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 2020

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 2021
A-18-20-11200

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.

Department of Health and Human Services

Federal Information Security Modernization Act Report

April 1, 2021

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

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

Building a better working world

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 2020 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, 2020, with the objective of assessing HHS' compliance with FISMA as defined in the FY 2020 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 alternatives 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 1, 2021

Report in Brief
Date: April 2021
Report No. A-18-20-11200

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

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020

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, 2020 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 HHS and 5 out of the 12 operating divisions (OpDivs); assessed the status of HHS' security program against HHS 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.

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 (1) the evaluation of HHS not meeting a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover function areas, (2) the deficiencies within the Identify, Protect and Respond function areas and (3) the evaluation of a maturity level below Consistently Implemented for some FISMA metric questions both at HHS overall and at selected operating divisions (OpDivs). 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. Also notable were increased maturation of data protection and privacy and information systems continuous monitoring. Weaknesses continue to persist in Contingency Planning, which was the only domain assessed with a maturity level of "Defined" in FY 19 and again in FY 20. We identified opportunities where HHS can strengthen its overall information security program.

What We Recommends and HHS Comments

We recommend that HHS further strengthen its cybersecurity program and enhance information security controls at HHS. Recommendations specific to a reviewed HHS OpDiv were provided to them separately.

HHS should 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. HHS' program should address gaps between the current maturity levels to the HHS-defined effective maturity level for each cybersecurity framework function areas. 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.

In written comments to our draft report, HHS concurred with 11 recommendations and did not concur with two recommendations. HHS also provided technical comments, which we addressed as appropriate. We maintain that our findings and recommendations are accurate and valid.

Table of Contents

Section 1: Background 1
- 1.1 Introduction 1
- 1.2 Background 1

Section 2: Conclusion and Enterprise-wide Recommendations 5
- 2.1 Conclusion 5
- 2.2 Recommendations 6

Section 3: Department and OpDiv Findings and Recommendations 9
- 3.1 Summary 9
- 3.2 Identify 9
- 3.3 Protect 11
- 3.4 Detect 17
- 3.5 Respond 18
- 3.6 Recover 20

Section 4: Appendices 22
- 4.1 Appendix A: Audit Scope and Methodology 22
- 4.2 Appendix B: Federal Requirements and Guidance 24
- 4.3 Appendix C: FY 2020 Inspector General FISMA Reporting Metrics 26
- 4.4 Appendix D: HHS Comments 55

Section 1
Background

1 Section 1: Background

1.1 Introduction

We conducted a performance audit of the Department of Health and Human Services' compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2020 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 2020 IG FISMA reporting metrics, issued April 17, 2020, in consultation with the Federal Chief Information Officers Council. These metrics leverage the *National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)* 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 2020 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 2020 metrics also mark a continuation of the work that OMB, DHS and CIGIE undertook in FY 2017 to transition the IG assessments to a

maturity model approach. This is the third year that all FISMA security domains were assessed using a maturity model.

For FY 2020, updates were made to the IG FISMA questions, as reported in the FY 2020 IG FISMA Reporting Metrics Version 4.0, dated April 17, 2020, which include:

- An additional focus on the security of mobile devices (Government Furnished Equipment (GFE) and non-GFE), particularly in the areas of mobile device management and enterprise mobility management. As such, the FY 2020 IG FISMA Reporting Metrics include updates to questions on asset management, security architecture, and flaw remediation to assess agency progress in securing mobile endpoints and employing secure application development processes.

- OMB Memorandum M-19-26, *Update to the Trusted Internet Connection (TIC) Initiative*, September 12, 2019 provides updated guidance to federal agencies on use of TIC capabilities in modern architectures and frameworks such as cloud environments. While the memorandum gave agencies until September 2020 to implement new TIC requirements, the IG FISMA metric on TIC implementation has been updated to assess agency's progress in planning for the effective implementation of the security capabilities outlined in M-19-26.

The FY 2020 IG FISMA Reporting Metrics are grouped into eight domains and organized around 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
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 2020 IG FISMA Metrics, a series of metrics (or questions) was developed for each IG FISMA domain (Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous

Monitoring, Incident Response, and Contingency Planning) to assess the effectiveness of an agency's cybersecurity framework (Identify, Protect, Detect, Respond, and Recover).

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.

Per OMB and DHS, within the context of the maturity model, Level 4 (Managed and Measurable) represents an "effective" level of security. However, DHS does allow OIG to deviate from the standard for determining the "effective" level of security when an agreed-upon methodology is determined. In FY 2020, we determined that control domains evaluated at the Consistently Implemented rating level may be considered "effective" when (1) no deficiencies are identified within the control domain and (2) the are no evaluations of a maturity level below Consistently Implemented for some FISMA metric questions within the control domain.

HHS Shared Responsibility Model

The HHS cybersecurity program follows a shared responsibility model that informally recognizes that the Department, the HHS OpDivs, and third-party stakeholders (including 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. Third-party stakeholders 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 criteria required for any of the five function areas: Identify, Protect, Detect, Respond and Recover. This determination was made based on (1) the evaluation of HHS not meeting a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover function areas, (2) the deficiencies identified within the Identify, Protect and Respond function areas, and (3) the evaluation of a maturity level below Consistently Implemented for individual metric questions both at HHS overall and at selected operating divisions (OpDivs).

Table 2 below provides a comparison from the FY 2019 and FY 2020 IG FISMA Metrics. In FY 2020, the HHS security program strengthened the maturity of its controls for several individual IG FISMA metrics. Areas where HHS improved in their performance from the prior year were in the consistent implementation of data exfiltration systems, ongoing Authorization to Operate (ATO) monitoring, and configuration management controls, specifically in the areas of baseline security standards and patch management. Areas where HHS' security program needed improvement are captured by our specific findings and enterprise-wide recommendations in Section 3.

