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 2022

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

May 2023
A-18-22-11200

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 2022 Federal Information Security Modernization Act (FISMA) Report

March 31, 2023

Building a better working world

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 2022 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 September 30, 2022, with the objective of assessing HHS' compliance with FISMA as defined in the FY 2022 Inspector General 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. 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 FISMA reporting metrics for the Inspector General. The specific scope and methodology are defined in Appendix A of this report.

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 as a result of 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 and is not intended to be and should not be used by anyone other than these specified parties.

Ernst + Young LLP

March 31, 2023

Report in Brief
Date: March 31, 2023
Report No. A-18-22-11200

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 2022

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 September 30, 2022, 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 4 of the 12 operating divisions (OpDivs); 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 not meeting the 'Managed and Measurable' maturity level for the Core Inspector General metrics in the function areas of Identify, Protect, Detect, Respond, and Recover. Overall, HHS remains in a similar position to their previously evaluated maturity level. The Department is aware of opportunities to strengthen their overall information security program. HHS has continued to implement changes that support progress towards improved maturity of their enterprise-wide cybersecurity program across all FISMA domains. HHS continues to define and update policies that are distributed to OpDivs to assist with their own policy definitions or to guide consistent implementation of a compliant cybersecurity strategy. We have identified a number of areas that would strengthen the Department's overall information security program.

What We Recommend and HHS Comments

We made recommendations to the Office of the Chief Information Officer that should further strengthen HHS's cybersecurity program and enhance information security controls at HHS. Recommendations specific to deficiencies found at the reviewed HHS OpDivs 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 cybersecurity program from its current maturity state to Managed and Measurable or to the maturity level that HHS deems as effective for their environment, in agreement with the OIG. HHS' information security program should address gaps between the current maturity levels to the appropriate effective maturity level for each function area. HHS should ensure that policies and procedures are being consistently implemented as defined across all OpDivs in order to meet the requirements for effective maturity. This oversight should extend to all requirements whether they are to be implemented using centralized, federated, or hybrid controls.

In written comments to our report, HHS concurred with our Department, Op-Div, and enterprise 1 and 2 recommendations; while not concurring with enterprise recommendations 3 and 4. For the two non-concurrence responses, both were associated with the separation of responsibilities between the HHS OCIO and the OpDivs. While we recognize the federated nature of the HHS environment, responsibility for OCIO to provide oversight of the OpDivs still exists which is why we recommended that OCIO work with the OpDivs to confirm appropriate controls are in place. We maintain that our recommendations are still 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 September 30, 2022, based upon the questions outlined in the FISMA reporting metrics for the Inspectors General (IG).

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 (CIGIE), Federal Civilian Executive Branch Chief Information Security Officers and their staff, and the Intelligence Community (IC) developed the FY 2022 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 2022 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 2022 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 2022, 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 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. HHS received an overall program assessment of not effective in FY21, therefore in addition to the 20 Core Metrics our methodology included an assessment of non-core metrics. While the results of our review of non-Core metrics and follow-up on prior year issues were not factored into the determination of the effectiveness of the Department’s information security program on the maturity model spectrum, relevant findings and recommendations within IG FISMA domains are included in Section III.

The FY 2022 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 2022 IG FISMA Metrics, a series of metrics (or questions) was 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.

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 cybersecurity 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 cybersecurity 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' cybersecurity program for each of the FISMA domains are based on the FISMA reporting metrics.

Based on the results of our performance audit of the twenty (20) Core Metrics, we determined that HHS' cybersecurity program was "Not Effective". This determination was made 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 2022 IG FISMA Maturity results. In FY 2022, the maturity levels for all domains remained the same as FY 2021. Areas where HHS' security program needed improvement are captured by our enterprise-wide recommendations and specific findings in Section 3.

Table 2: 2022 HHS Maturity Levels

Function	**Domain**	**OIG Assessed Domain Maturity**	**OIG Assessed Function Maturity**	**FY 2022 vs FY2021 IG Assessment**
Identify	***Risk Management***	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	No Change
	Supply Chain Risk Management	Defined (Level 2)		No Change
Protect	***Configuration Management***	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	No Change
	Identity & Access Management	Consistently Implemented (Level 3)		No Change
	Data Protection & Privacy	Consistently Implemented (Level 3)		No Change
	Security Training	Consistently Implemented (Level 3)		No Change
Detect	***Information Security Continuous Monitoring***	Defined (Level 2)	Defined (Level 2)	No Change
Respond	***Incident Response***	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	No Change
Recover	***Contingency Planning***	Defined (Level 2)	Defined (Level 2)	No Change

Progress in some function areas has not been achieved due to a lack of implementation of automated tools across all OpDivs, limiting the overall effectiveness of the cybersecurity program and requiring HHS to maintain legacy tools and processes. The automated tools should assist HHS in delivering continuous monitoring of its networks and systems along with providing real-time reporting of OpDiv status and progress. Effective implementation would help improve federal cybersecurity response capabilities and allow for proper prioritization of issues based on established risk criteria.

HHS has continued to progress in department-wide implementation of its Continuous Diagnostics and Mitigation (CDM) program. Use of CDM tools provide visibility into assets and awareness of vulnerabilities where it has been implemented. Ultimately, HHS should aim to dedicate efforts to fully implement the CDM program as required to achieve real-time reporting with continuous monitoring of all OpDiv networks and systems. This will enable HHS to identify and accurately prioritize issues based on established risk reporting metrics, as well as improve cybersecurity response capabilities.

As HHS continued their rollout of the prescribed CDM packages and begun efforts to define key performance indicators and benchmarks as part of its Information Security Continuous Monitoring (ISCM) strategy, they have not fully implemented the packages and tools across all OpDivs. This approach once implemented could support further HHS's goal of supporting the OpDivs in the improvement of their ISCM maturity level.

The lack of a fully implemented CDM structure across HHS continues to impact the department's maturity level and leaves the state of ISCM inconsistent across HHS. HHS continues to be exposed to the risk of not mitigating the most significant vulnerabilities first due to an inability to prioritize risks based on potential impact. A fully implemented CDM solution should allow HHS to identify cybersecurity risks on an ongoing basis and help the organization mitigate vulnerabilities at near-real-time.

