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 2021

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

April 2022
A-18-21-11200

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The 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. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These audits help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Department of Health and Human Services

FY 2021 Federal Information Security Modernization Act Report

April 6, 2022

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 2021 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, 2021, with the objective of assessing HHS' compliance with FISMA as defined in the FY 2021 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

April 6, 2022

Report in Brief
Date: April 2022
Report No. A-18-21-11200

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

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, 2021, 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 5 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; and inspected selected artifacts.

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021

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 Identify, Protect, Detect, Respond, and Recover function areas as required by DHS guidance and the FY 2021 Inspector General FISMA Reporting Metrics. However, HHS continues to implement changes to strengthen the maturity of its enterprise-wide cybersecurity program. Progress continues to be made to sustain cybersecurity maturity across all FISMA domains. HHS is aware of opportunities to strengthen the Department's overall information security program which would help ensure that all OpDivs are consistently implementing and in line with the requirements across their security programs. We identified opportunities where HHS can strengthen its 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 also commit to implementing the results of the pilot HHS-wide risk assessment into a formal Cybersecurity Maturity Migration 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 deemed effective maturity level for each function area. Roles and shared responsibilities should be articulated and implemented to meet the requirements for effective maturity, including whether requirements are to be implemented using centralized, federated, or hybrid controls.

After issuing our draft report and based on feedback and discussion with HHS prior to HHS providing written comments, we consolidated 3 of our enterprise-wide recommendations into 1 recommendation for an enterprise-wide risk assessment over known control weaknesses in this final report. In written comments to our draft report, HHS concurred with all of our recommendations and described actions it has taken or plans to take to address them. HHS also provided technical comments, which we addressed as appropriate.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/A182111200.asp.

Table of Contents

Section 1
Background

1 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, 2021, 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, DHS and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2021 IG FISMA reporting metrics, issued May 12, 2021, in consultation with the Federal Chief Information Officers Council and other stakeholders. These metrics leverage the *National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity* and are aligned with the five function areas: Identify, Protect, Detect, Respond, and Recover. 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 2021 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 2021 metrics also mark a continuation of the work that OMB, DHS, and CIGIE undertook in FY 2016 to transition the IG assessments to a maturity model approach.

For FY 2021, updates were made to the IG FISMA questions, as reported in the FY 2021 IG FISMA Reporting Metrics, which include:

- A new domain on Supply Chain Risk Management (SCRM) within the Identify function was established in FY 2021. This new domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the agency's cybersecurity and supply chain risk management requirements. As noted in the Federal Acquisition Supply Chain Security Act of 2018, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks. The new domain references SCRM criteria in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. To provide agencies with sufficient time to fully implement NIST 800-53, Rev 5., in accordance with OMB A-130, these new metrics were not considered for the purposes of the Identify framework function rating.

- Reorganizing and rewording specific metric questions within the Identify function to focus on the degree to which cyber risk management processes are integrated with enterprise risk management (ERM) processes. As an example, IGs are directed to evaluate how cybersecurity risk registers are used to communicate information at the information system, mission/business process, and organizational levels. These changes are consistent with NIST Interagency Report 8286, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," which provides guidance to help organizations improve the cybersecurity risk information they provide as inputs to their enterprise ERM programs.

- A new question (#24) to measure the extent to which agencies utilize a vulnerability disclosure policy as part of their vulnerability management program for internet-accessible federal systems was included. OMB has issued guidance on improving vulnerability identification, management, and remediation. Specifically, Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*, dated September 2, 2020, provides guidance to federal agencies on collaborating with members of the public to find and report vulnerabilities on federal information systems. In addition, DHS Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, dated September 2, 2020, provides guidance on the development and publishing of an agency's vulnerability disclosure policy and supporting handling procedures.

The FY 2021 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 (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Reporting Metrics

For the FY 2021 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 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.

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

2 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 in Appendix C.

Based on the results of our performance audit, we determined that HHS' cybersecurity program was "Not Effective", as it did not meet the required rating level for five of the five function areas: Identify, Protect, Detect, Respond and Recover. This determination was made based on HHS not meeting the 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, or Recover function areas.

Table 2 below provides a comparison from the FY 2020 and FY 2021 IG FISMA Metrics. In FY 2021, the HHS security program strengthened the maturity of its controls for several individual IG FISMA metrics. Areas where HHS' security program needed improvement are captured by our specific findings and enterprise-wide recommendations in Section 3.

Table 2: FY 2020 and 2021 HHS Maturity Levels

Maturity Level	FY 2020 IG FISMA Metrics	FY 2021 IG FISMA Metrics
Ad-Hoc	0	1
Defined	17	17
Consistently Implemented	42	35
Managed and Measurable	0	4

Note: The IG FISMA metrics are the aggregation of the assessment results for HHS and the OpDivs reviewed. The number of IG metrics may change from year to year.

Progress in some IG FISMA metric areas has not been achieved due to a lack of full implementation of ISCM efforts across the OpDivs. These efforts are critical to provide HHS CIO and OpDiv CIOs reliable data and metrics for multiple IG FISMA domains to make informed risk management decisions.

The partial implementation of the HHS FY21 Continuous Diagnostics and Mitigation (CDM) strategy provided visibility into some assets, awareness into some vulnerabilities and certain threat information through the use of RSA Archer and Splunk. HHS continues to work towards implementing a full Department-wide CDM program in collaboration with DHS with the ultimate goals of 1.) Continuous monitoring of HHS networks and systems, 2.) Real-time reporting of OpDivs status and progress to help address and implement strategies to combat risk, 3.) Prioritization of issues based on established risk criteria, and 4.) Improving federal cybersecurity response capabilities. HHS has created an enterprise-level ISCM strategy for OpDivs to assist with the implementation of CDM tools. However, HHS has not defined roadmaps, key performance indicators, or benchmarks for CDM implementation within this strategy or other documentation. The OCIO recognizes limitations associated with the CDM tool roll-out and has established that their main goal is to support the OpDivs in their implementation of the CDM tools that are prescribed by DHS. The Department has implemented their CDM tool across multiple OpDivs during FY 2021 with the goal of continued roll-out across the enterprise. In addition, HHS has established a monthly ISCM/CDM Working Group, where lessons learned inform implementation and improvements to its ISCM program.

While HHS has made strides in the implementation of their CDM tools/processes, there is no definitive schedule to fully implement the CDM program across all OpDivs. This has led to inconsistent ISCM across OpDivs and a lower maturity at the HHS enterprise. Without a fully implemented CDM program, HHS may not be able to identify cybersecurity risks on an ongoing basis, use CDM information to prioritize the risks based on potential impacts, and then mitigate the most significant vulnerabilities first.

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 implementation of an automated CDM solution that provides a centralized, enterprise-wide view of risks across all of HHS.

2. Update the ISCM strategy to include a more specific roadmap; including target dates, for ISCM deployment across the HHS enterprise.

3. HHS should perform an enterprise risk assessment over known control weaknesses (e.g., Authority to Operate, incomplete OpDiv provided system inventories, lack of OpDiv adherence to HHS information security policies) due to their federated environment and document an appropriate risk response (e.g., accept, avoid, mitigate, share, or transfer).

4. Develop a process to monitor information system contingency plans to ensure they are developed, maintained, and integrated with other continuity requirements by information systems.

HHS OCIO COMMENTS

HHS OCIO concurred with our recommendations.

Section 3
Department and OpDiv Findings and Recommendations

3 Section 3: Department and OpDiv Findings and Recommendations

3.1 Summary

This section consolidates the findings identified at each of the selected OpDivs reviewed against the Cybersecurity Framework five function areas. We identified several findings in HHS' security program and consolidated them into each of the nine domains. We also include recommendations that should assist the Department as they focus on achieving a higher maturity level.

Function	Domain	OIG Assessed Maturity	FY 2021 IG Assessment vs FY 2020 IG Assessment
Identify	***Risk Management***	Consistently Implemented (Level 3)	No Change
	Supply Chain Risk Management	Defined (Level 2)	New for FY 2021
Protect	***Configuration Management***	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)	Decrease
Respond	***Incident Response***	Consistently Implemented (Level 3)	No Change
Recover	***Contingency Planning***	Defined (Level 2)	No Change

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, for evaluation within the IG metrics. However, Supply Chain Risk Management was only assessed at the domain level and not factored into the conclusion of the function or overall effectiveness of HHS information security program for FY 2021 in accordance with the IG FISMA Reporting Metrics guidance. Risk Management is not yet at a maturity level of Managed and Measurable, 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 2021 IG Assessment	Change from FY 2020 IG Assessment
Identify	Risk Management	Consistently Implemented	No Change

HHS' risk management function has the following in place:

- Process for maintaining a comprehensive and accurate inventory of its information systems and system interconnections *(metric 1)*
- Standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the network with detailed information necessary for tracking and reporting *(metric 2)*
- 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 *(metric 3)*
- Information system security risks are adequately managed at the organizational, mission/business process, and information system levels (*metric 5*).
- Information security architecture provides a disciplined and structured methodology for managing risk *(metric 6).*
- Roles and responsibilities of internal and external stakeholders involved in risk management processes has been defined and communicated across the organization *(metric 7)*.

- Established a risk management framework for evaluating and reporting risks to internal and external stakeholders *(metric 9)*.

- Implemented 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 *(metric 10)*.

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 the 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, a system security plan (SSP), with an associated Federal Information Systems Processing Standards (FIPS) 199 categorizations, was not completed.

- At one (1) OpDiv, Security Assessment Reports (SARs) and the POA&Ms were not completed for four (4) of the sampled systems.

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

- Ensure that all operational systems have SSPs and FIPS 199 categorizations completed for information systems in accordance with HHS policy.

- Ensure that all OpDivs are completing security controls system assessments and POA&Ms at least quarterly or more frequently as defined by the OpDiv.

HHS OCIO Response:

HHS OCIO concurred with our recommendations.

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 2021 IG Assessment	Change from FY 2020 IG Assessment
Identify	Supply Chain Risk Management	Defined	Not evaluated in FY 2020.

HHS' SCRM function has the following in place:

- Established a SCRM strategy to manage supply risk associated with the system development life cycle and associated services *(metric 12)*.
- Defined SCRM policies to manage SCRM activities at all organization levels *(metric 13)*.
- Defined standards to ensure products, systems, and services of external providers are consistent with HHS cybersecurity and supply chain requirements *(metric 14).*
- Defined procedures for detecting and preventing counterfeit components from entering its information systems *(metric 15)*.

For FY 2021, there were no findings or recommendations for the SCRM domain. Also, SCRM was not considered in determining the overall effectiveness of the HHS information security program. However, during discussions with the HHS OCIO and OpDivs, it was noted that HHS is aware of SCRM developments, and they continue to make progress associated with SCRM as required in NIST 800-53, Revision 5.

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 2021 IG Assessment	Change from FY 2020 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.

HHS' configuration management domain has the following in place:

- Established configuration management roles and responsibilities to be implemented by OpDiv management *(metric 17)*.
- Defined baseline requirements and guidance for configuration management plans to be implemented by OpDiv management *(metric 18)*.
- Defined guidelines for the appropriate security configuration settings of information systems *(metric 20)*.
- Based on the complexity of the systems and associated architectures, each OpDiv and system owner can make risk-based decisions when implementing HHS requirements. When monitoring configuration management compliance and flaw remediations, OpDiv programs range from manual to automated *(metric 21)*.
- Established a Trusted Internet Connection program to assist in protecting its network and for implementation by the OpDivs *(metric 22)*.
- Defined requirements for OpDivs to utilize a vulnerability disclosure policy as part of its vulnerability management program *(metric 24)*.