Table 2: FY 2019 and 2020 HHS Maturity Levels

Maturity Level	FY 2019 IG FISMA Metrics	FY 2020 IG FISMA Metrics
Defined	17	17
Consistently Implemented	42	42
Managed and Measurable	0	0

Note: The IG FISMA metrics are the aggregation of the assessment results for HHS and the OpDivs reviewed.

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

HHS has created an enterprise-level ISCM strategy for OpDivs to assist with the implementation of CDM tools. HHS has not defined roadmaps, key performance indicators, or benchmarks for

CDM implementation within this strategy or other documentation. The Department recognizes limitations associated with the Security Governance, Risk and Compliance 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 established a monthly ISCM/CDM Working Group, where lessons learned inform implementation and improvements to its ISCM program. The DHS CDM program consists of three (3) different phases:

- Phase I – Focused on assets, identifying what resides on the agency's network.
- Phase II – Focused on access, identifying who is on the agency's network.
- Phase III - Focused on identifying and filling the gaps created by the previous phases.

HHS has not set a schedule to fully implement the CDM program phases and tools across all OpDivs. This has led to inconsistent maturity metrics across OpDivs and a lower maturity at the HHS enterprise versus the maturity level achieved by individual OpDivs.

2.2 Recommendations

To strengthen HHS' enterprise-wide cybersecurity program, we recommend that HHS:

1. Communicate to all stakeholders the roles and shared responsibilities that must be implemented to meet the requirements for an "effective" level of security in the context of the maturity model, including whether such requirements are to be implemented through centralized, federated, or hybrid controls. This should also include the responsibilities of the OCIO, the OpDivs, and third-party stakeholders (including contractors).

2. Continue implementation of an automated CDM solution that provides a centralized, enterprise-wide view of risks across the organization.

3. Develop oversight process and procedures to ensure comprehensive policies and procedures for managing the configurations of information systems are developed and tailored to the OpDivs environment.

4. Formalize policies, procedures, and processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to OpDiv systems.

5. Update the ISCM strategy to include a roadmap for complete deployment across all HHS OpDivs, and key performance indicators and benchmarks to facilitate the implementation of CDM toolsets across all OpDivs.

6. Increase focus on monitoring the status of ATO expirations across all OpDivs and ensuring that ATOs are reauthorized prior to their expiration dates.

7. Conduct an assessment of privileged IT staff to identify users with significant cybersecurity responsibilities and ensure they complete specialized role-based training.

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

HHS OCIO COMMENTS AND OFFICE OF INSPECTOR GENERAL REPONSE

HHS OCIO concurred with recommendations 1-4 and 6-8 and did not concur with recommendation 5.

While HHS OCIO agreed that they can be more verbose in the ISCM strategy about the requirements for enterprise tools, they believe the recommendation is misaligned. Specifically, they did not agree with the auditor's statements about CDM-specific roadmaps, key performance indicators (KPI), and benchmarks.

We believe that HHS management is responsible for establishing performance metrics and measures for CDM roll-out and adoption. HHS' management stance is it is individual OpDiv responsibilities. Through our review at the OpDivs, no such performance metrics or monitoring was required by the Department and the issue is pervasive across each OpDiv we reviewed. As a result, we issued the finding and recommendation as an enterprise issue to be address by the HHS OCIO. We maintain that our recommendation is valid.

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 eight domains. We also include recommendations that should assist the Department as they focus on achieving a higher maturity level.

Function	Identify	Protect				Detect	Respond	Recover
Domain	*Risk Management*	*Configuration Management*	*Identity & Access Management*	*Data Protection & Privacy*	*Security Training*	*ISCM*	*Incident Response*	*Contingency Planning*
OIG Assessed Maturity	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Defined (Level 2)
FY 2020 Audit vs FY 2019 Audit	No Change	No Change	No Change	No Change	No Change	No Change	No Change	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 is one domain, Risk Management, for evaluation within the IG metrics. 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 20 IG Assessment	Change from FY 19 IG Assessment
Identify	Risk Management	Consistently Implemented	No change

HHS' risk management function has the following in place:

- Established a risk management framework for evaluating and reporting risks.
- Categorization and communication of the importance/priority of information systems in enabling its missions and business functions.
- Uses an information security architecture to provide a disciplined and structured methodology for managing risk.
- Defined and communicated roles and responsibilities of internal and external stakeholders involved in risk management processes.
- Plans of action and milestones (POA&Ms) are utilized for mitigating security weaknesses.

The OCIO is responsible for ensuring that all of the OpDivs' systems are being reported to the OCIO, identifying high-value assets and appropriately reporting 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 Finding and Recommendations

The following findings were identified with HHS' risk management program:

- For five systems selected at one OpDiv, a security impact analysis (SIA) was not completed as required for all configuration change items by the OpDivs policy. The absence of a SIA being performed presents a risk that unknown or potentially harmful changes may be implemented into production.
- During our evaluation of the Risk Management Program in another OpDiv, there was no OpDiv-level strategy provided for risk management controls. The absence of an OpDiv-wide risk management strategy could lead to inconsistent risk management principles, policies, standards, and procedures across the OpDivs information technology environment. Further, it increases the risk that decisions made at the system level are not consistent with the requirements in place for the OpDiv, including those at the HHS entity-level.

We recommend that the HHS OCIO work with the OpDivs to:

- Develop a formal risk management strategy to establish, communicate, and implement its risk management controls, including for supply chain risk management. Additionally, within the Risk Management Strategy, the OpDiv should document procedures to ensure that all system owners have implemented processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk acceptance/tolerance levels, responding to risk, and monitoring risk.

- Update their configuration change control policy to (1) more accurately define the types of changes that require a SIA to be performed, and (2) for all unplanned and major changes as defined, perform the SIA and retain the resulting documentation in accordance with the OpDiv document retention requirements.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS OCIO has received a copy of the OpDiv findings and is coordinating a review of the specific findings. This will enable OCIO to track mitigation, evaluate trends, identify common issues, and assess if and/or procedures are adequate at both the Department and OpDiv level.