In the area of Supply-Chain Risk Management (SCRM), we noted that the OpDivs we reviewed did not consistently leverage HHS policies for SCRM. 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 exposure to supplier components that do not meet HHS's minimum-security requirements, which can lead to a lack of appropriately vetted assets, exposure, compromise, reputational harm etc.

In the area of Identity and Access Management (IAM), it was noted that there were several instances in which the system owner had not implemented multi-factor or an alternative strong authentication mechanism for privileged and non-privileged users. Without strong authentication mechanisms, HHS creates significant cybersecurity risk as passwords are more susceptible to be compromised. Additionally, within this domain it was noted that HHS had deficiencies across all of the in-scope OpDivs as they could not provide sufficient evidence that the system owners have reviewed privileged user activities on a periodic basis in accordance with policy for High Value Assets and/or critical systems. Lack of proper monitoring of privileged users increases the risk of exposure to malicious activities which may go undetected.

In the area of Contingency Planning (CP), several in-scope OpDivs did not ensure that system owners performed testing of their contingency plans within the timeframe required by the organization's policy. In the absence of a periodic testing of a contingency plan, OpDivs are at risk of not being able to maintain essential mission and business functions during a system disruption, compromise, or failure.

HHS should continue efforts on the planned risk assessment to identify the Department's optimal maturity level and obtaining a top-down view of significant risk exposures.

2.2 Enterprise-wide Recommendations

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

1. Continue to work with the OpDivs to implement automated CDM solutions to increase awareness and improve mitigation efforts across all of HHS.

2. Continue to advance the SCRM program to implement defined standards across HHS.

3. Continue to work with the OpDivs to ensure privileged users' logical access contains strong authentication mechanisms. Additionally, HHS should confirm that OpDivs are periodically performing sufficient monitoring over privileged user access.

4. Confirm that the OpDivs contingency plan testing is being performed within the timeframe required by HHS policy.

HHS OCIO COMMENTS AND OFFICE OF INSPECTOR GENERAL REPONSE

HHS OCIO concurred with recommendations 1 and 2 and did not concur with recommendations 3 and 4.

HHS stated that due to HHS's federated environment, OpDivs are responsible ensuring privileged users' access and user activities are reviewed periodically and contingency tests are performed.

While HHS is a federated environment, responsibility for OCIO to provide oversight of the OpDivs still exists which is why we recommended that OCIO work with the OpDivs to confirm appropriate controls are in place. 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. 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 C.

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 is 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 2022 IG Assessment	Change from FY 2021 IG Assessment
Identify	Risk Management	Consistently Implemented	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 Plans of Action and Milestones (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, the capability to deny mobile devices, such as smartphones and tablets, access to agency enterprise services when security and operating system updates had not been applied within a given period based on defined by agency policy or guidance, was not enforced.

- At one (1) OpDiv, there was a failure to ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels.

- At one (1) OpDiv, there was a failure to maintain an inventory of its information systems, an up-to-date inventory of software assets, and an up-to-date inventory of software licenses.

- At one (1) OpDiv, for 10 of 10 selected software licenses, they were not maintained or could not provide license information to match the software instances.

- At one (1) OpDiv, one (1) of the five (5) Security Control Assessments (SCA) reviewed was not performed within the last year as required by policy.

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

- Ensure that all OpDivs implement the capability to deny access to mobile devices, such as smartphones and tablets, from connecting to the network if the device's software is outdated.

- Ensure that all OpDivs remediate weaknesses identified during controls assessments and review/perform risk assessments within the timeframe established by HHS policy.

- Ensure that all OpDivs complete its discovery of all information systems and maintain an up- to-date inventory of systems, software, and licenses.

- Ensure that SCAs are conducted within the appropriate timeframe as defined by policy for all systems.

HHS OCIO Response:

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

Supply Chain Risk Management

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 2022 IG Assessment	Change from FY 2021 IG Assessment
Identify	Supply Chain Risk Management	Defined	No Change

Supply Chain Risk Management Findings and Recommendations

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

- At one (1) OpDiv, the inherited C-SCRM policy from HHS was not being consistently implemented and proper safeguards were not used to ensure that SCRM procedures and processes are followed for each sampled system.
- At two (2) OpDivs, SCRM policies had been drafted, however they had not been formally approved and disseminated.
- One (1) OpDiv has not defined and communicated its SCRM policies, procedures, and processes.

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

- Ensure that all OpDiv's SCRM policies and procedures are being consistently implemented across the organization and ensure their execution.
- Ensure that all OpDivs finalize and implement draft policies and procedures to include the review of suppliers or contractors for risks to the organization's systems and system components.

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 2022 IG Assessment	Change from FY 2021 IG Assessment
Protect	Configuration Management	Consistently Implemented	No Change
	Identity and Access Management	Consistently Implemented	No Change
	Data Protection and Privacy	Consistently Implemented	No Change
	Security Training	Consistently Implemented	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.

Configuration Management Findings and Recommendations

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

- At one (1) OpDiv, five (5) of 10 selected configuration vulnerabilities (including critical and high vulnerabilities) were not resolved within the required timelines or did not have a documented risk response (POA&M or Risk Acceptance).

- One (1) OpDiv has not consistently remediated configuration vulnerabilities within thirty (30) days in accordance with its policy. As of June 2022, five (5) of fifteen (15) sampled critical and high-risk vulnerabilities have not been resolved.

- One (1) OpDiv has not developed an associated Plan of Actions and Milestones (POA&M) for four (4) of the five (5) open configuration vulnerabilities.

- One (1) OpDiv, did not consistently assess, and maintain secure configuration settings for its information systems based on the principle of least functionality.

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

- Ensure that all OpDivs implement the requirement to resolve high and critical vulnerabilities within 30 and 15 days respectively and create POA&Ms to monitor and resolve the weakness in a timely manner.

- Ensure that secure configuration settings are being maintained as defined by existing policy.