HHS has made progress to come into compliance with the DHS Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy* (VDP), which was issued in September 2020. HHS has developed easy to use publicly facing reporting tools as well as publicly facing VDP requirements.

Configuration Management Findings and Recommendations

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

- At one (1) OpDiv, two (2) out of five (5) selected systems did not have evidence to validate that configuration baselines had been implemented per their Change Management Plan.
- At one (1) OpDiv, two (2) out of five (5) selected systems had no evidence provided for change management testing. We were informed that no significant changes were made to the systems during the audit period, however, no evidence was provided to validate that no changes occurred.
- At one (1) OpDiv, OpDiv specific configuration management policies and procedures, which are required by the *HHS Information Security and Privacy Policy,* were not documented.
- One (1) OpDiv was not tracking configuration changes made to their systems.

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

- Ensure that baseline configuration requirements are implemented and maintained across all systems within its environment. Additionally, ensure that system owners implement procedures to document and retain evidence of current baseline configurations.
- Ensure that all systems implement processes to track system changes throughout the change management process, to include testing, validation, and documentation. Additionally, procedures should be implemented to retain evidence of all changes.
- Develop a management approved Configuration Management policy that addresses purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities. This document should be tailored to the OpDivs' needs and be reviewed and updated according to HHS policy (at least every 3 years).

HHS OCIO Response:

HHS OCIO concurred with our recommendations.

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.

HHS' identity and access management domain had the following in place:

- A defined Identity, Credential and Access Management (ICAM) program with established roles and responsibilities *(metric 26)*.

- A defined ICAM policy, process, strategy, and technology solution that guide ICAM processes and activities *(metric 27)*.
- Appropriate configuration/connection requirements for remote access connections (*metric 33*)

Identity and Access Management Findings and Recommendations

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

- For a subset of selected users at one (1) OpDiv, we identified the following:
  - Nine (9) users had no evidence provided for assigning a position risk designation and the performance of appropriate personnel screening prior to granting access.
  - Eleven (11) users had no evidence provided for the completion of non-disclosure agreements.
  - Seven (7) users had no evidence provided for the completion of acceptable use agreements and signed Rules of Behaviors.
- At one (1) OpDiv, strong authentication mechanisms (PIV or an Identity Assurance Level 3/Authenticator Assurance Level) 3 credential) for non-privileged users to access the system was not implemented for two (2) of the four (4) sampled systems.
- Based on the selected subset of users at one (1) OpDiv, it was noted that annual access reviews were not performed for six (6) privileged users.
- At one (1) OpDiv, periodic access reviews were not provided for six (6) privileged users.

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

- Update and implement its personnel security policies to clearly articulate the personnel screening process along with the required access agreements that need to be completed prior to being granted system access. In addition, OpDivs should update and implement their procedures for retrieving and archiving user access agreements for internal control purposes.
- Develop and implement an ICAM strategy and authenticator management policy to ensure all information systems undergo a digital identity risk assessment to determine which systems require strong authentication. Once a risk assessment is complete, OpDivs should ensure that authentication mechanisms are implemented for all information systems.

- Establish a process for the review of privileged users on an annual basis to ensure compliance with HHS Policy. In addition, OpDivs should ensure that this process is created to identify:
    - User access is still needed.
    - User rights subscribe to the principle of least privileged.
    - User actions are captured and monitored appropriately as dictated by HHS policy.
- Implement a process to ensure that privileged user's access is reviewed at least within every 365 days by all system owners in compliance with *HHS Information System Security and Privacy Policy* (IS2P). Evidence of privileged users access reviews should be retained and provided upon request.

HHS OCIO Response:

HHS OCIO concurred with our recommendations.

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.

HHS' data protection and privacy domain had the following in place:

- HHS has a defined privacy program including a defined plan and guidelines, which have been communicated to the OpDivs *(metric 35)*.
- Defined security control guidance for protecting PII and agency sensitive data throughout the data lifecycle to be implemented by OpDiv management *(metric 36)*.
- Defined security control guidance to help prevent data exfiltration that is to be implemented by OpDiv management based on its mission *(metric 37)*.
- The OpDivs we reviewed have tailored their own privacy programs to implement the broader HHS guidelines and have integrated their incident response and privacy breach response program *(metric 38)*.

- The OpDivs we reviewed have provided privacy awareness training to all individuals, including role-based privacy training (*metric 39*)

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:

- A defined security awareness and training program with established roles and responsibilities *(metric 41)*.

- Security awareness and training strategy and plan that leverages its organizational skills assessment and is adapted to the HHS culture *(metric 42)*.

- Definition of security awareness and specialized security training policies and procedures, which are required to be implemented *(metric 43)*.

- Security awareness training to all system users that is tailored based on its organizational requirements, culture, and types of information systems *(metric 44).*

- Specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301 "Information systems security awareness training program") (*metric 45*)

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 monitoring program results in ongoing updates to system security plans, a periodic security assessment and POA&Ms, which are three principal documents in a security authorization package.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2021 IG Assessment	Change from FY 2020 IG Assessment
Detect	ISCM	Defined	Decreased

HHS' information security continuous monitoring function has the following in place:

- Formalization of its ISCM program through development of ISCM policies, procedures, and strategies *(metric 47)*.
- Defined ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies have been communicated, and implemented across the organization *(metric 48).*

OCIO is responsible for developing the enterprise ISCM strategy. Each OpDiv is responsible for adapting the overall HHS strategy and modifying it to meet the needs of its environment. Moreover, each OpDiv has its own cybersecurity team that is responsible for compliance with the DHS CDM program. OCIO has a Technical Working Committee which is providing oversight on OpDiv's CDM implementation.

ISCM Findings and Recommendations

For FY2021, multiple findings were identified within the ISCM domain which resulted in a decrease in the function rating from FY2020 to FY2021. The following findings were identified within the OpDiv's ISCM program:

- Three (3) OpDivs have systems with expired ATOs listed within their active system inventory. One (1) OpDiv had an expired ATOs for all systems on their network.
- Three (3) OpDivs have discrepancies between the OpDiv-maintained system listings and the listings supplied to HHS Security Data Warehouse (HSDW). One (1) OpDiv was underreporting the number of active systems on their network.
- One (1) OpDiv did not have a clear understanding or documentation of ownership requirements associated with some of their contractor systems.
- One (1) OpDiv had discrepancies between the OpDiv maintained system listings and the information provided within their quarterly FISMA submission.

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

- All systems on the network have a valid ATO. OpDivs should ensure that security authorization policies and procedures are fully developed and disseminated to the appropriate personnel to ensure that all OpDiv personnel understand the requirements for completing the ATO process.

- ISCM strategy and procedures should clearly define critical reporting metrics for reports utilized by internal and external stakeholders. Additionally, OpDivs should coordinate reporting efforts with the OCIO to ensure the definitions and reporting requirements are consistently implemented.

- Accurate system inventory listings are reported to HHS OCIO. OpDivs and HHS OCIO should also implement a process to ensure that ATO status in the HSDW system reporting tool are regularly updated and current.

HHS OCIO Response:

HHS OCIO concurred with our recommendations.

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 2021 IG Assessment	Change from FY 2020 IG Assessment
Respond	Incident Response	Consistently Implemented	No Change

HHS’ incident response function has the following in place:

- Defined incident response policies, procedures, plans and strategies, as appropriate, to respond to cybersecurity events, which are required to be implemented *(metric 52)*.

- Defined and communicated incident response team structures/models, stakeholders and their roles, responsibilities, levels of authority and dependencies *(metric 53)*.
- Established monitoring requirements for security incidents identified across the enterprise which includes detection, analysis, and handling *(metric 54 and 55)*.
- Established communication channels across the enterprise to ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner *(metric 56)*.
- Established collaborations through contracts and agreements to ensure on-site, technical assistance and surge capabilities can be leverage as appropriate *(metric 57)*.
- Implemented technologies to support the incident response program with web application protections, event and incident management, log aggregation, malware detection, and endpoint security *(metric 58)*.

The HHS OCIO is responsible for developing enterprise incident response strategy. Each OpDiv adapts the strategy but modifies it to meet the needs of its environment. Each OpDiv is required to report incidents to HHS Computer Security Incident Response Center (CSIRC). The HHS CSIRC reports the incidents to the United States Computer Emergency Readiness Team (US Cert). Incident tickets are created for incidents in HHS OCIO RSA Archer system for the Department oversight.

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. 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 2021 IG Assessment	Change from FY 2020 IG Assessment
Recover	Contingency planning	Defined	No Change

HHS' contingency planning function has the following in place:

- HHS has defined its roles, responsibilities, and requirements for contingency planning to the OpDivs for implementation at the system level *(metric 60)*.
- Planning efforts are based on risk-based decisions derived from business impact analyses both at the enterprise and system level *(metric 61)*.
- HHS has defined that information system contingency plans are to be developed, maintained, and integrated with other continuity plans *(metric 62)*.
- OpDivs communicate information on the planning and performance of recovery activities to internal stakeholders and executive management teams that is used to make risk-based decisions *(metric 65)*.

Contingency Planning Findings and Recommendations

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

- Two (2) of the selected OpDivs had expired Contingency Plan Tests (CPTs) for some of its systems.
- One (1) OpDiv had some systems which did not have evidence to support implementation of system backup and storage.

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

- A process exists for monitoring contingency plan testing to prevent CPTs from not being performed in accordance with the established HHS policies. Additionally, OpDiv management should improve their HSDW reporting process by educating system owners on required fields for reportable metrics and validating those fields are provided to the OCIO when consolidating HHS wide data.
- OpDivs should improve their processes for monitoring contingency plan testing for all systems to prevent CPTs from not being performed annually in accordance with the established policies.

- OpDiv management ensure that all systems are implementing information system backup and storage as documented in HHS policies and procedures. Additionally, management should require that evidence is retained to document backup and storage procedures.

HHS OCIO COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

After issuing our draft report and based on feedback and discussion with HHS prior to HHS providing written comments, we consolidated 3 of our enterprise-wide recommendations into 1 recommendation for an enterprise-wide risk assessment over known control weaknesses in this final report. In written comments to our draft report, HHS concurred with all of our recommendations and described actions it has taken or plans to take to address them. HHS also provided technical comments, which we addressed as appropriate.

HHS's comments, excluding technical comments, are included as Appendix C.

Section 4
Appendices

Appendix A
Audit Scope and Methodology

4 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 after the OIG's review and concurrence.

The FY 2021 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 five HHS OpDivs:

- Administration for Children and Families (ACF)
- Administration for Community Living (ACL)
- Centers for Disease Control and Prevention (CDC)
- Centers for Medicare & Medicaid Services (CMS)
- Office of the Secretary (OS)

For two (2) of the five (5) OpDivs selected, ACF and ACL, we limited our review to selected domains. The selected domains included: Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, and Information Security Continuous Monitoring.

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 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 2021 IG FISMA metrics. Incorporated the results as part of the FY 2021 IG FISMA metrics.

- Inspected results from GAO and OIG audits and reports that had a similar scope to the FY 2021 IG FISMA metrics. Incorporated the results as part of the FY 2021 IG FISMA metrics.

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).
- FISMA Evaluation Guide (2019 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 Information Systems Security and Privacy Policy* (July 30, 2014).
- *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 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 22, 2015).

- 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-21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements (November 9, 2020).
- US-CERT Federal Incident Notification Guidelines.