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.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 20 IG Assessment	Change from FY 19 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:

- Defined guidelines for the appropriate security configuration of information systems.
- Established roles and responsibilities to be implemented by OpDiv management.
- 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, OpDiv programs range from manual to automated.

HHS has made progress to stay in compliance with OMB Memorandum M-19-26 which was issued in September 2019. HHS is working to issue a new policy written with TIC 3.0 use cases and policy enforcement points as including inventorying for HHS OCIO and FISMA reporting.

Configuration Management Findings and Recommendations

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

- An OpDiv was unable to provide evidence of configuration item change request details or change control approvals for two selected contractor-owned and operated systems.
- At the same OpDiv, the submission, approval and implementation of the sampled changes was performed by the same individual for two selected government owned systems.

The absence of proper configuration change control activities such as appropriate segregation of duties, approval / disapproval with oversight from the configuration control board and retaining records of implemented changes can result in unauthorized and potentially harmful changes being implemented.

We recommend that the HHS OCIO work with the OpDivs to:

- Establish oversight procedures for contractor owned systems to ensure change control activities and record retention procedures are being implemented appropriately across all systems.
- Ensure that appropriate segregation of duties requirements is enforced for change control activities across all systems.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS OCIO has received a copy of the OpDiv findings and is coordinating a review of the specific findings. This will enable OCIO to track mitigation, evaluate trends, identify common issues, and assess if policies and/or procedures are adequate at both the Department and OpDiv level.

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 program with established roles and responsibilities.
- Use of an Identity, Credential and Access Management (ICAM) strategy is required to guide ICAM processes and activities.
- Defined ICAM policies and procedures that are required to be implemented.
- Use of access agreements, including non-disclosure agreements, acceptable-use agreements and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems.

Identity and Access Management Findings and Recommendations

The following finding was identified with OpDiv's identity and access management program:

- At one OpDiv, the OpDiv management was unable to provide evidence that contractors are complying with established screening criteria included within contractual requirements related to risk designations, appropriate screening, non-disclosure agreements (NDAs), rules of behavior, or acceptable use agreements for two selected users listed for two selected contractor systems.
- An OpDiv was unable to provide evidence of personnel risk designations for one user prior to granting access for one selected contractor system.
- One OpDiv was unable to provide evidence of (1) periodic review and adjustment (such as the removal/addition of roles or functionality for a user within the system to meet their job requirements) of privileged user accounts and permissions, and (2) that privileged user account activities are logged and periodically reviewed.

- At one OpDiv, management was unable to provide evidence of periodic access review for privileged system users. Management stated that there is no periodic review of users in place and such a process is being developed and implemented.

We recommend that the HHS OCIO work with the OpDivs to ensure that all OpDivs:

- Conduct periodic review and adjustment of privileged user accounts and permissions as required by OpDiv policy is being implemented consistently across all systems within the established time period. Additionally, the OpDiv should ensure that privileged user account activities are logged and periodically reviewed.

- Perform appropriate system user onboarding procedures and that appropriate records retention policies and procedures are in place and operating effectively. Although contractor management is responsible for performing the control, OpDiv management should have an oversight procedure in place to ensure that all contract requirements are being performed.

- Implement oversight of contractor system procedures to ensure that periodic user access reviews are performed and that privileged user account activities are logged and periodically reviewed. In addition, management should implement a review process for the monitoring activities by the Computer Security Incident Response Center (CSIRC) and DCIO Ops over government-owned systems with the OpDiv portfolio.

In addition, to ensure vulnerabilities were timely addressed, we provided specific findings, observations, and recommendations to the OpDivs.

HHS OCIO Response:

HHS OCIO concurred with our recommendation. HHS OCIO has received a copy of the OpDiv audit report and is coordinating a review of the specific finding. This will enable OCIO to track mitigation, evaluate trends, identify common issues, and assess if policies and/or procedures are adequate at both the Department and OpDiv level.

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 60 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.
- 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.
- Privacy awareness training is provided to individuals, including role-based privacy training.

For FY 2020, HHS had a smaller number of OpDiv's scoped for a data protection and privacy review. HHS has made progress regarding the Privacy Impact Assessments and ensuring that they are completed appropriately. While there are no specific findings regarding the HHS DPP domain, the enterprise recommendation captured in Section II Recommendation 1 and 3 should be adopted by HHS to demonstrate the overall effectiveness of the Cybersecurity Framework (CSF) Protect function.

Security Training

An effective IT security program cannot be established and maintained without giving a sufficient amount of 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:

- Use of a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to the HHS culture.
- Definition of security awareness and specialized security training policies and procedures, which are required to be implemented.
- Providing security awareness training to all system users that is tailored based on its organizational requirements, culture, and types of information systems.
- OCIO is working to finalize and implement more than 20 career paths. Additionally, the HHS Cybersecurity Workforce Development Group is in the process of developing plans to gain assurance around the utilization of the Career Paths and validating the NICE work role codes.

Security Training Findings and Recommendations

The following finding was identified with the OpDiv's security awareness training program:

- One OpDiv has not documented an up-to-date Security Training and Awareness Strategy. The Security Training Policy that was being used was dated September 04, 2013. In the past two (2) years, the OpDiv has stated the policy is being updated.

We recommend that the HHS OCIO work with the OpDivs to ensure that:

- All OpDivs complete an update of the Security Training Policy to incorporate current federal standards including an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the function areas of Identify, Protect, Detect, Respond, and Recover.

In addition, to ensure vulnerabilities were timely addressed, we provided specific findings, observations, and recommendations to the OpDivs.

HHS OCIO Response:

HHS OCIO concurred with our recommendation. OCIO has received a copy of the OpDiv audit report and is coordinating a review of the specific finding. This will enable OCIO to track mitigation, evaluate trends, identify common issues, and assess if security training policies and/or procedures are adequate at the Department and OpDiv levels.

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). 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 20 IG Assessment	Change from FY 19 IG Assessment
Detect	ISCM	Consistently Implemented	No Change

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

- Formalization of its ISCM program through development of ISCM policies, procedures, and strategies.
- Defined processes for 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.