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 OpDiv's identity and access management program:

- At one (1) OpDiv, for one (1) of five (5) selected systems, the system owner had not implemented multi-factor or an alternative strong authentication mechanism for privileged and non-privileged users.

- At one (1) OpDiv, for one (1) of five (5) selected systems, the system owner did not perform access review of privileged users. Additionally, one (1) of five (5) selected systems did not perform logging and monitoring of privileged activities.

- One (1) OpDiv had not consistently implemented its policies and procedures to periodically review privileged activities for unauthorized actions for three (3) of five (5) selected systems.

- One (1) OpDiv failed to implement two-factor authentication or strong authentication mechanisms for three (3) of five (5) sampled systems as required for privileged and non-privileged users. Further, in five (5) of five (5) sampled systems, the OpDiv did not provision, manage, and review privileged accounts as required by policy.

- One (1) OpDiv had not consistently implemented its policies and procedures to periodically review privileged activities in accordance with its policy. Specifically:

    - For one (1) of five (5) selected systems, the system owner had not developed and implemented an audit management program to review audited events, including logged events for privileged users.

    - For two (2) of five (5) selected systems, while the system owners provided evidence that audit events and alerts were configured, they did not provide sufficient evidence of monitoring and follow up activity (e.g., email communications, tickets, or reports) indicating that audit events were reviewed periodically.

- At two of the sampled OpDivs, for three (3) selected systems, system owners did not provide evidence to support that sampled users were assigned a risk designation to perform job responsibilities. Additionally, for one of those selected systems, there was no evidence that all users signed and renewed their access agreements, nor completion of their annual security awareness and role-based training. At another system, users were not appropriately screened prior to being granted system access or rescreened periodically. Additionally, an OpDiv did not ensure that access agreements for the sampled users were completed prior to granting users access to the system or maintained thereafter.

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

- Ensure that all operational systems have multifactor or an alternative strong authentication mechanism (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for both privileged and non-privileged users.

- Ensure that policies and procedures for identity and access management are being consistently implemented and proper safeguards (i.e., logging, monitoring, review of privileged user activity) are developed across the Department to ensure their execution.

- Ensure that all OpDivs enforce its policies and procedures established to review users' activities periodically.

- Implement oversight sufficient to ensure that all OpDivs review pre-defined privileged users' activities periodically and document the review and any follow-up activities for all systems.

- Consistently implement the requirement to assign risk designations, re-signing access agreements, and training for all systems so that OpDivs can restrict privileges for users based on risk designations.

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 personally identifiable information (PII) and personal health information (PHI) of US citizens. Many of HHS' 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 OpDiv's data protection and privacy program:

- At one (1) OpDiv, one (1) of five (5) selected systems had not implemented security controls to protect its PII and other agency data, as appropriate, throughout the data lifecycle. Specifically, the system currently does not implement data encryption methods to protect data in transit and data at rest.

- One (1) OpDiv failed to define policies and procedures for data exfiltration, enhanced network defenses, e-mail authentication, or Domain Name System (DNS) infrastructure tampering mitigation and implement data encryption at rest or in transit for five (5) of five (5) sampled systems.

- Two (2) of the OpDivs had at least one (1) of five (5) sampled systems with a Privacy Impact Assessment (PIA) that was last completed outside of the required performance cycle of every three (3) years.

- For one (1) of five (5) selected systems, the OpDiv did not ensure that individuals with responsibilities for PII completed role-based training at least annually.

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

- Ensure that data encryption methods to protect data determined to be PII or sensitive are implemented across the organization for all systems.

- Ensure that OpDivs define and implement policy for data exfiltration, enhanced network defenses, e-mail authentication, and DNS infrastructure tampering mitigation. Further, ensure the OpDiv enforces implementation of data encryption in transit and at rest in accordance with HHS policy, NIST standards, and OMB guidance.

- Ensure the timely completion of PIAs for all systems to identify privacy and compliance risk with federal regulations or laws, tracking implementation of privacy controls, identifying instances where the Agency collects or handles PII and/or PHI subject to the Privacy Act of 1974.
- Implement oversight procedures sufficient to ensure that all personnel complete role-based training in a timely manner.

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 giving enough training to its information system users. Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment and secured physical locations without providing their personnel adequate security training.

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

- Security awareness and training strategy and plan that leverages its organizational skills assessment and is adapted to the HHS culture.

While we did not identify any findings in the Security Training domain, we identified a finding regarding role-based training specific to privacy training and safeguarding PII. Please refer to the Data Protection and Privacy domain section for the role-based training finding and related recommendation.

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 Information Security Continuous Monitoring (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 (CDM) program results in an approach to fortifying the cybersecurity posture through ongoing updates to system security plans, a periodic security assessment and POA&Ms, which are the three principal documents in a security authorization package.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2022 IG Assessment	Change from FY 2021 IG Assessment
Detect	ISCM	Defined	No Change

ISCM Findings and Recommendations

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

- At one (1) OpDiv, two (2) of five (5) selected systems did not have an annual risk assessment; and fifteen (15) systems had expired ATOs with no extensions granted.

- At one (1) OpDiv, one (1) out of five (5) sampled systems did not produce a valid annual Security Assessment Report (SAR) as defined by policy and consequently did not communicate risks, POA&M status, vulnerabilities, or security assessment results with the OpDiv level officials (Risk Executive, CIO, CISO, and the Authorizing Official) as defined by their ISCM strategy.

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

- Ensure that operational systems have valid and current ATO’s and that security controls are assessed annually as per HHS policy.

- Implement oversight sufficient to ensure that ISCM policies and procedures are consistently implemented in accordance with NIST standards for all systems.

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 activities to act regarding a detected cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity event and is defined by the incident response program. The domain within this function is incident response. 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 2022 IG Assessment	Change from FY 2021 IG Assessment
Respond	Incident Response	Consistently Implemented	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.

We did not identify any findings in the Incident Response domain.

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 2022 IG Assessment	Change from FY 2021 IG Assessment
Recover	Contingency planning	Defined	No Change

Contingency Planning Findings and Recommendations

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

- At one (1) OpDiv, for two (2) of five (5) selected systems, system owners stated that contingency planning were conducted, however they were unable to provide evidence sufficient to document testing was performed within the required timeline.