Appendix C
FY 2021 Inspector General FISMA Reporting Metrics

4.3 Appendix C: FY 2021 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

2021

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' information security program, we executed an assessment plan that helped determine the maturity level for the questions listed in the FISMA reporting metrics. We assessed the maturity levels and effectiveness across the Identify (Risk Management, Supply Chain Risk Management (SCRM)), Protect (Configuration Management, Identity and Access Management, Data Protection & Privacy, and Security Training), Detect (Information Security Continuous Monitoring (ISCM)), Respond (Incident Response), and Recover (Contingency Planning) functional areas. In addition to the HHS Office of the Chief Information Officer, the following five HHS operating divisions (OpDivs) were in-scope for this assessment: Office of the Secretary, Centers for Medicare & Medicaid Services, Centers for Disease Control and Prevention, Administration for Community Living, and Administration for Children and Families. We also incorporated results from other IT audits and assessments performed throughout the year by the HHS OIG and GAO. We performed an inspection of HHS' and OpDivs' policies, procedures, standards and other guidance, as well as inspection of corresponding artifacts. Two significant areas preventing HHS from achieving an effective program are in the ISCM and Contingency Planning domains. The HHS FY21 Continuous Diagnostics and Mitigation (CDM) strategy resulted in visibility into some assets, awareness into some vulnerabilities and certain threat information through the use of RSA Archer and Splunk. HHS continues to work towards implementing a full Department-wide CDM program in coordination with DHS with the ultimate goals of 1.) Continuous monitoring of HHS networks and systems, 2.) Real-time reporting of OpDivs status and progress to help address and implement strategies to combat risk, 3.) Prioritization of issues based on established risk criteria, and 4.) Improving federal cybersecurity response capabilities. In the area of SCRM, HHS is in the beginning stages of implementing a supply chain risk management program as a result of it the new requirements in NIST 800-53 revision 5.

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

Function 0: Overall

domain that would allow HHS to have an effective program, and (4) the evaluation of a maturity level below Consistently Implemented for individual metric questions both at HHS overall and at selected OpDivs. HHS is cognizant of opportunities which arise to strengthen the overall information security program which would help ensure that policies and procedures in place at all OpDivs are consistently implemented and in line with the requirements across their security programs. Two significant areas preventing HHS from achieving an effective program are in the ISCM 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 & 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. 4: CA-3, PM-5, and CM-8; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for maintaining a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections.

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. 4: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is Managed and Measurable while two OpDivs are Consistently Implemented for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization’s network with the detailed information necessary for tracking and reporting. One OpDiv only has a Defined process for using standard data elements to maintain an up-to-date inventory of hardware assets connected to the organizations network.

Function 1A: Identify - Risk Management

3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Consistently Implemented at two OpDivs and Defined at another OpDiv 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. One OpDiv has a Managed and Measurable process for tracking and reporting software inventories connected to their network.

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 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-4, P-12, P-13, S-1 - S-3, NIST IR 8170)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Managed and Measurable at two OpDivs, and Consistently Implemented at two OpDivs for categorizing and communicating the importance/priority of information systems in enabling its missions and business functions.

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. 4: RA-3, 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 P-2, P-3, P-14, R-2, and R-3?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. HHS is Consistently Implemented at three OpDivs and Defined at one OpDiv. Three 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.

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 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. All OpDivs consistently implemented a security architecture across its enterprise, business process, and system levels. The OpDivs ensured system security engineering principles are followed and included assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment.

7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, and implemented 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; NIST IR 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)?

Consistently Implemented (Level 3)

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

8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are 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-04-14, M-19-03, CSF v1.1, ID.RA-6)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. For all OpDivs reviewed, management consistently utilized POA&Ms to effectively mitigate security weaknesses. Management utilized a prioritized and consistent approach to POA&Ms that considers items such as, but not limited to, security categorization, specific control deficiencies, and POA&M attributes captured in M-04-14.

9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders (OMB A-123; OMB Circular A-11 and OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NIST IR 8170 and 8286)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with 2 OpDivs at the Defined level. Two OpDivs did not consistently utilize a cybersecurity risk register, or other comparable mechanism to ensure that information about risks are communicated in a timely and effective manner to appropriate internal and external stakeholders with a need-to-know.

10. To what extent does the organization 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 and NIST IR 8286)?

Function 1A: Identify - Risk Management

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. One OpDiv is Consistently Implemented and one OpDiv is Managed and Measurable. Two OpDivs did not 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.

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at the Consistently Implemented level for its Risk Management program.

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?

We have assessed the Risk Management domain as Consistently Implemented. According to the FY2021 Inspector General FISMA Reporting Metrics, at Level 4 (Managed and Measurable), the information security program is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Consistently Implemented rating at HHS for this domain is ineffective. With full implementation of the CDM tools at the Department and OpDiv level, HHS should have the capability to move to a managed and measurable risk management program which should be effective across HHS.

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Four OpDivs did not consistently implement a SCRM strategy across the organization and utilize the strategy to guide supply chain analyses, communication with internal and external partners and stakeholders, and in building consensus regarding the appropriate resources for SCRM.

13. To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (The Federal Acquisition Supply Chain Security Act of 2018, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Four OpDivs did not consistently implement policies, procedures, and processes for managing supply chain risks for organizationally-defined products, systems, and services provided by third parties.

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, 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).

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. 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 ensure that counterfeit components are detected and prevented from entering the organization`s systems? (800-53 rev 5 SR-11, 11 (1), and 11(2)

Ad Hoc (Level 1)

Comments: Overall, HHS is at an Ad Hoc maturity level. Four OpDivs have not defined and communicated their component authenticity policies and procedures.

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

Defined (Level 2)

Comments: Overall, HHS is at the Defined level for its Supply Chain Risk Management program.

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at the Consistently Implemented level for the Identify function.

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?

We have assessed the Supply Chain Risk Management program as Defined. According to the FY 2021 Inspector General FISMA Reporting Metrics, at Level 4 (Managed and Measurable), an information security program is considered to be operating at an effective level of security. We have concluded that a Defined rating across HHS for SCRM is ineffective. Since the Risk Management domain is Consistently Implemented, the risk management program is not effective.

Function 2A: Protect - Configuration Management

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs are Consistently Implemented, one OpDiv is at the Defined level and one OpDiv is at the Managed and Measurable level. Three OpDivs did not allocate resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively perform information system configuration management activities.

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)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Four OpDivs did not monitor, analyze, and report to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, use this information to take corrective actions when necessary, and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

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 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Four OpDivs did not consistently record, implement, and maintain baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.

20. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs consistently implement, assess, and maintain secure configuration settings for its information systems. Two OpDivs are Defined and did not maintain secure configuration settings.

Function 2A: Protect - Configuration Management

21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2021 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02 and 19-02)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Four 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.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26, DHS-CISA TIC 3.0 Core Guidance Documents)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for implemented its TIC approved connections and critical capabilities that it manages internally. HHS has consistently implemented defined TIC security controls, as appropriate, and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.

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).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs are rated Defined since they did not consistently implement their change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation.

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)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Four OpDivs have developed, documented, and publicly disseminated a comprehensive VDP.

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

Consistently Implemented (Level 3)

Function 2A: Protect - Configuration Management

Comments: The HHS configuration management program is at the Consistently Implemented level.

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?

We have assessed the Configuration Management domain as Consistently Implemented. According to the FY 2021 Inspector General FISMA Reporting Metrics, at Level 4 (Managed and Measurable), the information security program is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Consistently Implemented rating at HHS for this domain is ineffective.

Function 2B: Protect - Identity and Access Management

26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (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 (FICAM) playbooks and guidance (see idmanagement.gov), OMB M-19-17)?

Consistently Implemented (Level 3)

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

27. To what extent does the organization 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; SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. One OpDiv is Managed and Measurable, one OpDiv is Consistently Implemented, and two OpDivs are Defined. Two OpDivs did not consistently implement their ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones.

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)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Two OpDivs are at the Defined level since they did not ensure that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. Two OpDivs are at the Managed and Measurable level since they employed an automation to centrally document, track, and share risk designations and screening information with necessary parties.

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)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is at Managed and Measurable level and three OpDivs are at the Consistently Implemented level. One OpDiv did not ensure that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. One OpDiv employed automation to centrally document, track, and share risk designations and screening information with necessary parties.

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 non-privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: 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 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is Defined and three OpDivs are Consistently Implemented. Four OpDivs 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 (HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented level. One OpDiv is Consistently Implemented and two OpDivs are Defined. Two OpDivs are 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 (FY 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4).

Defined (Level 2)

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

33. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote 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 2021 CIO FISMA Metrics: 2.10 and 2.11).

Consistently Implemented (Level 3)

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

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

Consistently Implemented (Level 3)

Comments: The Identify and Access Management program was Consistently Implemented.

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?

We have assessed the Configuration Management domain as Consistently Implemented. According to the FY 2021 Inspector General FISMA Reporting Metrics, at Level 4 (Managed and Measurable), an information security program is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Consistently Implemented rating at HHS for this domain is ineffective.

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), NIST Privacy Framework)?

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a Managed and Measurable maturity level. Two OpDivs are Managed and Measurable and two OpDivs are Consistently Implemented. Two OpDivs did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments.

36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle. (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2021 CIO FISMA Metrics: 2.8, 2.12; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

·Encryption of data at rest

·Encryption of data in transit

·Limitation of transfer to removable media

·Sanitization of digital media prior to disposal or reuse

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. 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.

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs reviewed for this metric conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. However, they did not analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses.

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)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs are Consistently Implemented, one OpDiv is Managed and Measurable, and one OpDiv is Defined. One OpDiv did not consistently implement their Data Breach Response plan. One OpDiv monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its Data Breach

Response Plan, as appropriate.

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)?

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a Managed and Measurable maturity level. Two OpDivs are Managed and Measurable and two OpDivs are Consistently Implemented. Two OpDivs measured the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII.

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

Consistently Implemented (Level 3)

Comments: Data Protection and Privacy is at the Consistently Implemented level.

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?

We have assessed the Data Protection and Privacy domain as Consistently Implemented. According to the FY 2021 Inspector General FISMA Reporting Metrics, Level 4 (Managed and Measurable) an information security program is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Consistently Implemented rating for this domain is ineffective.

Function 2D: Protect - Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. While two OpDivs are Managed and Measurable, one OpDiv is Consistently Implemented and one OpDiv is Defined. Two OpDivs allocate resources (people, processes, and technology) in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities.

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 (NIST SP 800-53 REV. 4: AT-2 and AT-3; 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/SANS Top 20: 17.1)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. One OpDiv is Managed and Measurable and one OpDiv is Consistently Implemented. One OpDiv and the Department have not 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.

43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs are Managed and Measurable, one OpDiv is Consistently Implemented and one OPDIV is Defined. Two OpDivs monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans.

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-1, AT-2; FY 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is Defined. Three OpDivs monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices.

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization`s security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2021 CIO FISMA Metrics: 2.15, and 5 Code of Federal Regulation 930.301)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OpDivs monitor and analyze qualitative and

Function 2D: Protect - Security Training

quantitative performance measures on the effectiveness of its security training policies, procedures, and practices.

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

Consistently Implemented (Level 3)

Comments: We have assessed the Security Training domain as Consistently Implemented.

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at the Consistently Implemented level for Protect function.

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?

We have assessed the Security Training domain as Consistently Implemented. According to the FY 2021 Inspector General FISMA Reporting Metrics, at Level 4 (Managed and Measurable), the security program is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Consistently Implemented rating at HHS is ineffective for the Security Training domain.

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 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Two OpDivs 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, communicated, and implemented 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)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is at the Consistently Implemented maturity level and one OPDIV is at a Managed and Measurable maturity level. Two of the OpDivs did not define and communicate the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.

