

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 2018**

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



**Gloria L. Jarmon
Deputy Inspector General
for Audit Services**

**April 2019
A-18-18-11200**

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 assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at <https://oig.hhs.gov>

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

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

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



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

Ms. Amy J. Frontz
Assistant Inspector General for Audit Services
Office of the Inspector General
Wilbur J. Cohen Building
330 Independence Avenue, SW
Washington, D.C. 20201

March 29, 2019

Dear Ms. Frontz:

Attached is our final report on audit procedures performed in accordance with *Government Auditing Standards* on the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) in accordance with the FY 2018 Inspector General FISMA Reporting Metrics (reporting metrics).

Our procedures were designed to respond to the reporting metrics and not for the purpose of expressing an opinion on internal control or the effectiveness of the entire information security program. Accordingly, we do not express an opinion on internal control or the effectiveness of HHS' information security program.

Our audit procedures were performed to provide our report as of September 30, 2018. The projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the information security program or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

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.

Sincerely,



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

Report of Independent Auditors on HHS' Compliance with the Federal
Information Security Modernization Act of 2014 for Fiscal Year 2018
Based on a Performance Audit Conducted in Accordance
with *Government Auditing Standards*

Ms. Amy J. Frontz
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, 2018, with the objective of assessing HHS' compliance with FISMA as defined in the FY 2018 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

March 29, 2019

Report in Brief

Date: April 2019

Report No. A-18-18-11200

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



Why We Did This Review

The Federal Information Security Modernization Act of 2014 (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 such programs and practices. OIG engaged Ernst & Young LLP to conduct this review.

We conducted a performance audit of HHS' compliance with FISMA as of September 30, 2018 based upon the questions outlined in the FISMA reporting metrics for the Inspectors General.

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

How We Did This Review

We reviewed applicable Federal laws, regulations, and guidance; gained an understanding of the current security program at HHS and selected 4 out of the 12 operating divisions (OPDIV); assessed the status of HHS' security program against HHS and selected OPDIV information security program policies, other standards and guidance issued by HHS management, and prescribed performance measures; inquired of personnel to gain an understanding of the FISMA reporting metric areas; and inspected selected artifacts.

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018

What We Found

Overall, HHS continues to implement changes to strengthen its enterprise-wide information security program. We identified opportunities where HHS can strengthen their overall information security program. HHS continues to work toward implementing a Department-wide Continuous Diagnostics and Mitigation program with the Department of Homeland Security. This should help HHS achieve a higher level of maturity for its information security program in subsequent years. Additionally, we identified weaknesses in the following areas: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

HHS needs to ensure that all OPDIVs consistently review and remediate or address the risk presented by vulnerabilities discovered, consistently implement account management procedures, and accurately track systems to ensure they are operating with a current and valid Authority to Operate. Additionally, the Department should focus on configuring recently deployed continuous diagnostic monitoring tools to automate the integration of cyber risks into newly developed enterprise risk management programs. These steps will strengthen the program and further enhance the HHS mission.

What We Recommend and HHS Comments

We recommend that HHS further strengthen its information security program. We made a series of recommendations to enhance information security controls at HHS, specific recommendations were also provided to the OPDIVs.

HHS concurred with all of our recommendations and described the actions it is taking and plans to take to implement them. HHS also provided technical comments, which we addressed.

Table of Contents

Introduction	1
Section I — Background	1
Section II — Conclusion	4
Section III — Findings and Recommendations	5
Identify	5
Risk Management.....	5
Protect.....	6
Configuration Management.....	7
Identity and Access Management	8
Data Protection and Privacy	9
Security Training	10
Detect.....	11
Information Security Continuous Monitoring	11
Respond	12
Incident Response.....	13
Recover	13
Contingency Planning	14
Appendix A: Audit Scope and Methodology.....	16
Appendix B: Federal Requirements and Guidance	18
Appendix C: FY 2018 Inspector General FISMA Reporting Metrics	19
Appendix D: HHS Comments	46

Introduction

We conducted a performance audit of the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2018 based upon the questions outlined in the FISMA reporting metrics for the Inspectors General (IG).

Section I — Background

On December 17, 2002, the President signed the FISMA 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 amendments 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 through 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 the FISMA, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2018 IG FISMA reporting metrics, issued May 24, 2018, 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 such program and practices, including (1) testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems; and (2) an assessment of the effectiveness of the information security policies, procedures and practices of the agency. The FY 2018 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 2018 metrics also mark a continuation of the work that OMB, DHS, and CIGIE undertook in the past (4) years to move the IG assessments to a maturity model approach. This is the second year that all FISMA security domains were assessed using a maturity model. For FY 2018, updates were made to the IG FISMA questions

including the addition of questions to assess the mitigation of supply chain risk and the Data Protection and Privacy domain. The FY 2018 IG FISMA Reporting Metrics are grouped into eight metric 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 domain
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 FY 2018 IG FISMA Metrics, a series of metrics (or questions) were developed for each IG FISMA domain (Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring (ISCM), Incident Response, and Contingency Planning) to assess the effectiveness of an agency’s cybersecurity framework function (Identify, Protect, Detect, Respond, and Recover). The maturity level scoring was prepared by OMB and DHS. 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.

Level 1 (Ad-hoc) is the lowest security function and Level 5 (Optimized) is the highest maturity level. Within the context of the maturity model, Level 4 (Managed and Measurable) represents an effective level of security.