- One (1) OpDiv has not consistently implemented its policies and procedures to perform contingency plan testing in accordance with the timeframe defined by policy. Specifically:

  - One (1) of five (5) selected systems, the system owner did not perform a contingency plan testing every 365 days in accordance with HHS policy

  - For sixteen (16) of sixty-eight (68) OpDiv FISMA systems, the system owners had not ensured that contingency plan tests were tested within 365 days of the previous test.

- One (1) OpDiv failed to implement sufficient contingency planning efforts as defined by policy for five (5) of five (5) sampled systems. In each of the five (5) sampled systems the OpDiv failed to perform business impact analyses (BIA); did not perform contingency plan testing within one year as required by the defined policy; and did not facilitate prioritizing the systems and processes based on the FIPS 199 impact level or develop priority recovery strategies for minimizing loss.

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

- Ensure that all OpDivs implement its policies and procedures to perform periodic BIAs and contingency plan testing within the timeframe required by HHS policy.

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' compliance with FISMA. To assess HHS' FISMA compliance, we leveraged the FISMA reporting metrics for the Inspector General. 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 2022 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
- Indian Health Services
- National Institutes of Health
- Office of the Secretary

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' security program against HHS and selected OpDiv cybersecurity program policies, other standards and guidance issued by HHS management, and reporting metrics.
- Inspected and analyzed selected artifacts including but not limited to system security plans, evidence to support testing of security controls, POA&M records, security training records, asset compliance reports, system inventory reports and account management documentation.
- Inspected internal assessments performed on behalf of HHS and OpDivs' managements that had a similar scope to the FY 2022 IG FISMA metrics. Incorporated the results as part of the FY 2022 IG FISMA metrics.

- Inspected any results from GAO and OIG audits and reports that had a similar scope to the FY 2022 IG FISMA metrics. Incorporated the results as part of the FY 2022 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 (ASA OSSI), HSPD-12 Implementation Policy for the Use of the Personal Identity Verification (PIV) Card for Strong Authentication (January 13, 2017).
- DHS Binding Operational Directive 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems, (April 29, 2019).
- Core IG FISMA Metrics Evaluation Guide (2022 Publication)
- Federal Information Security Modernization Act of 2014 (December 2014)
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (February 2004).
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006).
- HHS Cybersecurity 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 (IS2P) (November 2021).
- HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII) (May 2020).
- HHS Policy for Privacy Impact Assessments (PIA) (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 (POA&M) 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 2022 Inspector General FISMA Reporting Metrics

4.3 Appendix C: FY 2022 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 2021 FISMA audit results and narrative comments into the CyberScope system. The report begins on the following page.

Inspector General

Section Report

2022

IG Annual

Department of Health and Human Services

Function 0: Overall

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

Not Effective

Comments: 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 level of the questions listed in the FISMA reporting metrics. Our audit included five functional areas: Identify, Protect, Detect, Respond, and Recover. The five areas spanned nine domains, which were incorporated as follows: Identify covers risk management and supply chain risk management (SCRM). Protect covers configuration management, identity and access management, data protection and privacy, and security training. Detect covers information security continuous monitoring. Respond covers incident response and Recover contains contingency planning. In addition to the HHS Office of the Chief Information Officer, the following four HHS Operating Divisions (OpDivs) were in-scope for this assessment: Centers for Medicare & Medicaid Services, Indian Health Services, National Institutes of Health, and the Office of the Secretary. We also assessed results from other IT audits and assessments performed throughout the year by HHS OIG and GAO, where applicable. Through these evaluations we reached a Not Effective conclusion. Two significant areas preventing HHS from achieving an effective program are in the Detect and Recovery functional areas, which were both assessed as Defined. For the Detect function, HHS continues their FY21 strategy into FY22 of implementing a number of automated continuous monitoring tools across all OpDivs. These tools look to assist HHS in delivering continuous monitoring of its networks and systems along with providing real-time reporting of OpDiv status and progress. These implementations would help improve federal cybersecurity response capabilities and allow for proper prioritization of issues based on established risk criteria. However, some OpDivs have yet to implement automated tools limiting the overall effectiveness and requiring HHS to maintain legacy tools and processes. 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, while the Identify function was rated Consistently Implemented, there were issues identified within the SCRM domain which contributed to the ineffective program. While the Department has made strides in developing policies and processes for addressing the associated SCRM metrics, full implementation is lacking. At the OpDivs, processes for SCRM are in their beginning stages with no clear implementations strategy identified.

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.

Through the evaluation of FISMA core metrics, it was determined that the HHS' information security program was 'Not Effective.' This determination was made based on a number of factors including: (1) the evaluation

Function 0: Overall

of HHS not meeting a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover functional areas; (2) the deficiencies identified across all functional areas; (3) HHS not identifying mitigating processes associated with ratings below Managed and Measurable for each control domain that would allow HHS to have an effective program and; (4) the evaluation of a maturity level below Consistently Implemented for individual metric question both at HHS overall and at selected OpDivs. Three significant areas preventing HHS from achieving an effective program are in the ISCM, SCRM, and CP domains. For other areas evaluated as Consistently Implemented, HHS should define risk-based metrics to measure the effectiveness of their program in the domains of: Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, and Incident Response. These metrics should be based on a central risk reporting process and appropriate toolsets being deployed to provide HHS with the necessary information to make informed cybersecurity risk decisions. These steps will help HHS achieve its mission through an effective and coordinated information security program.