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. 4: CA-2, CA-6, and CA-7; 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. Three OpDivs are at the Defined level. Two OpDivs consistently implemented its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system’s contribution to said security posture.

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OpDiv is Defined. Three OpDivs consistently captured qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.

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 50/50 between Consistently Implemented and Defined, during the assessment we noted multiple findings associated with the ISCM domain in regard to ATO's and their consistent completion as well as reporting to the appropriate stakeholders. In addition, during the assessment of one OpDiv, we identified a system with no clear ownership or chain of command.

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?

We have assessed the ISCM domain as Defined. According to the FY 2021 Inspector General FISMA Reporting Metrics, at Level 4 (Managed and Measurable), an information security program is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Defined rating for ISCM is ineffective.

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)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its incident response plan and made updates, as appropriate and one OpDiv did not. HHS is still working on improving their Incident Response program.

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (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 2021 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs allocated resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively implement incident response activities. One OpDiv did not allocate resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively implement incident response activities. HHS is still working on improving their Incident Response program.

54. How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three 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 and one OpDiv did not. HHS is still working on improving their Incident Response program in order to bring it to a Managed and Measurable level.

55. How mature are the organization's processes for incident handling (NIST 800-53: 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. Two OpDivs managed and measured the impact of successful incidents and could quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability. Two OpDivs did not manage and measure the impact of successful incidents.

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)

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a Managed and Measurable maturity level. Three OpDivs used incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. One OpDiv did not ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

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).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs utilized Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises. One OpDiv did not utilize Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises.

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)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Three OpDivs evaluated the effectiveness of its incident response technologies and made adjustments to configurations and toolsets, as appropriate. One OpDiv did not evaluate the effectiveness of its incident response technologies.

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

Consistently Implemented (Level 3)

Comments: We have assessed the Incident Response domain as Consistently Implemented.

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?

According to the FY2021 Inspector General FISMA Reporting Metrics, Level 4 (Managed and Measurable),

Function 4: Respond - Incident Response

is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Consistently Implemented rating for the incident response program is ineffective.

Function 5: Recover - Contingency Planning

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Four OpDivs ensured that contingency training is provided consistent with roles and responsibilities to ensure that the appropriate content and level of detail is included.

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Two OpDivs consistently incorporated the results of organizational and system level BIAs into strategy and plan development efforts. Two OpDivs did not consistently incorporate the results of organizational and system level BIAs into strategy and plan development efforts. In addition, HHS has outstanding recommendations associated with Contingency Planning which still need to be addressed to help them towards a Consistently Implemented program.

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 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Three OpDivs consistently developed and implemented information system contingency plans for systems as appropriate. One OpDiv was not developing and implementing information system contingency plans for all systems as appropriate. In addition, HHS has outstanding recommendations associated with Contingency Planning which still need to be addressed to help them towards a Consistently Implemented program.

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?

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.

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 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Three OpDivs consistently implemented its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. One OpDiv did not implement its policies, procedures, processes, strategies, and technologies for information system backup and storage. In addition, HHS has outstanding recommendations associated with Contingency Planning which still need to be addressed to help them towards a Consistently Implemented level.

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)?

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a Managed and Measurable maturity level. Two OpDivs were managed and measurable at communicating metrics on the effectiveness of recovery activities to relevant stakeholders and the OpDiv has ensured that the data supporting the metrics were obtained accurately, consistently, and in a reproducible format. Two OpDivs had not ensured that the data supporting the metrics being communicated are obtained accurately, consistently, and in a reproducible format.

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

Defined (Level 2)

Comments: We have assessed the Contingency Planning domain as Defined.

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?

According to the FY2021 Inspector General FISMA Reporting Metrics, a Level 4 (Managed and Measurable) information security program is considered to be operating at an effective level of security. Therefore, we have concluded that an overall Defined rating for the contingency planning program is ineffective.

APPENDIX A: Maturity Model Scoring

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

Function 1A: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	9
Managed and Measurable	0
Optimized	0
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 1B: Identify - Supply Chain Risk Management

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

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0

Defined	3
Consistently Implemented	5
Managed and Measurable	0
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Assessed Rating: Consistently Implemented (Level 3)

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	5
Managed and Measurable	0
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Assessed Rating: Consistently Implemented (Level 3)

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	3
Managed and Measurable	2
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Assessed Rating: Consistently Implemented (Level 3)

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	4
Managed and Measurable	0
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Assessed Rating: Consistently Implemented (Level 3)

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	2
Managed and Measurable	0
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0

Consistently Implemented	6
Managed and Measurable	1
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	4
Consistently Implemented	1
Managed and Measurable	1
Optimized	0

Calculated Rating: Defined (Level 2)

Overall

Function	Calculated Maturity Level	Accessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Overall, HHS is at the Consistently Implemented level for the Identify function.
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Overall, HHS is at the Consistently Implemented level for Protect function.

Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Defined (Level 2)	We have assessed the ISCM domain as Defined. While overall ratings were split 50/50 between Consistently Implemented and Defined, during the assessment we noted multiple findings associated with the ISCM domain in regard to ATO's and their consistent completion as well as reporting to the appropriate stakeholders. In addition, during the assessment of one OpDiv, we identified a system with no clear ownership or chain of command.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We have assessed the Incident Response domain as Consistently Implemented.
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	We have assessed the Contingency Planning domain as Defined.

Overall	Not Effective	Not Effective	To assess and determine the effectiveness of HHS' information security program, we executed an assessment plan that helped determine the maturity level for the questions listed in the FISMA reporting metrics. We assessed the maturity levels and effectiveness across the Identify (Risk Management, Supply Chain Risk Management (SCRM)), Protect (Configuration Management, Identity and Access Management, Data Protection & Privacy, and Security Training), Detect (Information Security Continuous Monitoring (ISCM)), Respond (Incident Response), and Recover (Contingency Planning) functional areas. In addition to the HHS Office of the Chief Information Officer, the following five HHS operating divisions (OpDivs) were in-scope for this assessment: Office of the Secretary, Centers for Medicare & Medicaid Services, Centers for Disease Control and Prevention, Administration for Community Living, and Administration for Children and Families. We also incorporated results from other IT audits and assessments performed throughout the year by the HHS OIG and GAO. We performed an inspection of HHS' and OpDivs' policies,

procedures, standards and other guidance, as well as inspection of corresponding artifacts. Two significant areas preventing HHS from achieving an effective program are in the ISCM and Contingency Planning domains.

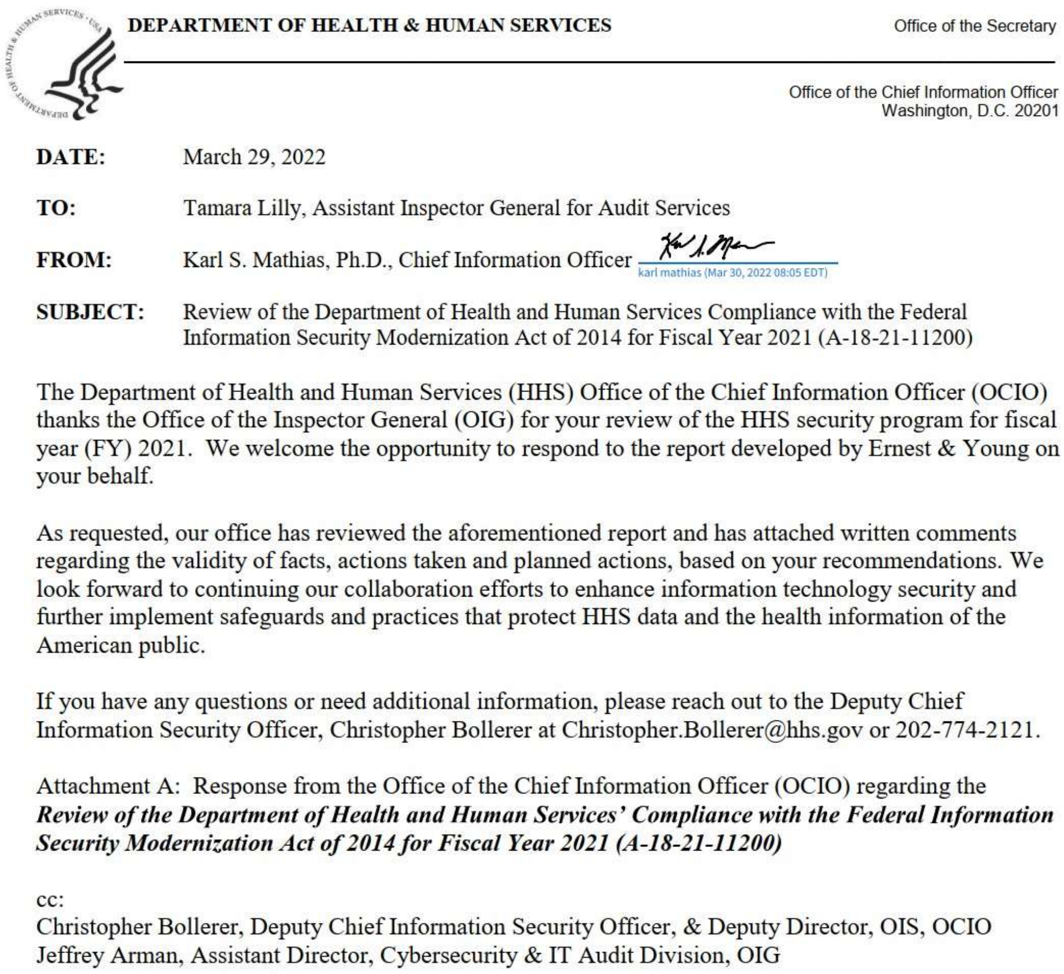
The HHS FY21 Continuous Diagnostics and Mitigation (CDM) strategy resulted in visibility into some assets, awareness into some vulnerabilities and certain threat information through the use of RSA Archer and Splunk. HHS continues to work towards implementing a full Department-wide CDM program in coordination with DHS with the ultimate goals of 1.) Continuous monitoring of HHS networks and systems, 2.) Real-time reporting of OpDivs status and progress to help address and implement strategies to combat risk, 3.) Prioritization of issues based on established risk criteria, and 4.) Improving federal cybersecurity response capabilities.

In the area of SCRM, HHS is in the beginning stages of implementing a supply chain risk management program as a result of it the new requirements in NIST 800-53 revision 5.