While there were no specific findings regarding the HHS ISCM domain, the enterprise recommendation captured in Section II Recommendation 5 should be adopted by HHS to demonstrate the overall effectiveness of the Detect function area of the CSF.

3.5 Respond

The goal of the Respond function is to develop and implement the appropriate activities to take action 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".

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 20 IG Assessment	Change from FY 19 IG Assessment
Respond	Incident Response	Consistently Implemented	No Change

HHS' incident response function has the following in place:

- Established monitoring requirements for security incidents identified across the enterprise.
- Defined incident response policies, procedures, plans and strategies, as appropriate, to respond to cybersecurity events, which are required to be implemented.
- Defined and communicated incident response team structures/models, stakeholders and their roles, responsibilities, levels of authority and dependencies.

Incident Response Findings and Recommendations

In addition to the recommendations included within Section II, the following finding was identified with HHS' incident response program:

- HHS' incident response process to determine whether an event should be declared a "major incident" based on all of the criteria defined by OMB could be enhanced. Specifically, the process did not determine whether the incident had or may have had a perceived or actual impact to the American people's public confidence in US Government systems, their civil liberties, or their public health and safety. HHS' process relied upon DHS' Cybersecurity and Infrastructure Security Agency's (CISA) determination with no documentation of HHS leadership review and acceptance of that determination. It is the responsibility of each agency to assess and determine the incident level based on its mission and circumstances under which the incident occurred.

We recommend that the HHS OCIO work with its OpDivs to:

- Improve the incident evaluation process for determining whether an incident is major in accordance with the full OMB definition contained in the OMB FISMA guidance. This process should include a documented adjudication process that assesses the perceived or actual impact of the American people's public confidence in US Government systems, their civil liberties, or their public health and safety from the knowledge of the incident as noted in the OMB guidance.

HHS OCIO RESPONSE AND OFFICE OF INSPECTOR GENERAL REPONSE:

The HHS OCIO disagreed with our finding and recommendation. Specifically, the HHS OCIO identified that the HHS CSIRC has a Major Incidents Standard Operating Procedures (SOP) and develops an executive summary for incidents which details how the Major Incidents SOP is implemented. The CSIRC's documentation sets a clear escalation path for an incident to all leadership as well as coordination efforts with external entities (CISA, FBI, etc.). CSIRC developed a process, actively implements this process, and has never deferred to CISA for any determination; all of the aforementioned was included as evidentiary artifacts during the audit.

HHS's disagreement with our finding is rooted in the required criteria for the determination of a major incident per OMB Memorandum 20-04. The additional requirement in OMB Memorandum 20-04 related to the classification of "Major Incidents" that are "likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.". Our recommendation is focused on the enhancement of the process to include documentation to capture the internal sharing and acceptance of CISA determination for the Potential Impact category to be in line with HHS leaderships determination of potential impact of their mission and public confidence given real-time Department priorities within their enterprise risk management program. We maintain that our recommendation is valid.

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. 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 20 IG Assessment	Change from FY 19 IG Assessment
Recover	Contingency planning	Defined	No change

HHS' contingency planning function has the following in place:

- HHS has distributed its defined requirements to the OpDivs for implementation at the system level.
- HHS communicates information on the planning and performance of recovery activities to internal stakeholders and executive management teams that is used to make risk-based decisions.

While there are no specific findings regarding the HHS Contingency Planning domain during the audit, the OIG has noted findings around contingency planning in other audits. The enterprise recommendation captured in Section II Recommendation 8 should be adopted by HHS to demonstrate the overall effectiveness of the Recover function area of the CSF.

Section 4
Appendices

Appendix A
Audit Scope and Methodology

4 Section 4: Appendices

4.1 Appendix A: Audit Scope and Methodology

Scope

In tandem with the work being undertaken for the Chief Financial Officer audit, 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 2020 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 during the FY 2020 performance audit:

- Centers for Medicare & Medicaid Services (CMS)
- Agency for Healthcare Research and Quality (AHRQ)
- Food and Drug Administration (FDA)
- Office of the Secretary (OS)
- Substance Abuse and Mental Health Services Administration (SAMHSA)

For two (2) of the five (5) OpDivs selected, AHRQ and SAMHSA, we limited our review to selected domains. The selected domains included: 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 20 IG FISMA metrics. Incorporated the results as part of the FY 20 IG FISMA metrics.

- Inspected results from GAO and OIG audits and reports that had a similar scope to the FY 20 IG FISMA metrics. Incorporated the results as part of the FY 20 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 PUB 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 Office of Information Security, High Value Asset Program Policy (March 2018).
- HHS OCIO, Information Systems Security and Privacy Policy (July 30, 2014).
- HHS OCIO, HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII) (May 2020).
- HHS OCIO, HHS Policy for Privacy Impact Assessments (PIA) (June 4, 2019).
- HHS OCIO, HHS System Inventory Management Standard (December 27, 2018).
- HHS OCIO, Minimum Security Configuration Standards Guidance (October 5, 2017).
- HHS Plan of Action and Milestones Standards (POA&M) Version 2 (June 2019).
- Homeland Security Presidential Directive 12 (HSPD 12): Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004).
- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems (May 2010).
- NIST SP 800-37, revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (June 2014).

- 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-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements (October 16, 2017).
- US-CERT Federal Incident Notification Guidelines.

Appendix C
FY 2020 Inspector General FISMA Reporting Metrics

4.3 Appendix C: FY 2020 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 2020 FISMA audit results and narrative comments into the CyberScope system. The report begins on the following page.

Inspector General

Section Report

2020

Annual FISMA Report

Department of Health and Human Services

Function 1: 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 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity model 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; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2020 CIO FISMA Metrics: 1.2

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for this question. Four OPDIVs have consistently implemented a process 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 had an Ad Hoc process for using standard data elements to maintain an up-to-date inventory of hardware assets connected to its network.