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? (NIST SP 800-53, Rev. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev. 2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks)

   Consistently Implemented (Level 3)

   Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs were rated at Consistently Implemented, one OpDiv was rated as Managed and Measurable, and one OpDiv was rated as Defined. Three of the four OpDivs maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections. One OpDiv rated as Defined is still undergoing discovery of current systems and does not have a comprehensive system inventory at either the OpDiv or Department 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 ? (NIST SP 800-53, Rev. 5: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework, v2; FY 2022 CIO FISMA Metrics: 1.2-1.2.3; CSF: ID.AM-1, ID.AM-5; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 1)

Function 1A: Identify - Risk Management

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is Managed and Measurable while three 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. 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 software 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 ? (NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800- 37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2)

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Two OpDivs are rated as Defined, and two OpDivs are rated as Consistently Implemented 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 one OpDiv rated as Defined, the software inventory does not include data elements regarding the software details as required by organizational policies and procedures. For the last OpDiv rated as Defined, the organization does not maintain an up to date software license inventory.

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 (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2022 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-12, P-13, S-1 - S-3)?

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? (NIST SP 800-39; NIST SP 800-53, Rev. 5: RA-3 and PM-9; NIST IR 8286; CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P2, P-3, P-14, R-2, and R-3)

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. One OpDiv is rated as Consistently Implemented, one OpDiv at Ad-Hoc, one OpDiv at Managed and Measurable, and one OpDiv at Defined. Two OpDivs had consistently 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 four 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 utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

7. To what extent have roles and responsibilities of internal and external stakeholders involved in cyber security risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NISTIR 8286, Section 3.1.1, OMB A-123;; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?

8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-19-03, CSF v1.1, ID.RA-6)?

9. To what extent does the organization ensure that information about cyber security risks is communicated in a timely manner to all necessary internal and external stakeholders (OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NISTIR 8286)?

10. To what extent does the organization utilize 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? (NIST SP 800-39; OMB A-123; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs are Consistently Implemented, one OpDiv is Defined, and one OpDiv is Managed and Measurable. Three OpDivs consistently implement 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)

Function 1A: Identify - Risk Management

11.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize supply chain risk management policies and procedures to manage SCRM activities at all organizational tiers (NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-1, NIST CSF v1.1, ID.SC-1, NIST 800-161)?

13. To what extent does the organization utilize a supply chain risk management plan(s) to ensure the integrity, security, resilience, and quality of services, system components, and systems (OMB A-130, NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-2, SR-3; NIST 800-161, section 2.2.4 and Appendix E)?

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? (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276, NIST 800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15)

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Three OpDivs are at a Defined maturity level and one OpDiv is rated at Ad-Hoc. All four 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 maintain and monitor the provenance and logistical information of the systems and system components it acquires? (NIST SP 800-53 REV. 5: SR-4 and NIST SP 800-161, Provenance (PV) family)?

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 organization’s 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?

Function 2A: Protect - Configuration Management

Function 2A: Protect - Configuration Management

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?

18. To what extent does the organization utilize 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 contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

19. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2022 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

20. To what extent does the organization utilize settings/common secure configurations for its information systems? (NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M - 22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is at Managed and Measurable, two OpDivs are rated as Consistently Implemented, and one OpDiv is rated as Defined. Three OpDivs consistently implement, assess, and maintain secure configuration settings for its information systems. One OpDiv is Defined and did not maintain secure configuration settings.

21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities? (EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02, 19-02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks)

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. One OpDiv reached a Managed and Measurable maturity level and three OpDivs were evaluated at Defined. 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. Three of the four OpDivs failed to provide evidence of vulnerability resolution or showed that they did not resolve critical vulnerabilities in a timely manner.

Function 2A: Protect - Configuration Management

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)?

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, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).

24. To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?

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 organization's 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?

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 across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?

27. To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17, Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

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 (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11, OMB M-19-17)?

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 (NIST SP 800-53 REV. 4: AC-8, PL-4, and PS-6)?

30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level

(IAL)3/Authenticator Assurance Level (AAL) 3 credential) for nonprivileged users to access the organization's facilities [organizationdefined entry/exit points], networks, and systems, including for remote access? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; OMB M19-17, NIST SP 800-157; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)

Defined (Level 2)

Comments: Overall, HHS is at a Defined 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. Two 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 strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented level. One OpDiv is Consistently Implemented. Two OpDivs are Defined since they did not ensure that all privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and facilities. One OpDiv is Managed and Measurable since they ensured that all privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems.

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? (EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; NIST SP 800-53, Rev. 5: AC-1, AC2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18 Security Controls v.8: Controls 5, 6, and 8)

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. All four OpDivs did not ensure that their processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization.

Function 2B: Protect - Identity and Access Management

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 access sessions (NIST SP 800-53 REV. 4: AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2022 CIO FISMA Metrics: 2.10 and 2.11).

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 organization's 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?

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 (NIST SP 800-122; NIST SP 800-37 (Rev. 2) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b))?

36. To what extent has the organization implemented the encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs are rated as Consistently Implemented and one OpDiv is rated as Defined. For three 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. For the one OpDiv rated as Defined, the use of encryption methods for data at rest and in transit for was not provided for all sampled systems.

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 19- 01; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10)

Defined (Level 2)

Function 2C: Protect - Data Protection and Privacy

Comments: Overall, HHS is at a Defined 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, they did not analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. However, 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.

38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)

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 organization's 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?

Function 2D: Protect - Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated 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 security responsibilities (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).

42. To what extent does the organization utilize 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? (FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS Top 18 Security Controls v.8: Control 14)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. All four OpDivs are Consistently Implemented. The OpDivs have assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and identified its skill gaps. One OpDiv periodically updates its assessment to account for a changing risk environment.

Function 2D: Protect - Security Training

43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (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, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, 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 (NIST SP 800-53 REV. 4: AT-2; FY 2022 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

45. To what extent does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2022 CIO FISMA Metrics: 2.15)?

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 organization's 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?

Function 3: Detect - ISCM

47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier? (NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13)

Consistently Implemented (Level 3)

Comments: 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

Function 3: Detect - ISCM

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.

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)

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? (OMB A-130; NIST SP 800-137: Section 2.2; NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03)

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Two OpDivs are at the Defined level. Two OpDivs are Managed and Measurable and utilize the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans. While HHS is Managed and Measurable at two OpDivs and Defined and two OpDivs, overall HHS is at a Defined maturity level. Based on testing, one OpDiv was identified as having several systems operating which were not currently authorized to be on the network. In addition, one OpDiv does not currently maintain an inventory of systems sufficient to identify if systems operating on the network are authorized. The current inventory of systems for this OpDiv is currently maintained on an ad hoc basis.