APPENDIX A: Maturity Model Scoring

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: March 29, 2022

TO: Tamara Lilly, Assistant Inspector General for Audit Services

FROM: Karl S. Mathias, Ph.D., Chief Information Officer
karl mathias (Mar 30, 2022 08:05 EDT)

SUBJECT: Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021 (A-18-21-11200)

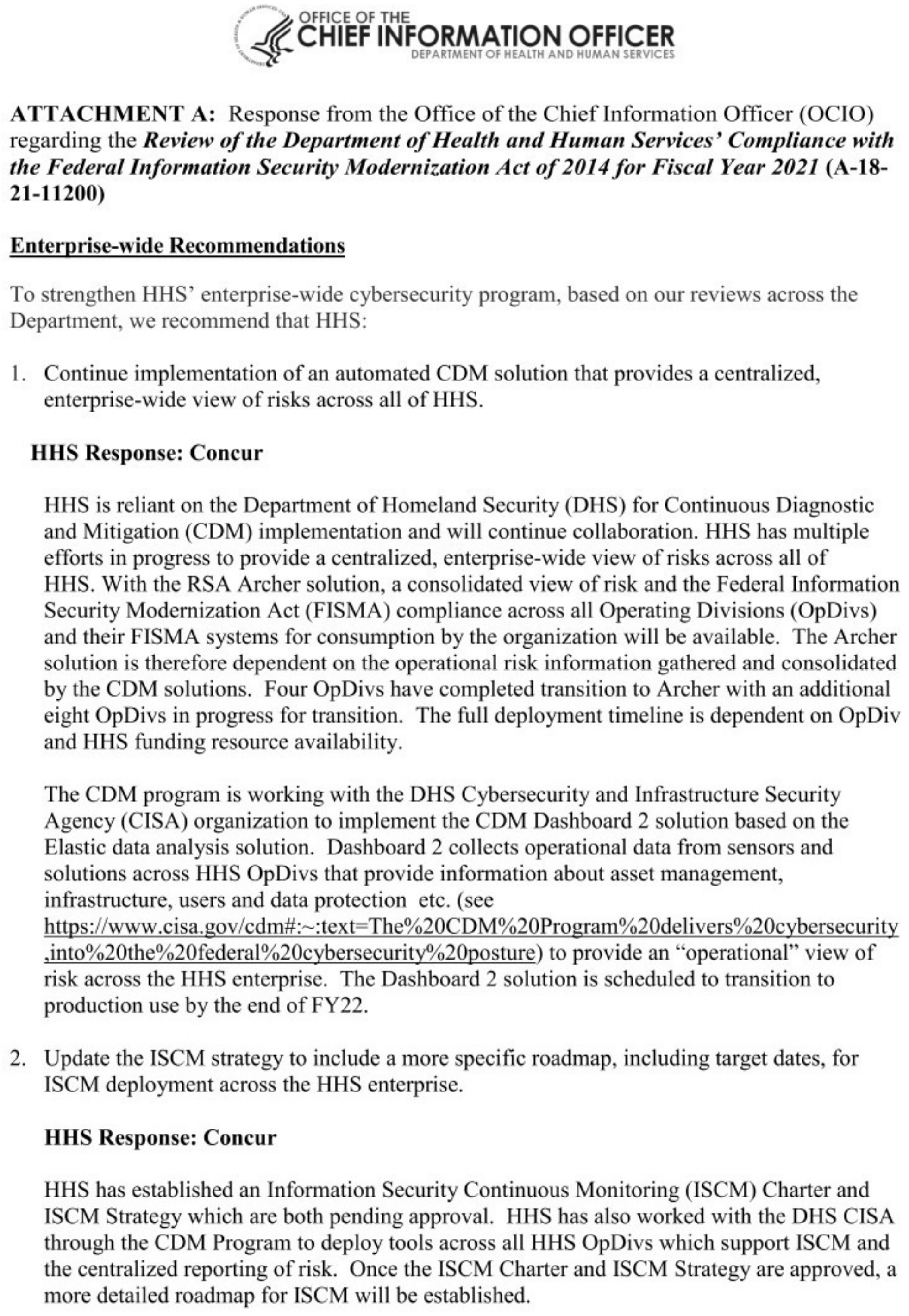
The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) thanks the Office of the Inspector General (OIG) for your review of the HHS security program for fiscal year (FY) 2021. We welcome the opportunity to respond to the report developed by Ernest & Young on your 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 Deputy Chief Information Security Officer, Christopher Bollerer at Christopher.Bollerer@hhs.gov or 202-774-2121.

Attachment A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021 (A-18-21-11200)***

cc:
Christopher Bollerer, Deputy Chief Information Security Officer, & Deputy Director, OIS, OCIO
Jeffrey Arman, Assistant Director, Cybersecurity & IT Audit Division, OIG



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 2021*** **(A-18-21-11200)**

Enterprise-wide Recommendations

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

1. Continue implementation of an automated CDM solution that provides a centralized, enterprise-wide view of risks across all of HHS.

HHS Response: Concur

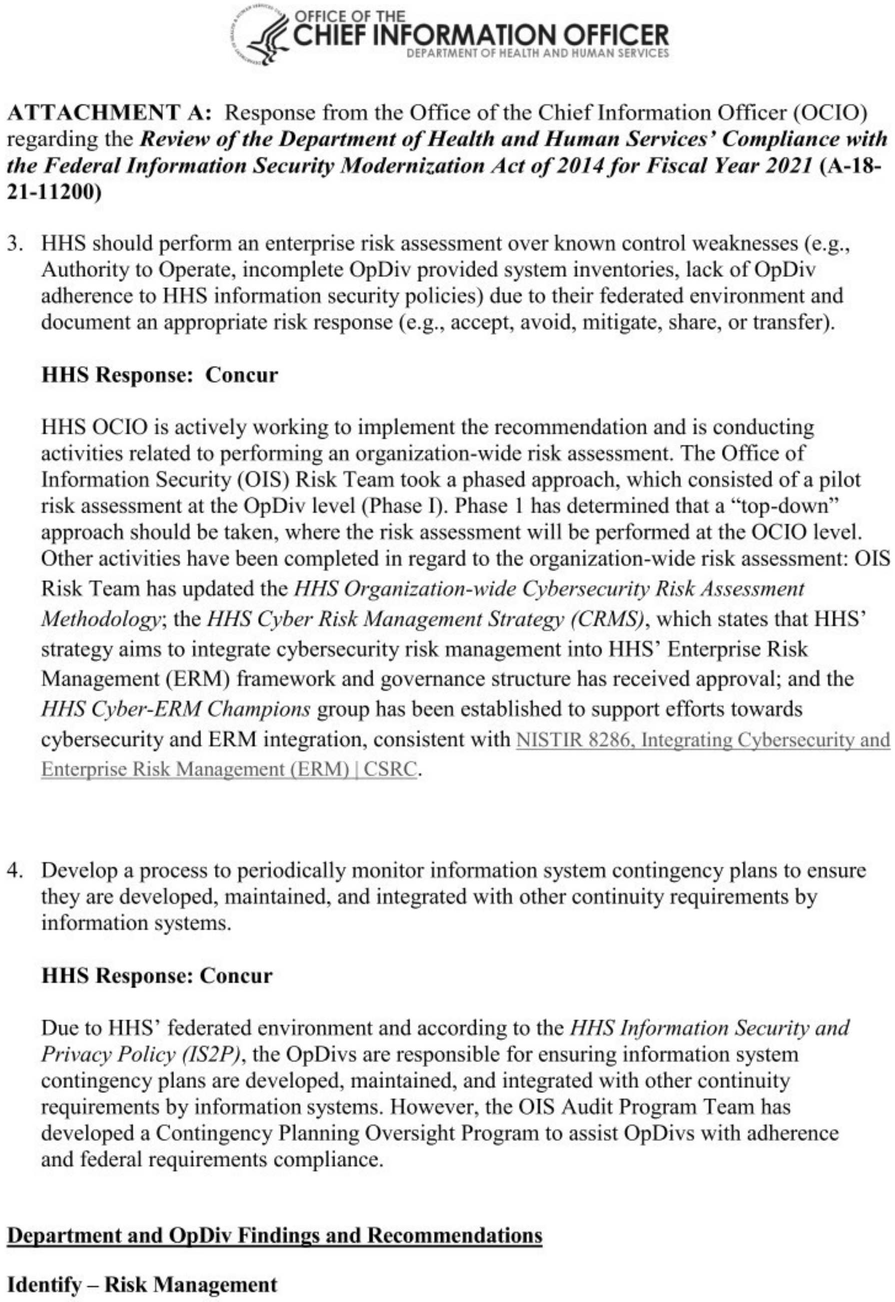
HHS is reliant on the Department of Homeland Security (DHS) for Continuous Diagnostic and Mitigation (CDM) implementation and will continue collaboration. HHS has multiple efforts in progress to provide a centralized, enterprise-wide view of risks across all of HHS. With the RSA Archer solution, a consolidated view of risk and the Federal Information Security Modernization Act (FISMA) compliance across all Operating Divisions (OpDivs) and their FISMA systems for consumption by the organization will be available. The Archer solution is therefore dependent on the operational risk information gathered and consolidated by the CDM solutions. Four OpDivs have completed transition to Archer with an additional eight OpDivs in progress for transition. The full deployment timeline is dependent on OpDiv and HHS funding resource availability.

The CDM program 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,into%20the%20federal%20cybersecurity%20posture) to provide an "operational" view of risk across the HHS enterprise. The Dashboard 2 solution is scheduled to transition to production use by the end of FY22.

2. Update the ISCM strategy to include a more specific roadmap, including target dates, for ISCM deployment across the HHS enterprise.

HHS Response: Concur

HHS has established an Information Security Continuous Monitoring (ISCM) Charter and ISCM Strategy which are both pending approval. HHS has also worked with the DHS CISA through the CDM Program to deploy tools across all HHS OpDivs which support ISCM and the centralized reporting of risk. Once the ISCM Charter and ISCM Strategy are approved, a more detailed roadmap for ISCM will be established.



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 2021*** **(A-18-21-11200)**

3. HHS should perform an enterprise risk assessment over known control weaknesses (e.g., Authority to Operate, incomplete OpDiv provided system inventories, lack of OpDiv adherence to HHS information security policies) due to their federated environment and document an appropriate risk response (e.g., accept, avoid, mitigate, share, or transfer).

   HHS Response: Concur

   HHS OCIO is actively working to implement the recommendation and is conducting activities related to performing an organization-wide risk assessment. The Office of Information Security (OIS) Risk Team took a phased approach, which consisted of a pilot risk assessment at the OpDiv level (Phase I). Phase 1 has determined that a "top-down" approach should be taken, where the risk assessment will be performed at the OCIO level. Other activities have been completed in regard to the organization-wide risk assessment: OIS Risk Team has updated the *HHS Organization-wide Cybersecurity Risk Assessment Methodology*; the *HHS Cyber Risk Management Strategy (CRMS)*, which states that HHS' strategy aims to integrate cybersecurity risk management into HHS' Enterprise Risk Management (ERM) framework and governance structure has received approval; and the *HHS Cyber-ERM Champions* group has been established to support efforts towards cybersecurity and ERM integration, consistent with NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM) | CSRC.