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; NISTIR 8011; FEA Framework, v2; FY 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; CSF: ID.AM-2)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Two OPDIVs are at the Consistently implemented level and one is at the Ad Hoc level 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 defined a process of tracking and reporting software inventories connected to its network. Four OPDIVs did not ensure that the software assets on the network (and their associated licenses) are subject to the monitoring processes defined within the organization's ISCM strategy.

Function 1: Identify - Risk Management

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 2020 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Consistently Implemented (Level 3)

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

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 - 2; SECURE Technology Act: s. 1326, Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at managed and measurable and one OPDIV at Defined for this question. Three OPDIVs did not monitor and analyze its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines.

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); OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at defined for this question. Three OPDIVs did not integrate security architecture with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the organization's information systems.

Function 1: Identify - Risk Management

7 To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M-19-03)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Managed and Measurable. Three OPDIVs did not utilize an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.

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); OMB M-19-03, CSF v1.1, ID.RA-6)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for this question. For two OPDIVs, POA&Ms data were not consistently reported to HHS.

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system-level risks (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Managed and Measurable for this question. Two OPDIVs did not consistently monitor the effectiveness of risk responses to ensure that enterprise-wide risk tolerance is maintained at an appropriate level.

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for this question. Three OPDIVs did not employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization.

Function 1: Identify - Risk Management

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800-152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with 2 OPDIVs at Managed and Measurable for this question. Three OPDIVs did not use qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor information security performance of contractor-operated systems and services.

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level for this question. Four OPDIVs did not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data.

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Consistently Implemented (Level 3)

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

13.2 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?

The HHS risk management program is not effective since all aspects of its program are not at the Managed and Measurable maturity level. 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.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2A: Protect - Configuration Management

Function 2A: Protect - Configuration Management

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for ensuring that stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities.

15 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)?

Defined (Level 2)

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

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: 2.2.1)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Four OPDIVs did not monitor, analyze, and report on the qualitative and quantitative performance measures used to gauge the effectiveness of its configuration management policies and procedures and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

17 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 2020 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 for this question. For one OPDIV, baselines were not developed for platforms. Four OPDIVS did not employ automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.

Function 2A: Protect - Configuration Management

18 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 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 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. Four OPDIVs did not employ automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.

19 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 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OPDIV is Managed and Measurable and one OPDIV is Defined for this question. Two OPDIVs did not centrally manage its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe.

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

Consistently Implemented (Level 3)

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

21 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).

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level for this question. Two OPDIVs did not monitor, analyze, and report on the qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

Function 2A: Protect - Configuration Management

22 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?

The HHS configuration management program is not currently effective across HHS.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OPDIV is at the Defined level and three OPDIVs are at Consistently Implemented. Four OPDIVs did not ensure that stakeholders have adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level and Managed and Measurable at two OPDIV for this question. Three OPDIVs have not transitioned to its desired or "to-be" ICAM architecture and integrates its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture.

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Managed and Measurable and one OPDIV at Defined. Three OPDIVs did not use automated mechanisms (e.g. machine-based, or user based enforcement), where appropriate, to manage the effective implementation of its policies and procedures.

Function 2B: Protect - Identity and Access Management

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate 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)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level with one OPDIV at Consistently Implemented. Four OPDIVs did not employ automation to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate.

27 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 PS6)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Defined for this question. Three OPDIVs did not centrally manage user access agreements for privileged and non-privileged users.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Defined and one OPDIV at Managed and Measurable. Four OPDIVs did not ensure that all non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. Two OPDIVs are Defined and one OPDIV is Managed and Measurable for this question. Two OPDIVs did not ensure that all privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

Function 2B: Protect - Identity and Access Management

30 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 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level with one OPDIV at Consistently Implemented. Three OPDIVs did not employ automated mechanisms (e.g., machine-based, or user based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.

31 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-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10)?.

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Managed and Measurable. Three OPDIVs did not ensure that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.

32 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?

Overall, HHS's identity and access management program is not effective since it is not at the Managed and Measurable level across HHS.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2C: Protect - Data Protection and Privacy

Function 2C: Protect - Data Protection and Privacy

33 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); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with two OPDIVS at Managed and Measurable. For one OPDIV, system PIAs were not maintained during the appropriate timeframe. Three OPDIVs did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make appropriate adjustments as needed.

34 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 2019 CIO FISMA Metrics: 2.8; 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

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. One OPDIV does not ensure that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.

35 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 2019 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 for this question. Two OPDIVs did not measure the effectiveness of its data exfiltration and enhanced network defenses by conducting exfiltration exercises.

36 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 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Defined. One OPDIV did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan.

Function 2C: Protect - Data Protection and Privacy

37 To what degree 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)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Consistently Implemented and two OPDIVs at the Managed and Measurable level. One OPDIV did not measure 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.

38 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?

HHS's data protection and privacy program is not effective since all OPDIVs have not consistently implemented security controls to protect its PII and other sensitive data.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2D: Protect - Security Training

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Managed and Measurable and one OPDIV at Ad Hoc.

Function 2D: Protect - Security Training

40 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 at Consistently Implemented and one OPDIV is at Managed and Measurable. Two OPDIVs have not addressed all of their identified knowledge, skills, and abilities gaps through the training or hiring of additional staff/contractors.

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

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs at Managed and Measurable and one OPDIV at Defined. One OPDIV did not monitor and analyzes qualitative and quantitative performance measures on the effectiveness of their security awareness and training strategies and plans.

42 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs at Managed and Measurable. Two OPDIVs did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures.

Function 2D: Protect - Security Training

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 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. Two OPDIVs were Managed and Measurable and one OPDIV was Consistently Implemented. Two OPDIVs did not measure the effectiveness of its awareness training program.

44 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800- 53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level with one OPDIV at Managed and Measurable and one OPDIV at Consistently Implemented. Two OPDIVs did not obtain feedback on its security training content and make updates to their program and did not measure the effectiveness of its specialized security training program.

45.1 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.

45.2 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?