50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

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

Defined (Level 2)

Comments: We have assessed the ISCM domain as Defined. While overall ratings were split between Consistently Implemented and Defined, some OpDivs have yet to implement automated tools, limiting the overall effectiveness and requiring HHS to maintain legacy tools and processes. We also noted multiple findings associated with the ISCM domain.

51.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

Function 4: Respond - Incident Response

52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to

responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 - National Preparedness)?

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2022 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

54. How mature are the organization's processes for incident detection and analysis? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is rated as Managed and Measurable, and three are rated as Consistently Implemented. While one OpDiv was rated as Managed and Measurable, all four 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? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv 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. Three OpDivs did not manage and measure the impact of successful incidents but still reached a Consistently Implemented level.

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 (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)

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 (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41).

Function 4: Respond - Incident Response

58. To what extent does the organization utilize 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 server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

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

Consistently Implemented (Level 3)

59.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

Function 5: Recover - Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts? (FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs consistently incorporated the results of organizational and system level BIAs into strategy and plan development efforts. One OpDiv did not consistently incorporate the results of organizational and system level BIAs into strategy and plan development efforts.

62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2022 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes? (FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP10; CIS Top 18 Security Controls v.8: Control 11)

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. One OpDiv is at the Consistently Implemented level. Three 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 (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2022 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

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 teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?

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

Defined (Level 2)

Comments: Since one of the metrics is rated as Defined and the other at Consistently Implemented, we are assessing CP as Defined (lower of the 2) since HHS is not at the CI for both metrics.

66.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

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

Summary

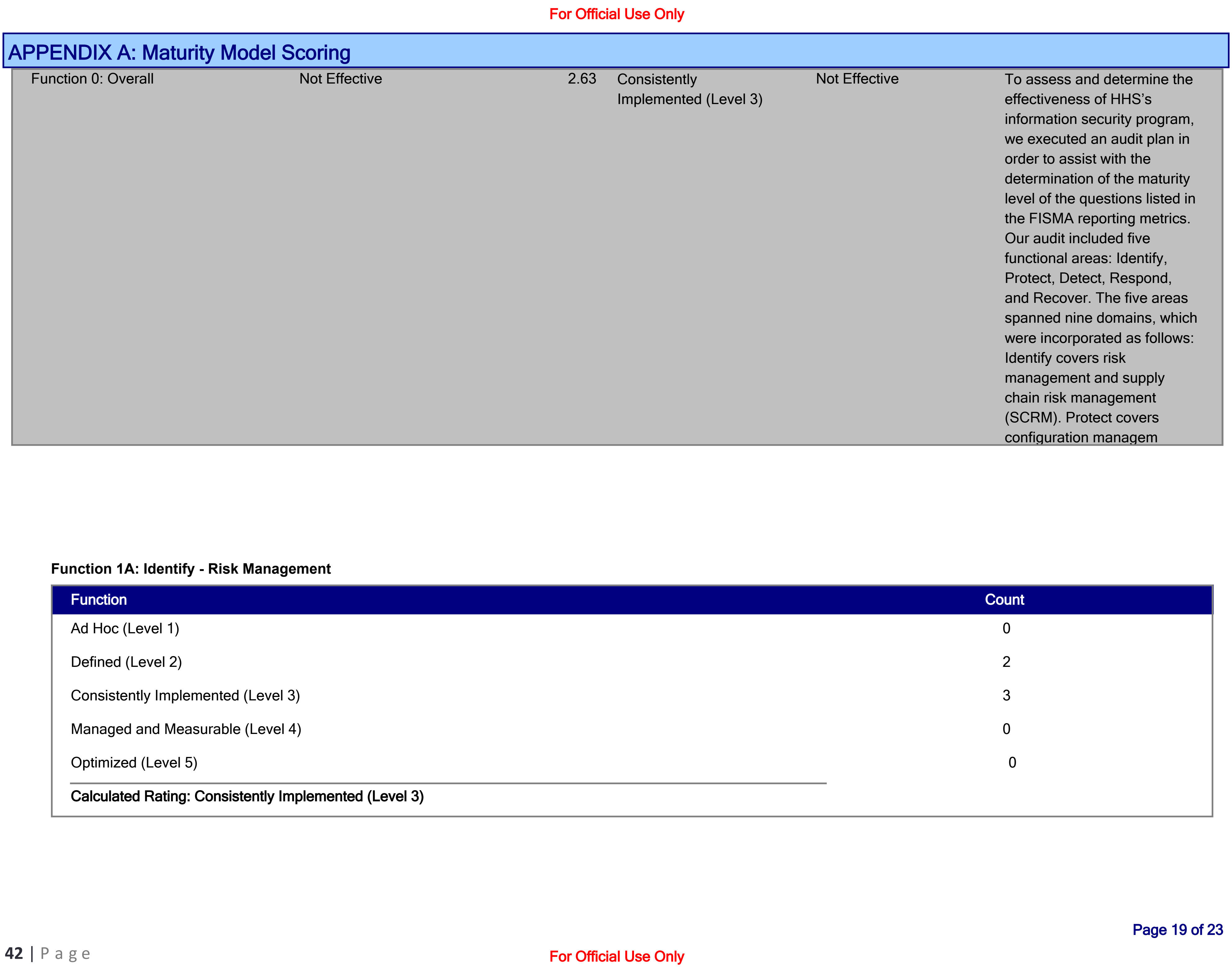
Cycle	Maturity Level	Mean	Mode
FY22 Core Metrics	Consistently Implemented (Level 3)	2.63	Consistently Implemented (Level 3)
FY22 Supplementary Metrics			
FY22 Overall	Consistently Implemented (Level 3)	2.63	Consistently Implemented (Level 3)

Overall

Function	Calculated Maturity Level	Mean	Mode	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain Risk Management	Consistently Implemented (Level 3)	2.50	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Consistently Implemented (Level 3)	2.56	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	

APPENDIX A: Maturity Model Scoring

Function 3: Detect - ISCM	Consistently Implemented (Level 3)	2.50	Consistently Implemented (Level 3)	Defined (Level 2)	We have assessed the ISCM domain as Defined. While overall ratings were split between Consistently Implemented and Defined, some OpDivs have yet to implement automated tools, limiting the overall effectiveness and requiring HHS to maintain legacy tools and processes. We also noted multiple findings associated with the ISCM domain.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	3.33	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	2.78	Consistently Implemented (Level 3)	Defined (Level 2)	Since one of the metrics is rated as Defined and the other at Consistently Implemented, we are assessing CP as Defined (lower of the 2) since HHS is not at the CI for both metrics.



