls SI-4 System Monitoring, AC-17 Remote Access, and its enhancements, the OpDivs are responsible for ensuring that systems are properly implementing remote session timeouts of 30 minutes (or less) for operating systems HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) and systems in scope to ensure remediation of this recommendation.

4. Ensure that all OpDivs consistently implement access policies and procedures in accordance with the organization's Risk Management Safeguards policy across the organization.

   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 2023*** **(A-18- 23-11200)**

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically controls AC-1 Access Control Policy and Procedures and PS-6 Access Agreements, the OpDivs are responsible for implementing access policies and procedures in accordance with the organization's Risk Management Safeguards policy across the organization.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

Protect - Data Protection and Privacy

OIG Recommendations

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

1. Ensure that all OpDivs' operational systems have an approved and up-to-date PIA in accordance with the HHS Policy of Privacy Impact Assessment.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control RA-8 Privacy Impact Assessments (PIAs), and the HHS Policy for Privacy Impact Assessments, the OpDivs are responsible for ensuring timely completion of PIAs.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) and systems in scope to ensure remediation of this recommendation.

2. Ensure that all OpDivs implement data encryption methods to protect data determined to be PII or sensitive by the systems and enhanced network defenses in accordance with NIST standards.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls SC-8 Transmission Confidentiality and Integrity

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 2023*** **(A-18- 23-11200)**

and SC-28 Protection of Information at Rest and its enhancements, and the HHS Policy for Encryption of Computing Devices and Information, the OpDivs are responsible for ensuring data encryption methods to protect data determined to be PII or sensitive by the systems and enhanced network defenses in accordance with NIST standards.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

Protect - Security Training

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

1. Require and confirm that all OpDivs have a process in place to evaluate their workforce gaps. Furthermore, confirm that all OpDivs are implementing a compliant security training strategy as defined by overarching HHS policy.

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control AT-3 Role-based Training and its enhancements, and the HHS Requirements for Role-Based Training of Personnel with Significant Security Responsibilities Memorandum (2017), the OpDivs are responsible for ensuring that processes are in place to evaluate their workforce gaps and that all personnel complete role-based training in a timely manner.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

Detect - Information Security Continuous Monitoring

OIG Recommendations

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO:

1. Ensure that all OpDivs are inheriting and consistently implementing policies and procedures defined by HHS department level policy.

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 2023*** **(A-18- 23-11200)**

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, the OpDivs are responsible for inheriting and consistently implementing policies and procedures defined by HHS department level policy.

HHS OCIO has received a copy of the OpDiv OARS and will reiterate the departmental level policy to the OpDiv(s) in scope.

Respond - Incident Response

OIG Recommendations

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO continuously monitor to ensure that all OpDivs:

1. Inherit and consistently implement policies or procedures to govern their incident response strategy.

   HHS Response: Concur

   Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls IR-4 Incident Handling, IR-5 Incident Monitoring, and IR-6 Incident Reporting, the OpDivs are responsible for Inheriting and implementing policies or procedures to govern their incident response strategy.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

2. Define common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents in accordance with NIST standards, USCERT Federal Incident Notification Guidelines and OMB guidance across the organization.

   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 2023*** **(A-18- 23-11200)**

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically control IR-4 Incident Handling and its enhancements, and the Policy for Information Technology (IT): Security and Privacy Incident Reporting and Response (2019), the OpDivs are responsible for defining common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents in accordance with NIST standards, USCERT Federal Incident Notification Guidelines and OMB guidance across the organization.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

Recovery - Contingency Planning

OIG Recommendations

Based on our findings at the OpDivs reviewed, we recommend that the HHS OCIO work with the OpDivs to:

1. Require and confirm that all OpDivs' operational systems have a complete and up-to-date BIA.

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control CP-2 Contingency Plan and its enhancements, the OpDivs are responsible for ensuring that operational systems have a complete and up-to-date BIA.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

2. Require and confirm that all OpDivs' operational systems conduct Contingency Plan testing and exercises as required by their risk rating. Any testing and exercises conducted should be followed with after-action reports as necessary.

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 2023*** **(A-18- 23-11200)**

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls CP-2 Contingency Plan, CP-4 Contingency Plan Testing, and their enhancements, the OpDivs are responsible for ensuring that operational systems conduct Contingency Plan testing and exercises as required by their risk rating; and testing and exercises conducted followed with after-action reports as necessary.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.

3. Confirm that all OpDivs' policies and procedures covering Contingency Plan testing are in accordance with policy requirements by Departmental policy, NIST standards, and OMB guidance.

HHS Response: Concur

Due to HHS' federated environment, Delegation of Authority to the HHS OpDiv CIOs and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog specifically controls CP-1 Contingency Planning Policy and Procedures and its enhancements, the OpDivs are responsible for ensuring that policies and procedures covering Contingency Plan testing are in accordance with policy requirements by Departmental policy, NIST standards, and OMB guidance.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope to ensure remediation of this recommendation.