Overall, the security training program is not effective since it is not at the managed and measurable level across HHS.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 3: Detect - ISCM

46 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organizationwide approach to ISCM (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?.

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level with one OPDIV at Ad-Hoc. Three OPDIVs did not monitor and analyzes qualitative and quantitative performance measures on the effectiveness of the ISCM strategy.

Function 3: Detect - ISCM

47 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?.

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for this question. Three OPDIVs did not monitor and analyzes qualitative and quantitative performance measures on the effectiveness of the ISCM policies and procedures.

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; and FY 2019 CIO FISMA Metrics)?.

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs at Managed and Measurable. Two OPDIVs' staff did not consistently collect, monitor, and analyze qualitative and quantitative performance measures across the organization and reporting data on the effectiveness of the OPDIVs' ISCM program.

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (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); NISTIR 8011; OMB M-14-03; OMB M-19-03)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at Consistently Implemented. Four OPDIVs did not utilize the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.

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

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity levels for this question. Two OPDIVs did not integrate metrics on the effectiveness of the ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains.

51.1 Please provide the assessed maturity level for the agency's Detect Function.

Consistently Implemented (Level 3)

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

Function 3: Detect - ISCM

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?

Since HHS and its OPDIVs are not at the Managed and Measurable level, overall, the ISCM program is not effective.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M- 17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. One OPDIV did not monitor and analyzes qualitative and quantitative performance measures on the effectiveness of incident response policies, procedures, plans, and strategies.

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 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 with two OPDIVs at Managed and Measurable. Two OPDIVs have not assigned responsibility for monitoring and tracking the effectiveness of incident response activities. Additionally, incident response functions that are incorporated in high level IT infrastructure budgets result in inconsistent/inaccurate budget allocation tracking.

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-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-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 for this question. One OPDIV did not utilize profiling techniques to measure the characteristics of expected activities on their networks and systems so that they can more effectively detect security incidents.

Function 4: Respond - Incident Response

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 for this question. One OPDIV did not manage and measure the impact of successful incidents in order to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.

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-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs at Managed and Measurable. Two OPDIVs did not measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

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-18-02; PPD-41).

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs at Managed and Measurable. Two OPDIVs did not utilize Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.

58 To what degree 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 with one OPDIV at Managed and Measurable. Two OPDIVs did not use technologies for monitoring and analyzing qualitative and quantitative performance across the organization and are not collecting, analyzing, and reporting data on the effectiveness of their technologies for performing incident response activities.

Function 4: Respond - Incident Response

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

Consistently Implemented (Level 3)

Comments: HHS is at the Consistently Implemented maturity level.

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?

Since not all HHS OPDIVs are at the Managed and Measurable level, the HHS incident response program is not effective.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

60 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1 and CP-2; 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 for this question. Four OPDIVs have not allocated resources in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

61 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800- 161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5).

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level for this question. One OPDIV did not manage their information and communications technology (ICT) supply chain risks related to contingency planning activities.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level for this question. Four OPDIVs did not incorporate the results of organizational and system level BIAs into strategy and do not plan development efforts consistently.

Function 5: Recover - Contingency Planning

63 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 2019 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 with two OPDIVs at Consistently Implemented. Two OPDIVs did not integrate metrics on the effectiveness of their information system contingency plans with information on the effectiveness of related plans.

64 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 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level with three OPDIVs rated at Consistently Implemented. Four OPDIVs did not employ automated mechanisms to thoroughly and effectively test system contingency plans.

65 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 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. Two OPDIVs did not consistently implement their processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites.

66 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)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level for this question. For two OPDIVs, metrics on the effectiveness of recovery activities were not communicated to relevant stakeholders and the organization had not ensured that the data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

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

Defined (Level 2)

Comments: HHS and its OPDIVs have not consistently implemented its contingency planning functions, therefore HHS is at the Defined level.

Function 5: Recover - Contingency Planning

67.2 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?

HHS and its OPDIVs have not consistently implemented its contingency planning functions, therefore HHS's contingency planning program is not effective.

Calculated Maturity Level - Defined (Level 2)

Function 0: Overall

Function 0: Overall

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

Not Effective

Comments:

Overall, while HHS was evaluated at the same level in FY20 and FY19 across the function domains, we noted improvement in their program which has strengthened the enterprise-wide information security program. Through the evaluation of FISMA metrics, it was determined that the HHS' information security program was 'Not Effective'. This determination was made based on (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 within the Identify, Protect and Respond functional areas, (3) the lack of Managed and Measurable ratings to mitigate the Consistently Implemented ratings in control domains that were further evaluated for effectiveness and (4) the evaluation of a maturity level below consistently implemented for individual metric questions both at HHS overall and at selected operating divisions (OPDIVs). HHS is cognizant of opportunities which arise to strengthen the overall information security program which 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 information security program are in the ISCM and Contingency Planning domains. For ISCM, HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (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. Based on our assessment, the Governance, Risk and Compliance tools continue to be implemented across the OPDIVs. The HHS FY20 strategy supported clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, mission/business impacts and the use of RSA Archer and Splunk to support the Department's efforts with implementing an effective CDM program. In the area of Contingency Planning, HHS was evaluated at the Defined level and should work with OPDIVs and system owners to consistently implement the established program. 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, Identity and Access Management, Security Training, Configuration Management, Data Protection & Privacy, 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 0: Overall

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.

·Do not include the names of specific independent auditors, these entities should be referred to as "independent assessor" or "independent auditor"

·The assessment of effectiveness should not include a list of ratings by NIST CSF Function-level, as these will already be included in the performance summary

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, Protect, Detect, Respond, and Recover functional areas. In addition to the HHS Office of the CIO, the following five HHS OPDIVs were in-scope for this assessment: Centers for Medicare & Medicaid Services, Food and Drug Administration, Agency for Healthcare Research and Quality, Substance Abuse and Mental Health Services Administration, and the Office of the Secretary. Three of the five OPDIVs in scope this year were not reviewed last year. We also incorporated results from other IT audits and assessments. We performed a review of HHS' and OPDIVs' policies, procedures, standards and other guidance, as well as examined corresponding artifacts.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	10
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	3
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Overall, HHS is at the Consistently Implemented level for its Risk Management program.
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)	Consistently Implemented (Level 3)	Overall, HHS is at the Consistently Implemented maturity level for the Detect function.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	HHS is at the Consistently Implemented maturity level.
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	HHS and its OPDIVs have not consistently implemented its contingency planning functions, therefore HHS is at the Defined level.