APPENDIX A: Maturity Model Scoring

Function 0: Overall	Not Effective	2.63	Consistently Implemented (Level 3)	Not Effective	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 level of the questions listed in the FISMA reporting metrics. Our audit included five functional areas: Identify, Protect, Detect, Respond, and Recover. The five areas spanned nine domains, which were incorporated as follows: Identify covers risk management and supply chain risk management (SCRM). Protect covers configuration managem

Function 1A: Identify - Risk Management

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

APPENDIX A: Maturity Model Scoring

Function 1B: Identify - Supply Chain Risk Management

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

Function 2A: Protect - Configuration Management

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

Function 2B: Protect - Identity and Access Management

Function	Count
Ad Hoc (Level 1)	0
Defined (Level 2)	2
Consistently Implemented (Level 3)	1
Managed and Measurable (Level 4)	0

Optimized (Level 5)	0
Calculated Rating: Defined (Level 2)	

Function 2C: Protect - Data Protection and Privacy

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

Function 2D: Protect - Security Training

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

Function 3: Detect - ISCM

Function	Count
Ad Hoc (Level 1)	0

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

Function 4: Respond - Incident Response

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

Function 5: Recover - Contingency Planning

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

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: January 18, 2023

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

FROM: Karl S. Mathias, Ph.D., Chief Information Officer
karl mathias (Jan 23, 2023 12:45 EST)

SUBJECT: 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)

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) 2022. 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 2022 (A-18-22-11200)***

cc:
Karl Mathias, Ph.D., Chief Information Officer
La Monte Yarborough, Chief Information Security Officer
Christopher Bollerer, Deputy Chief Information Security Officer
Jeffrey Arman, Assistant Director, OIG Cybersecurity & IT Audit Division
Jarvis Rodgers, Director, OIG Cybersecurity & IT Audit Division

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022 (A-18- 22-11200)***

Enterprise-wide Recommendations

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

1. Continue to work with the OpDivs to implement automated CDM solutions to increase awareness and improve mitigation efforts across all of HHS.

   HHS Response: Concur

   HHS OCIO is reliant on the Department of Homeland Security (DHS) for the implementation of its Continuous Diagnostics and Mitigation (CDM) program. The HHS CDM program will continue its collaboration and is working with the DHS Cybersecurity and Infrastructure Security Agency (CISA) organization to implement the CDM Dashboard 2 solution based on the Elastic data analysis solution. Dashboard 2 collects operational data from sensors and solutions across HHS OpDivs that provide information about asset management, infrastructure, users and data protection etc. (see https://www.cisa.gov/cdm#:~:text=The%20CDM%20Program%20delivers%20cybersecurity) to provide an "operational" view of risk across the HHS enterprise. The Dashboard 2 solution (Elastic) is scheduled to transition to full operational capability by summer of 2023.

2. Continue to advance the SCRM program to implement defined standards across HHS.

   HHS Response: Concur

   HHS has made progress by developing an Enterprise-Supply Chain Risk Management Program (E-SCRM Program) within the Immediate Office of the Secretary, Office of National Security to implement defined standards and ensure consistent processes across HHS. One of the first accomplishments of this program was to finalize the HHS Supply Chain Risk Management Program Policy. This policy includes OpDiv roles and responsibilities which includes designating a primary SCRM POC to focus on SCRM for their OpDiv and interface with the E-SCRM Program. The E-SCRM Program also worked with the HHS Enterprise Risk Management Council to add SCRM as a Departmental risk focus. Additionally, the E-SCRM Program is also developing a Strategic Framework and Implementation Plan to ensure defined standards and processes across the Department. Another goal of this program is to continue increasing SCRM assessments across HHS. Finally, HHS also has a Cyber Supply Chain Risk Management Policy for the OpDivs to adhere to.

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 2022 (A-18- 22-11200)***

3. Continue to work with the OpDivs to ensure privileged users' logical access contains strong authentication mechanisms. Additionally, HHS should confirm that OpDivs are periodically performing sufficient monitoring over privileged user access.

   HHS Response: Non-Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO, 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.

4. Confirm that the OpDivs contingency plan testing is being performed within the timeframe required by HHS policy.

   HHS Response: Non-Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO, 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.

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 2022 (A-18- 22-11200)***

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. Ensure that all OpDivs implement the capability to deny access to mobile devices, such as smartphones and tablets, from connecting to the network if the device's software is outdated.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically control, CM-8 System Component Inventory and its enhancements, and the HHS Policy for Mobile Devices and Removable Media, the OpDivs are responsible for implementing the capability to deny access to mobile devices, such as smartphones and tablets, from connecting to the network if the device's software is outdated.

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

2. Ensure that all OpDivs remediate weaknesses identified during controls assessments and review/perform risk assessments within the timeframe established by HHS policy.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Standard for Plan of Action and Milestones (POA&M) Management and Reporting, HHS Policy for Vulnerability Management, and the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls RA-3 Risk Assessment and SI-2 Flaw Remediation and their enhancements, the OpDivs are responsible for remediating weaknesses identified during controls assessments and performing risk assessments within the timeframe established by HHS 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.

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022 (A-18- 22-11200)***

3. Ensure that all OpDivs complete its discovery of all information systems and maintain an up- to-date inventory of systems, software, and licenses.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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.