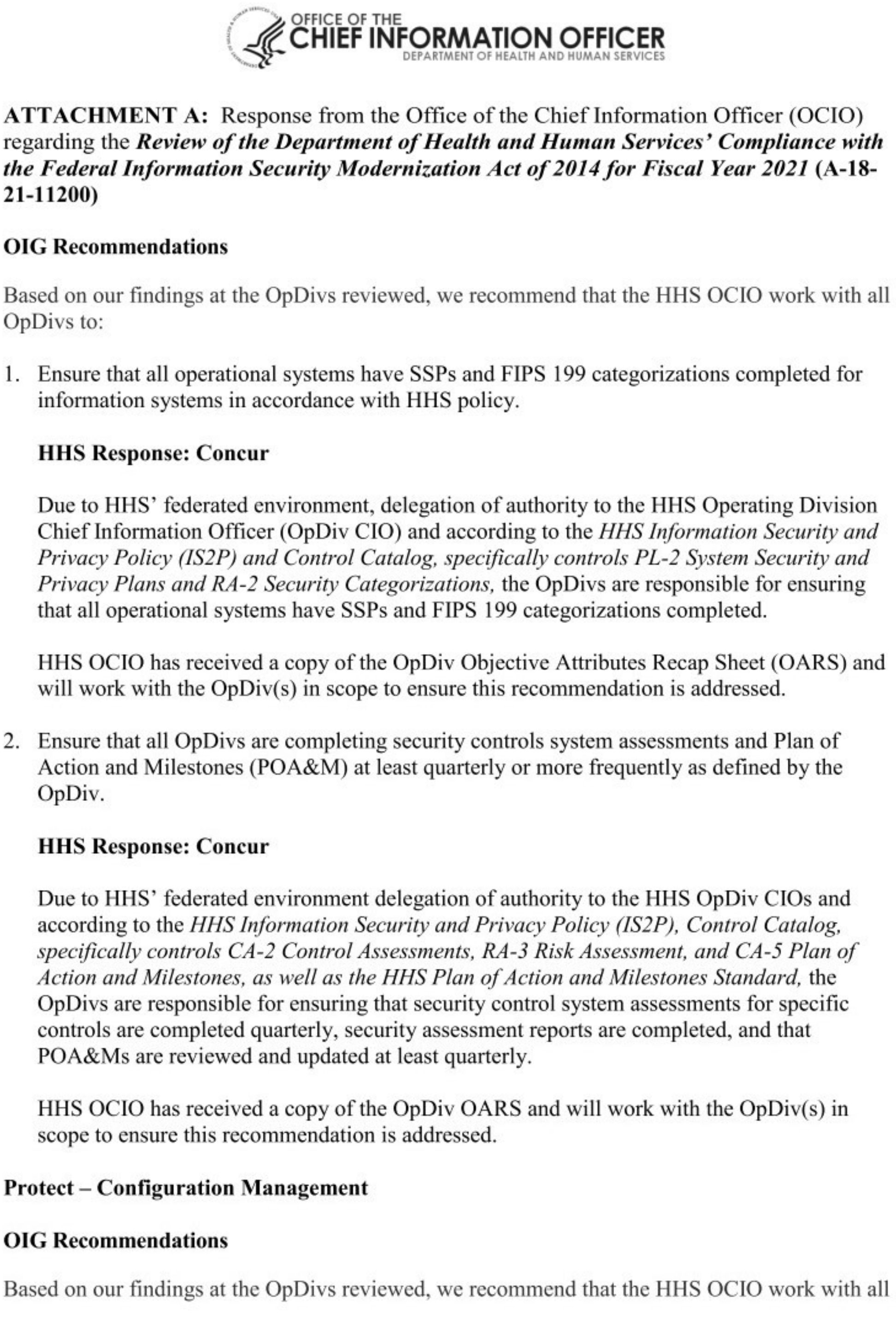
4. Develop a process to periodically monitor information system contingency plans to ensure they are developed, maintained, and integrated with other continuity requirements by information systems.

   HHS Response: Concur

   Due to HHS' federated environment and according to the *HHS Information Security and Privacy Policy (IS2P)*, the OpDivs are responsible for ensuring information system contingency plans are developed, maintained, and integrated with other continuity requirements by information systems. However, the OIS Audit Program Team has developed a Contingency Planning Oversight Program to assist OpDivs with adherence and federal requirements compliance.

Department and OpDiv Findings and Recommendations

Identify – Risk Management



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 2021*** **(A-18-21-11200)**

OIG Recommendations

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

1. Ensure that all operational systems have SSPs and FIPS 199 categorizations completed for information systems in accordance with HHS policy.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS Operating Division Chief Information Officer (OpDiv CIO) and according to the *HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically controls PL-2 System Security and Privacy Plans and RA-2 Security Categorizations,* the OpDivs are responsible for ensuring that all operational systems have SSPs and FIPS 199 categorizations completed.

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

2. Ensure that all OpDivs are completing security controls system assessments and Plan of Action and Milestones (POA&M) at least quarterly or more frequently as defined by the OpDiv.

   HHS Response: Concur

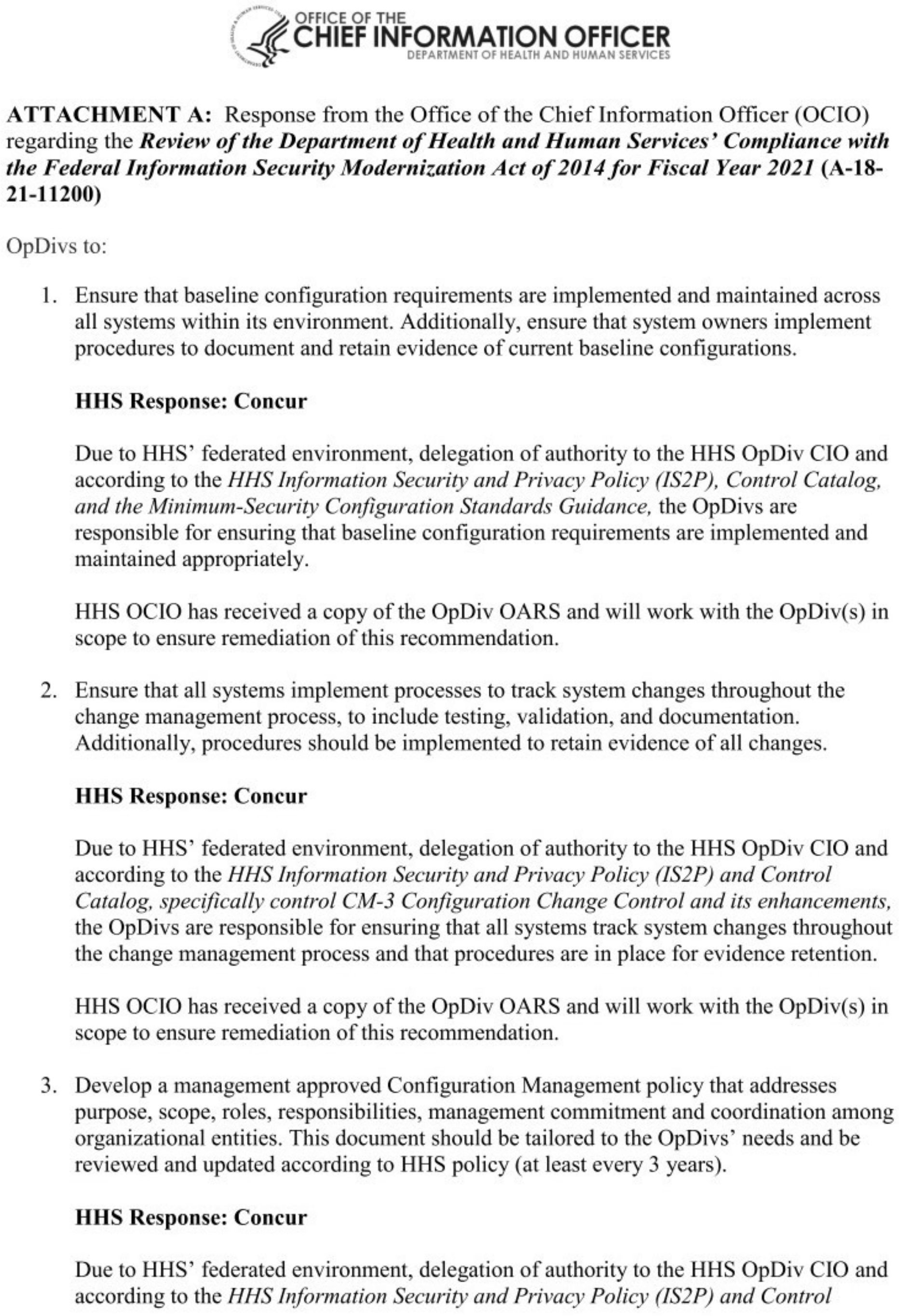
   Due to HHS' federated environment delegation of authority to the HHS OpDiv CIOs and according to the *HHS Information Security and Privacy Policy (IS2P), Control Catalog, specifically controls CA-2 Control Assessments, RA-3 Risk Assessment, and CA-5 Plan of Action and Milestones, as well as the HHS Plan of Action and Milestones Standard,* the OpDivs are responsible for ensuring that security control system assessments for specific controls are completed quarterly, security assessment reports are completed, and that POA&Ms are reviewed and updated at least quarterly.

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

Protect – Configuration Management

OIG Recommendations

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



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 2021*** **(A-18-21-11200)**

OpDivs to:

1. Ensure that baseline configuration requirements are implemented and maintained across all systems within its environment. Additionally, ensure that system owners implement procedures to document and retain evidence of current baseline configurations.

   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), Control Catalog, and the Minimum-Security Configuration Standards Guidance,* the OpDivs are responsible for ensuring that baseline configuration requirements are implemented and maintained appropriately.

   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 systems implement processes to track system changes throughout the change management process, to include testing, validation, and documentation. Additionally, procedures should be implemented to retain evidence of all changes.

   HHS Response: Concur

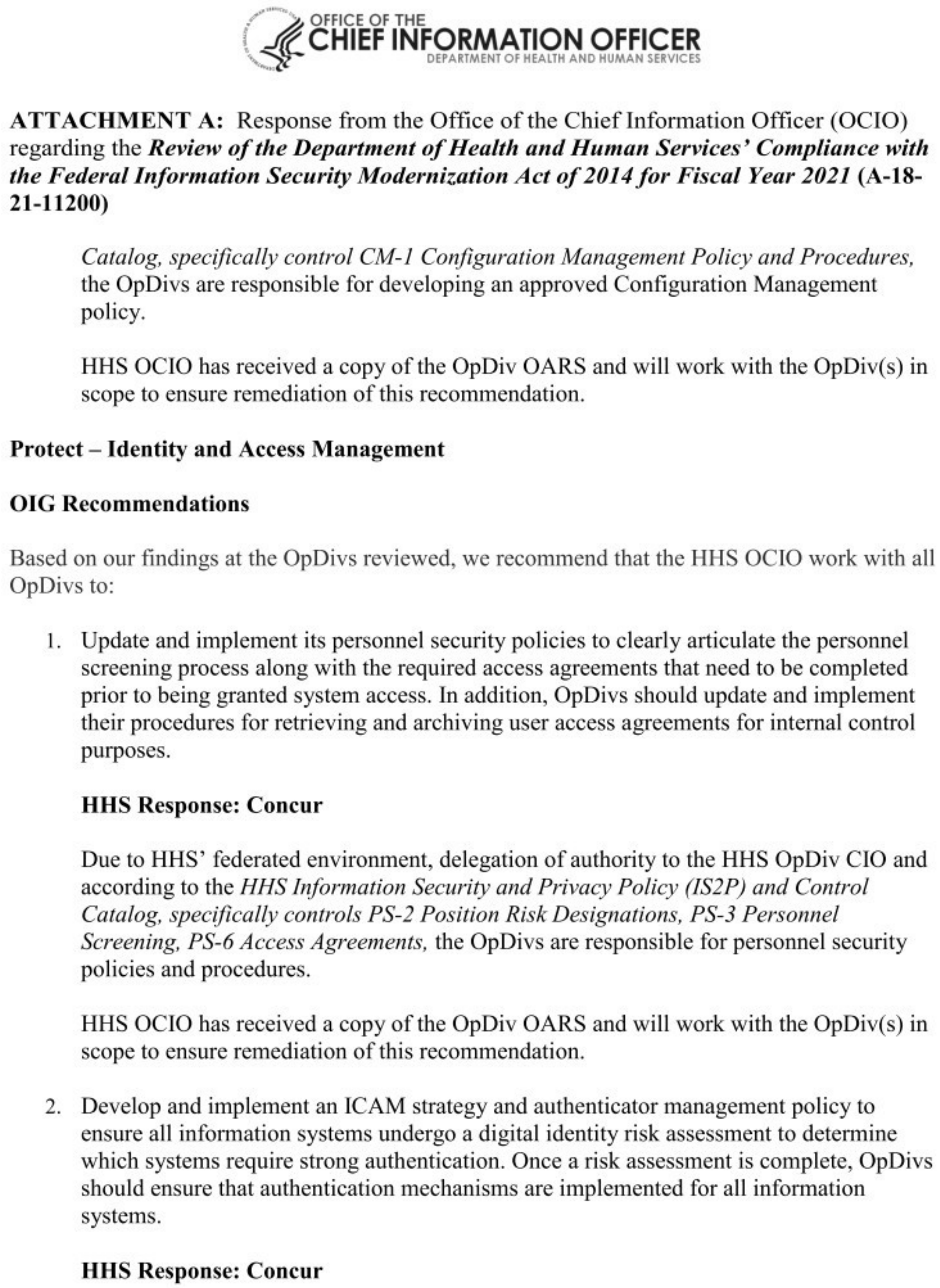
   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the *HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control CM-3 Configuration Change Control and its enhancements,* the OpDivs are responsible for ensuring that all systems track system changes throughout the change management process and that procedures are in place for evidence retention.