Overall	Not Effective	Not Effective	Overall, while HHS was evaluated at the same level in FY20 and FY19 across the function domains, we noted improvement in their program which has strengthened the enterprise-wide information security program. Through the evaluation of FISMA metrics, it was determined that the HHS' information security program was 'Not Effective'. This determination was made based on (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 within the Identify, Protect and Respond functional areas, (3) the lack of Managed and Measurable ratings to mitigate the Consistently Implemented ratings in control domains that were further evaluated for effectiveness and (4) the evaluation of a maturity level below consistently implemented for individual metric questions both at HHS overall and at selected operating divisions (OPDIVs). HHS is cognizant of opportunities which arise to strengthen the overall information security program which 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 information security program are in the ISCM and Contingency Planning domains. For ISCM, HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (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. Based on our assessment, the Governance, Risk and Compliance tools continue to be implemented across the OPDIVs. The HHS FY20 strategy supported clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, mission/business impacts and the use of RSA Archer and Splunk to support the Department's efforts with implementing an effective CDM program. In the area of Contingency Planning, HHS was evaluated at the Defined level and should work with OPDIVs and system owners to consistently implement the established program. 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, Identity and Access Management, Security Training, Configuration Management, Data Protection & Privacy, 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.

Appendix D
HHS Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

Office of the Chief Information Officer
Assistant Secretary for Administration
Washington, D.C. 20201

DATE: March 10, 2021

TO: Tamara Lilly, Assistant Inspector General for Audit Services

FROM: Perryn B. Ashmore, Chief Information Officer *Perryn Ashmore* Perryn Ashmore (Mar 8, 2021 10:07 EST)

SUBJECT: Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020 (A-18-20-11200)

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) 2020. We welcome the opportunity to respond to the report developed by Ernest & Young on your behalf.

As requested, our office has reviewed the aforementioned report and has attached written comments regarding the validity of facts, actions taken and planned actions, based on your recommendations. We look forward to continuing our collaboration efforts to enhance information technology security and further implement safeguards and practices that protect HHS data and the health information of the American public.

If you have any questions or need additional information, please reach out to the HHS Chief Information Security Officer, Janet Vogel at Janet.Vogel@hhs.gov or 202-774-2446.

Attachment A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020 (A-18-20-11200)***

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

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

February 24, 2021
OCIO Response to *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020* for
Engagement Number: A-18-20-11200

ATTACHMENT A

Enterprise-wide Recommendations

To strengthen HHS' enterprise-wide cybersecurity program we recommend that HHS:

1. Communicate to all stakeholders the roles and shared responsibilities that must be implemented to meet the requirements for an "effective" level of security in the context of the maturity model, including whether such requirements are to be implemented through centralized, federated, or hybrid controls. This should also include the responsibilities of the OCIO, the OpDivs, and third-party stakeholders (including contractors).

   HHS Response: Concur

   Upon completion of the organization-wide risk assessment, the effective maturity level for HHS will be determined. HHS will develop a roadmap, metrics, key performance indicators (KPI), and key risk indicators that will determine if its cybersecurity program is advancing from its current maturity state to an improved and appropriate level of maturity.

2. Continue implementation of an automated CDM solution that provides a centralized, enterprise-wide view of risks across the organization.

   HHS Response: Concur

   HHS is reliant on DHS for CDM implementation and will continue collaboration.

3. Develop oversight process and procedures to ensure comprehensive policies and procedures for managing the configurations of information systems are developed and tailored to the OpDivs environment.

   HHS Response: Concur

   The *HHS Minimum Security Configurations Standards & Guidance* provides standards for configuration management and recommends use of the checklists available at the National Checklist Program (NCP) Repository to configure operating systems, applications, and devices. The document will be updated this calendar year.

   Due to HHS' federated environment and according to the *HHS Information Security and Privacy Policy (IS2P)*, the OpDivs are responsible for developing and tailoring configuration management documentation for their OpDiv environment. The OCIO will look into how oversight will be provided.

1

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

February 24, 2021
OCIO Response to *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020* for
Engagement Number: A-18-20-11200

4. Formalize policies, procedures, and processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to OpDiv systems.

   HHS Response: Concur

   The *HHS IS2P* has requirements on personnel security including position risk designations and personnel screening (PS-2 and PS-3 on page 175). These requirements will be updated with the updates of the *HHS IS2P* which is anticipated to be completed in Q4 FY21. OpDivs will be responsible for formalizing policies, procedures, and processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to OpDiv systems.

5. Update the ISCM strategy to include a roadmap for complete deployment across all HHS OpDivs, and key performance indicators and benchmarks to facilitate the implementation of CDM toolsets across all OpDivs.

   HHS Response: Non-Concur

   While HHS agrees that we can be more verbose in the ISCM strategy about the requirements for enterprise tools, we believe the recommendation is misaligned. Specifically, we do not agree with the auditor's statements about CDM-specific roadmaps, key performance indicators (KPI) and benchmarks.

   The strategy and program plan does state what enterprise tool types should be implemented. HHS will include a more specific roadmap with objectives for HHS-wide ISCM across the enterprise; however, they will not be specific to CDM. Due to HHS' federated environment, we cannot force the OpDivs to use specific CDM tools or control how much they mature those tools.

6. Increase focus on monitoring the status of ATO expirations across all OpDivs and ensuring that ATOs are reauthorized prior to their expiration dates.