4. Ensure that SCAs are conducted within the appropriate timeframe as defined by policy for all systems.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control RA-3 Risk Assessment and its enhancements, the OpDivs are responsible for ensuring that SCAs 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.

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022 (A-18- 22-11200)***

Identify - Supply Chain Risk Management

OIG Recommendations

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

1. Ensure that all OpDiv's SCRM policies and procedures are being consistently implemented across the organization and ensure their execution.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically controls SA-1 Policy and Procedures and 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.

   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 finalize and implement draft policies and procedures to include the review of suppliers or contractors for risks to the organization's systems and system components.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control, PM-30 Supply Chain Risk Management Strategy and its enhancements, and control SR-6 Supplier Assessments and Reviews, and its enhancement, the HHS Policy for Cyber Supply Chain Risk Management, the HHS Enterprise Supply Chain Risk Management Policy, and the HHS Policy for Information Technology Procurements - Security And Privacy Language, the OpDivs are responsible for finalizing and implementing draft policies and procedures that includes the review of suppliers or contractors for risks to the organization's systems and system components.

   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.

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022 (A-18- 22-11200)***

Protect – Configuration Management

OIG Recommendations

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

1. Ensure that all OpDivs implement the requirement to resolve high and critical vulnerabilities within 30 days and create POA&Ms to monitor and resolve the weakness in a timely manner.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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 high and critical vulnerabilities are resolved within 30 days and 15 days respectively of discovery and POA&Ms are created to monitor and resolve weaknesses 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.

2. Ensure that secure configuration settings are being maintained as defined by existing policy.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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, RA-3 Risk Assessment, and SR-1 Policy and Procedures, and their enhancements, and the Minimum- Security Configuration Standards Guidance, the OpDivs are responsible for ensuring that configuration settings are being maintained as defined by 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.

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 2022 (A-18- 22-11200)***

Protect - Identity and Access Management

OIG Recommendations

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

1. Ensure that all operational systems have multifactor or an alternative strong authentication mechanism (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for both privileged and non-privileged users.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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, and the HSPD-12 Implementation Policy for the Use of the Personal Identity Verification (PIV) Card for Strong Authentication, 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.

   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.

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 2022 (A-18- 22-11200)***

2. Ensure that policies and procedures for identity and access management are being consistently implemented and proper safeguards (i.e., logging, monitoring, review of privileged user activity) are developed across the Department to ensure their execution.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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, and the IA controls and their enhancements, the OpDivs are responsible for ensuring that policies and procedures for identity and access management are being consistently implemented and proper safeguards (i.e., logging, monitoring, review of privileged user activity) are developed across the Department to ensure their execution.

   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 enforce its policies and procedures established to review users' activities periodically.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P), and Control Catalog, specifically controls AC-2 Account Management, AC-6 Least Privilege, and their enhancements, the OpDivs are responsible for enforcing policies and procedures established to review users' activities periodically.

   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.

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 2022 (A-18- 22-11200)***

4. Implement oversight sufficient to ensure that all OpDivs review pre-defined privileged users' activities periodically and document the review and any follow-up activities for all systems.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control AC-6 Least Privilege and its enhancements, the OpDivs are responsible for reviewing pre-defined privileged users' activities periodically and document the review and any follow-up activities 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.

5. Consistently implement the requirement to assign risk designations, re-signing access agreements, and training for all systems so that OpDivs can restrict privileges for users based on risk designations.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls PS-2 Position Risk Designation, PS-3 Personnel Screening, and PS-6 Access Agreements, the OpDivs are responsible for consistently implementing the requirement to assign risk designations, re-signing access agreements, and training for all systems so they can restrict privileges for users based on risk designations.

   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.

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022 (A-18- 22-11200)***

Protect - Data Protection and Privacy

OIG Recommendations

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

1. Ensure that data encryption methods to protect data determined to be PII or sensitive are implemented across the organization for all systems.

   HHS Response: Concur

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

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022 (A-18- 22-11200)***

2. Ensure that OpDivs define and implement policy for data exfiltration, enhanced network defenses, e-mail authentication, and DNS infrastructure tampering mitigation. Further, ensure the OpDiv enforces implementation of data encryption in transit and at rest in accordance with HHS policy, NIST standards, and OMB guidance.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest, SI-3 Malicious Code Protection and its enhancements, the HHS Policy for Encryption of Computing Devices and Information, HHS Policy for Domain Name System (DNS) and Domain Name System Security Extensions (DNSSEC) Services, and the HHS Policy for Internet and Email Security, the OpDivs are responsible for implementing policy for data exfiltration, enhanced network defenses, e-mail authentication, DNS infrastructure tampering mitigation, and data encryption in transit and at rest.

   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 the timely completion of PIAs for all systems to identify privacy and compliance risk with federal regulations or laws, tracking implementation of privacy controls, identifying instances where the Agency collects or handles PII and/or PHI subject to the Privacy Act of 1974.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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) in scope to ensure remediation of this recommendation.

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 2022 (A-18- 22-11200)***

4. Implement oversight procedures sufficient to ensure that all personnel complete role-based training in a timely manner.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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 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 work with the OpDivs to:

1. Ensure that operational systems have valid and current Authorization to Operate (ATO) and that security controls are assessed annually as per HHS policy.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls CA-2 Control Assessments and CA-6 Security Authorizations, the OpDivs are responsible for having valid and current ATO's and that security controls are assessed at the frequency per HHS policy and Control Catalog.

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

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 2022 (A-18- 22-11200)***

2. Implement oversight sufficient to ensure that Information Security Continuous Monitoring (ISCM) policies and procedures are consistently implemented in accordance with NIST standards for all systems.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control CA-7 Continuous Monitoring and its enhancements, and the HHS Information Security Continuous Monitoring Strategy, the OpDivs are responsible for ensuring that ISCM policies and procedures are consistently implemented in accordance with NIST standards 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.

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. Ensure that all OpDivs implement its policies and procedures to perform periodic BIAs and contingency plan testing within the timeframe required by HHS policy.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO 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 performing BIAs and contingency plan testing within the timeframe required by HHS 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.