   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. Develop a management approved Configuration Management policy that addresses purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities. This document should be tailored to the OpDivs' needs and be reviewed and updated according to HHS policy (at least every 3 years).

   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*



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 2021* (A-18-21-11200)**

Catalog, specifically control CM-1 Configuration Management Policy and Procedures, the OpDivs are responsible for developing an approved Configuration Management 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.

Protect – Identity and Access Management

OIG Recommendations

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

1. Update and implement its personnel security policies to clearly articulate the personnel screening process along with the required access agreements that need to be completed prior to being granted system access. In addition, OpDivs should update and implement their procedures for retrieving and archiving user access agreements for internal control purposes.

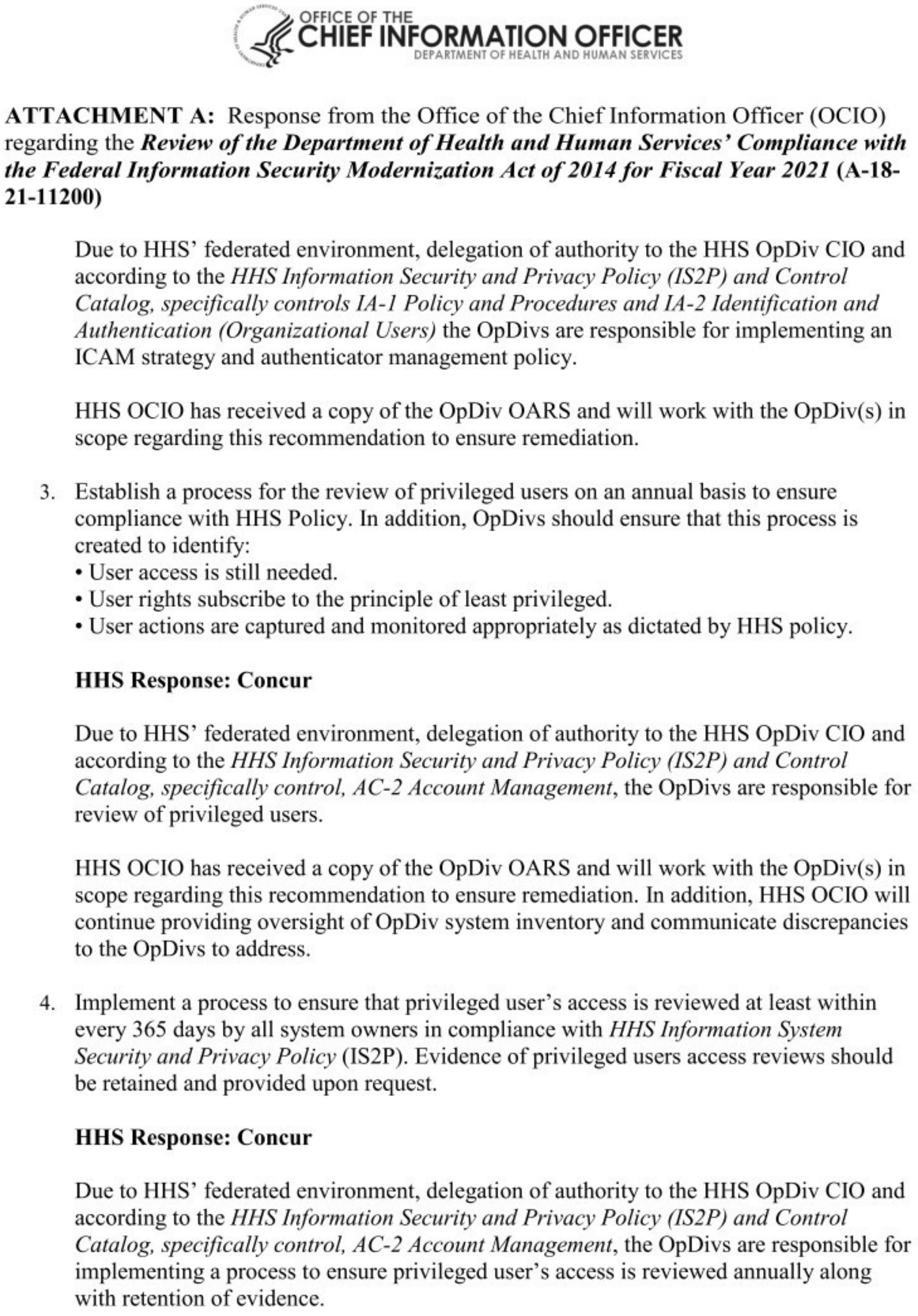
   HHS Response: Concur

   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 Designations, PS-3 Personnel Screening, PS-6 Access Agreements,* the OpDivs are responsible for personnel security policies and procedures.

   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. Develop and implement an ICAM strategy and authenticator management policy to ensure all information systems undergo a digital identity risk assessment to determine which systems require strong authentication. Once a risk assessment is complete, OpDivs should ensure that authentication mechanisms are implemented for all information systems.

   HHS Response: Concur



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 2021* (A-18-21-11200)**

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 IA-1 Policy and Procedures and IA-2 Identification and Authentication (Organizational Users)* the OpDivs are responsible for implementing an ICAM strategy and authenticator management policy.

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

3. Establish a process for the review of privileged users on an annual basis to ensure compliance with HHS Policy. In addition, OpDivs should ensure that this process is created to identify:
   • User access is still needed.
   • User rights subscribe to the principle of least privileged.
   • User actions are captured and monitored appropriately as dictated by HHS policy.

   HHS Response: Concur

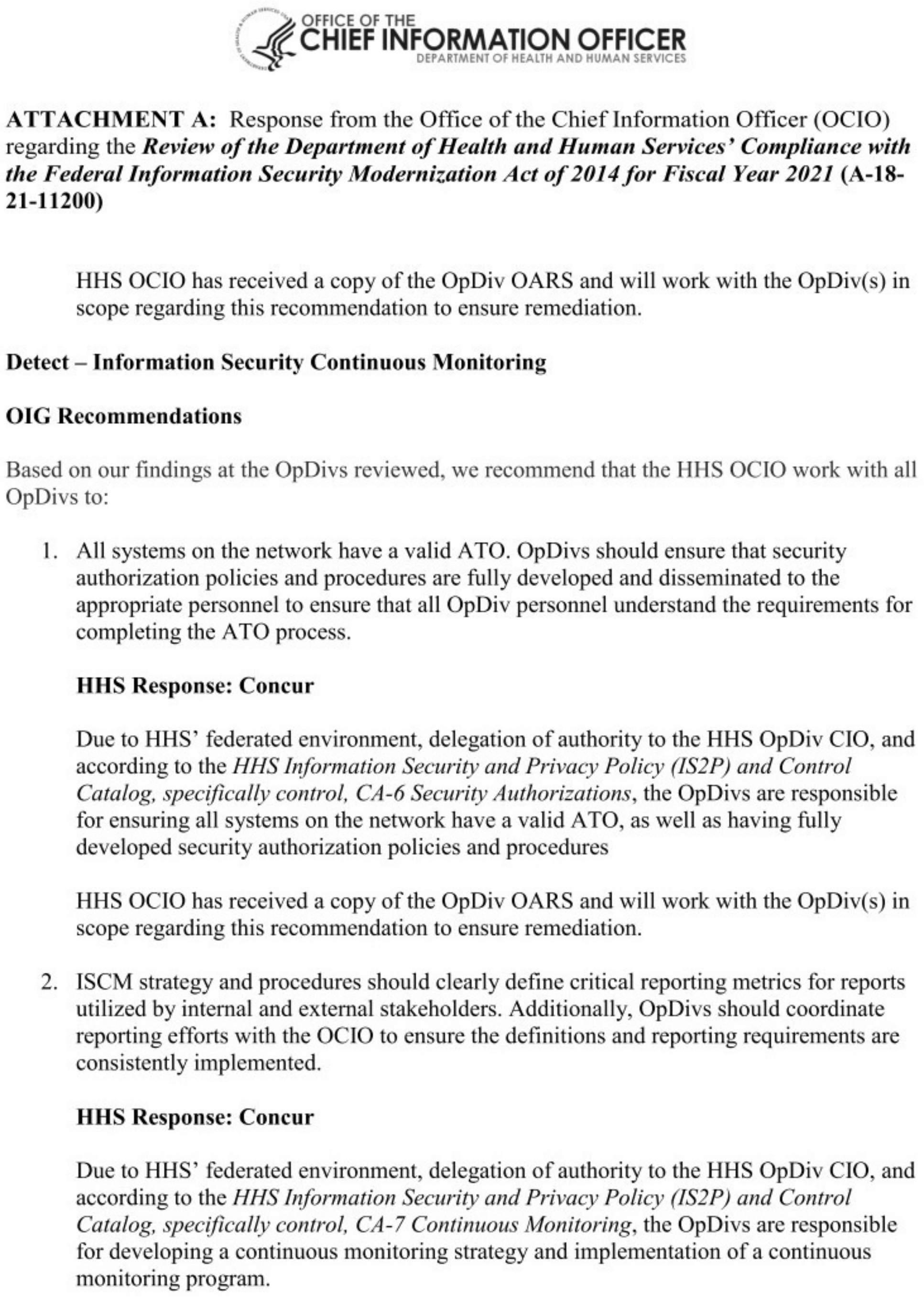
   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO and according to the *HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control, AC-2 Account Management*, the OpDivs are responsible for review of privileged users.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope regarding this recommendation to ensure remediation. In addition, HHS OCIO will continue providing oversight of OpDiv system inventory and communicate discrepancies to the OpDivs to address.

4. Implement a process to ensure that privileged user's access is reviewed at least within every 365 days by all system owners in compliance with *HHS Information System Security and Privacy Policy* (IS2P). Evidence of privileged users access reviews should be retained and provided upon request.

   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-2 Account Management*, the OpDivs are responsible for implementing a process to ensure privileged user's access is reviewed annually along with retention of evidence.



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 2021*** **(A-18-21-11200)**

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

Detect – Information Security Continuous Monitoring

OIG Recommendations

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

1. All systems on the network have a valid ATO. OpDivs should ensure that security authorization policies and procedures are fully developed and disseminated to the appropriate personnel to ensure that all OpDiv personnel understand the requirements for completing the ATO process.