   HHS Response: Concur

   The *HHS (IS2P)*, Page 87, CA-1 Security Assessment and Authorization Policies and Procedures, mandates OpDiv systems and networks be formally assessed and authorized using the methods defined in *NIST SP 800-37 (Rev. 1); Guide for Applying the Risk Management Framework to Federal Information Systems* at least every three (3) years.

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

February 24, 2021
OCIO Response to *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020* for
Engagement Number: A-18-20-11200

HHS will continue to provide oversight through FISMA reporting and the HHS Data Warehouse (HSDW) reports but ultimately the OpDivs hold responsibility for managing their system ATOs.

7. Conduct an assessment of privileged IT staff to identify users with significant cybersecurity responsibilities and ensure they complete specialized role-based training.

   HHS Response: Concur

   This requirement is addressed in the HHS memorandum, *Requirements for Role-Based Training of Personnel with Significant Security Responsibilities*. Due to HHS' federated environment, the OpDivs are responsible for assessing privileged IT staff to identify users with significant responsibilities and ensure they complete specialized role-based training.

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

   HHS Response: Concur

   The OCIO will develop a process to ensure information system contingency plans are developed, maintained, and integrated with other continuity requirements by information systems. In addition, The *HHS (IS2P), Page 111, CP-2 Contingency Plan*, mandates information system contingency plans are developed in accordance with *NIST SP 800-34, Contingency Planning Guide for Information Technology (IT) Systems.*

Department and OpDiv Findings and Recommendations

Identity - Risk Management

OIG Recommendation:

We recommend that the HHS OCIO work with the OpDivs to:

- Develop a formal risk management strategy to establish, communicate, and implement its risk management controls, including for supply chain risk management. Additionally, within the Risk Management Strategy, the OpDiv should document procedures to ensure that all system owners have implemented processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk acceptance/tolerance levels, responding to risk, and monitoring risk.

- Update their configuration change control policy to (1) more accurately define the types

February 24, 2021
OCIO Response to *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020* for
Engagement Number: A-18-20-11200

of changes that require a SIA to be performed, and (2) for all unplanned and major changes as defined, perform the SIA and retain the resulting documentation in accordance with the OpDiv document retention requirements.

HHS Response: Concur

HHS OCIO has received a copy of the OpDiv audit report and is coordinating a review of the specific findings. This will enable us to track mitigation, evaluate trends, identify common issues and assess if and/or procedures are adequate at both the Department and OpDiv level.

Protect - Configuration Management

OIG Recommendation:

We recommend that the HHS OCIO work with the OpDivs to:

- Establish oversight procedures for contractor owned systems to ensure change control activities and record retention procedures are being implemented appropriately across all systems.

- Ensure that appropriate segregation of duties requirements is enforced for change control activities across all systems.

HHS Response: Concur

HHS OCIO has received a copy of the OpDiv audit report and is coordinating a review of the specific findings. This will enable us to track mitigation, evaluate trends, identify common issues and assess if policies and/or procedures are adequate at both the Department and OpDiv level.

Protect - Identity and Access Management

OIG Recommendation:

We recommend that the HHS OCIO work with the OpDivs to ensure that all OpDivs:

- Conduct periodic review and adjustment of privileged user accounts and permissions as required by OpDiv policy is being implemented consistently across all systems within the established time period. Additionally, the OpDiv should ensure that privileged user account activities are logged and periodically reviewed.

- Perform appropriate system user onboarding procedures and that appropriate records

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

February 24, 2021
OCIO Response to *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020* for
Engagement Number: A-18-20-11200

retention policies and procedures are in place and operating effectively. Although contractor management is responsible for performing the control, OpDiv management should have an oversight procedure in place to ensure that all contract requirements are being performed.

- Implement oversight of contractor system procedures to ensure that periodic user access reviews are performed and that privileged user account activities are logged and periodically reviewed. In addition, management should implement a review process for the monitoring activities by the Computer Security Incident Response Center (CSIRC) and DCIO Ops over government-owned systems with the OpDiv portfolio.

In addition, to ensure vulnerabilities were timely addressed, we provided specific findings, observations, and recommendations to the OpDivs.

HHS Response: Concur

HHS OCIO has received a copy of the OpDiv audit report and is coordinating a review of the specific finding. This will enable us to track mitigation, evaluate trends, identify common issues and assess if policies and/or procedures are adequate at both the Department and OpDiv level.

Protect - Security Training

OIG Recommendation:

We recommend that the HHS OCIO work with the OpDivs to ensure that:

- All OpDivs complete an update of the Security Training Policy to incorporate current federal standards including an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the function areas of Identify, Protect, Detect, Respond, and Recover.

In addition, to ensure vulnerabilities were timely addressed, we provided specific findings, observations, and recommendations to the OpDivs.

HHS Response: Concur

OCIO has received a copy of the OpDiv audit report and is coordinating a review of the specific finding. This will enable us to track mitigation, evaluate trends, identify common issues and assess if security training policies and/or procedures are adequate at the Department and OpDiv levels.

Respond - Incident Response

OIG Recommendation:

We recommend that the HHS OCIO work with its OpDivs to:

- Improve the incident evaluation process for determining whether an incident is major in accordance with the full OMB definition contained in the OMB FISMA guidance. This process should include a documented adjudication process that assesses the perceived or actual impact of the American people's public confidence in US Government systems, their civil liberties, or their public health and safety from the knowledge of the incident as noted in the OMB guidance.

HHS Response: Non-Concur

The HHS CSIRC has a Major Incidents Standard Operating Procedures (SOP) and develops an executive summary for incidents which details how the Major Incidents SOP is implemented. CSIRC's process documents the event in question, lists all actions taken, and outlines the severity so the stakeholders can make an informed decision. The CSIRC's documentation sets a clear escalation path for an incident to all leadership as well as coordination efforts with external entities (CISA, FBI, etc). HHS and OpDivs utilize the seven (7) day window to evaluate the impact to HHS and externally (public confidence), at which point the Major Incident classification is determined. CSIRC developed a process, actively implements this process, and has never deferred to CISA for any determination; all of the aforementioned was included as evidentiary artifacts during the audit.