   HHS Response: Concur

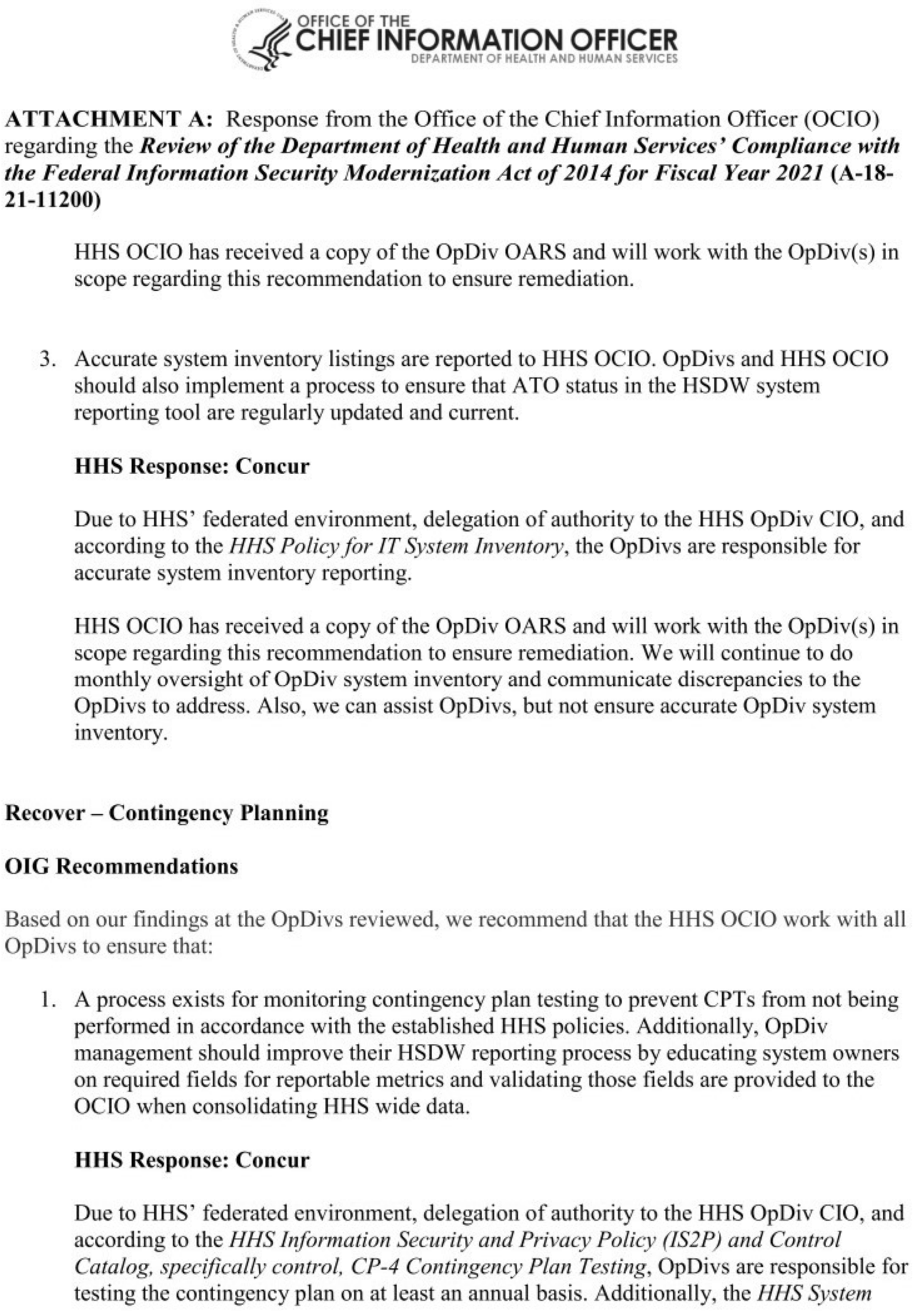
   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO, and according to the *HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control, CA-6 Security Authorizations*, the OpDivs are responsible for ensuring all systems on the network have a valid ATO, as well as having fully developed security authorization policies and procedures

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

2. ISCM strategy and procedures should clearly define critical reporting metrics for reports utilized by internal and external stakeholders. Additionally, OpDivs should coordinate reporting efforts with the OCIO to ensure the definitions and reporting requirements are consistently implemented.

   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*, the OpDivs are responsible for developing a continuous monitoring strategy and implementation of a continuous monitoring program.



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 2021*** **(A-18-21-11200)**

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

3. Accurate system inventory listings are reported to HHS OCIO. OpDivs and HHS OCIO should also implement a process to ensure that ATO status in the HSDW system reporting tool are regularly updated and current.

   HHS Response: Concur

   Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO, and according to the *HHS Policy for IT System Inventory*, the OpDivs are responsible for accurate system inventory reporting.

   HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope regarding this recommendation to ensure remediation. We will continue to do monthly oversight of OpDiv system inventory and communicate discrepancies to the OpDivs to address. Also, we can assist OpDivs, but not ensure accurate OpDiv system inventory.

Recover – Contingency Planning

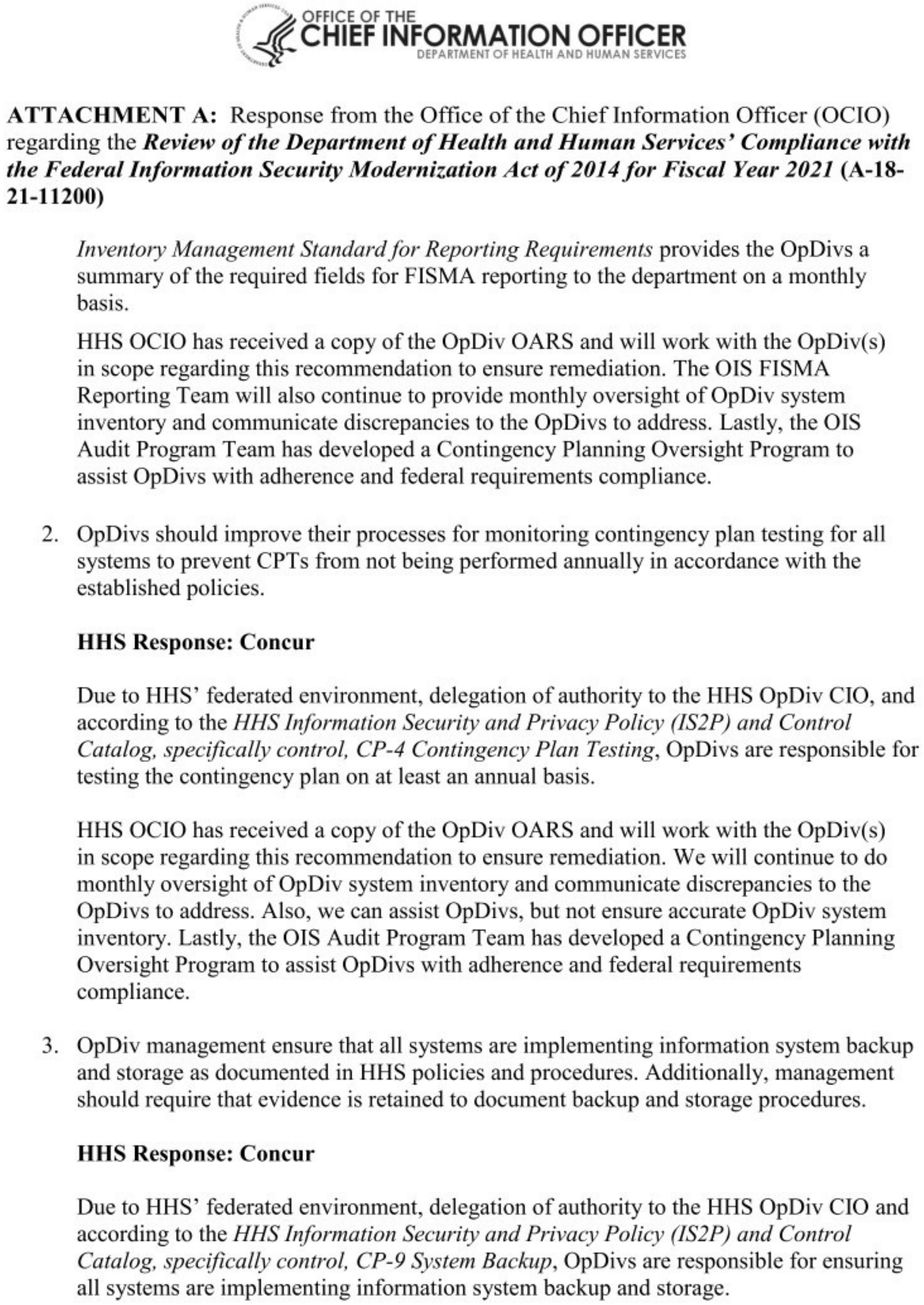
OIG Recommendations

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

1. A process exists for monitoring contingency plan testing to prevent CPTs from not being performed in accordance with the established HHS policies. Additionally, OpDiv management should improve their HSDW reporting process by educating system owners on required fields for reportable metrics and validating those fields are provided to the OCIO when consolidating HHS wide data.

   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, CP-4 Contingency Plan Testing*, OpDivs are responsible for testing the contingency plan on at least an annual basis. Additionally, the *HHS System*



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 2021*** **(A-18-21-11200)**

Inventory Management Standard for Reporting Requirements provides the OpDivs a summary of the required fields for FISMA reporting to the department on a monthly basis.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope regarding this recommendation to ensure remediation. The OIS FISMA Reporting Team will also continue to provide monthly oversight of OpDiv system inventory and communicate discrepancies to the OpDivs to address. Lastly, the OIS Audit Program Team has developed a Contingency Planning Oversight Program to assist OpDivs with adherence and federal requirements compliance.

2. OpDivs should improve their processes for monitoring contingency plan testing for all systems to prevent CPTs from not being performed annually in accordance with the established policies.

HHS Response: Concur

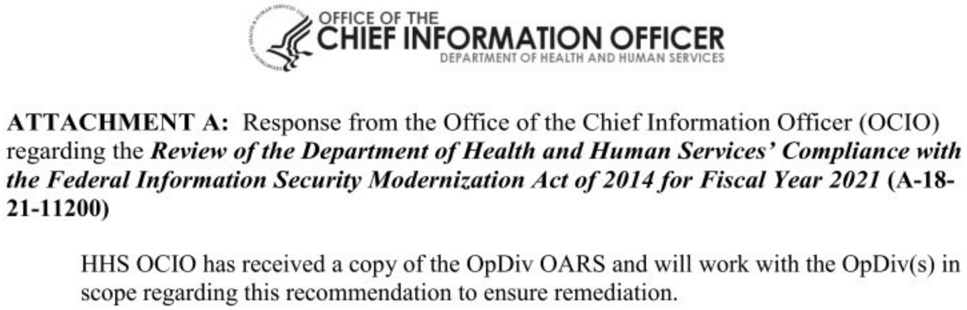
Due to HHS' federated environment, delegation of authority to the HHS OpDiv CIO, and according to the *HHS Information Security and Privacy Policy (IS2P) and Control Catalog, specifically control, CP-4 Contingency Plan Testing*, OpDivs are responsible for testing the contingency plan on at least an annual basis.

HHS OCIO has received a copy of the OpDiv OARS and will work with the OpDiv(s) in scope regarding this recommendation to ensure remediation. We will continue to do monthly oversight of OpDiv system inventory and communicate discrepancies to the OpDivs to address. Also, we can assist OpDivs, but not ensure accurate OpDiv system inventory. Lastly, the OIS Audit Program Team has developed a Contingency Planning Oversight Program to assist OpDivs with adherence and federal requirements compliance.

3. OpDiv management ensure that all systems are implementing information system backup and storage as documented in HHS policies and procedures. Additionally, management should require that evidence is retained to document backup and storage procedures.

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, CP-9 System Backup*, OpDivs are responsible for ensuring all systems are implementing information system backup and storage.



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 2021*** **(A-18-21-11200)**

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