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

The Office of the Chief Information Officer (OCIO) serves this mission by leading 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; IT security and privacy; performance measurement; policies to provide improved management of information resources and technology; strategic development and application 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. The HHS enterprise-wide information security and privacy program is designed to help protect HHS against potential IT threats and vulnerabilities. This program plays an important role in protecting HHS' ability to provide mission-critical operations by providing a baseline for security and privacy policies and guidance; overseeing the guidance and completion of privacy impact assessments, providing incident reporting, policy and incident management guidelines, and promoting IT security awareness and training.

Each Operating Division's (OPDIV) CIO is responsible for establishing, implementing, and enforcing an OPDIV-wide framework to facilitate its information security program based on guidance provided by the HHS CIO and CISO. The OPDIV CISOs are responsible for implementing Department and OPDIV IT security policies and procedures.

Section II — Conclusion

Our specific conclusions related to HHS' information security program for each of the FISMA domains are contained within the FISMA reporting metrics in Appendix C. ¹ Overall, HHS continues to implement changes to strengthen its enterprise-wide information security program.

This year's assessment demonstrates the improvements in both the Identify and Protect function areas from previous years while the Respond function area maturity rating was lowered from FY 17. Based on the results of our evaluation, we determined that HHS' information security program was 'Not Effective' as it did not meet the 'Managed and Measurable' level in the following functional areas: Identify, Protect, Detect, Respond, and Recover. HHS is a federated environment which brings challenges in attaining a "Managed and Measurable" maturity model for all OPDIVs. We assessed Identify and Protect at the "Consistently Implemented" level, with Detect, Respond, and Recover being assessed at the "Defined" level.

HHS is aware of the opportunities that will strengthen its overall information security program to ensure that OPDIVs are consistently implemented in areas of its security program. To achieve this, HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program in coordination with DHS to include continuous monitoring of its networks and systems, documenting OPDIVs' progress to address and implement strategies, and reporting its progress through DHS dashboards. Attaining a "Managed and Measurable" maturity level is dependent on the full implementation of CDM, which has its own challenges. Through the full implementation of the CDM program, HHS hopes to gain ongoing, data driven insights into cyber risks and achieve managed and measurable maturity levels across the cybersecurity framework functions.

However, we have identified some opportunities that will strengthen the overall information security program, which should allow HHS to achieve a higher level of maturity for each domain and function. HHS needs to continue to build towards a working model where all the functional areas interact with each other in real-time and provide holistic and coordinated responses to security events. This will be achieved as HHS deploys the CDM tools, continues to modernize their IT processes and optimize their security controls, as a result of the data generated and monitored by the CDM tools. We continued to identify weaknesses in each of the five Cybersecurity framework areas: Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training), Detect (ISCM), Respond (Incident Response), and Recover (Contingency Planning).

¹ The FY 2018 IG FISMA Reporting Metrics are assessed based on a selection of HHS OPDIVs and the aggregation of their results. The FY 2017 and FY 2018 IG FISMA reporting metrics may not be comparable since this year one of the OPDIVs reviewed was not assessed in FY 2017. Also, the scope of testing of some of the FY 2018 IG FISMA reporting metrics differed from the testing in FY 2017, which can affect the IG assessment of the individual metrics and the overall assessment of each FISMA domain and function.

Section III — Findings and Recommendations

This report consolidates findings identified at the Department level and each of the selected OPDIVs reviewed. Vulnerabilities with sensitive information are not highlighted in this report. However, risks were communicated to HHS and appropriate OPDIV management.

We identified several reportable exceptions in HHS' security program. The exceptions have been consolidated into each of the eight function areas below:

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 was one domain, Risk Management, for evaluation within the IG metrics. Our overall assessment of this function was "Not Effective." Identified below are the findings and recommendations associated with that domain.

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 plans; 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 18 IG assessment
Identify	Risk Management	Consistently Implemented

HHS's risk management function has the following in place:

- ▶ Established a risk framework for evaluating and reporting risks.
- ▶ Provided an overarching IT strategy to OPDIVs to guide leaders as they make risk decisions.
- ▶ HHS Office of the CISO hosts monthly meetings to communicate emerging risks and trends to individual OPDIVs.
- ▶ Selected OPDIVs followed the defined process for identification, assessment, response, and monitoring of IT risks.

The OCIO is responsible for ensuring that each of the OPDIVs systems are being tracked at the Department, identifying high value assets, and appropriately reporting plan of action and milestones (POA&Ms). OPDIVs are responsible for the implementation of the risk management program, which includes the assessment or risk, monitoring of vulnerabilities, and the resolution of security weaknesses.

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

- ▶ Department standards and OPDIV strategies for how to handle and address risk were not always followed or updated. Specifically we noted that at one OPDIV, the lack of a formal strategy resulted in many POA&Ms not being reported to HHS.
- ▶ A process for tracking and reporting systems and software inventories needed improvement. Specifically, we noted one OPDIV lacked a process for identifying software installed on various IT platforms, as a result, one of the selected systems had not been incorporated into the overarching Department's risk management program.

The lack of a formal communication strategy of POA&M status by the OPDIV to the Department may result in vulnerabilities not being adequately and timely addressed. Without an effective program to identify and define all system inventories, HHS and its OPDIVs may not be able to protect their information systems, which exposes the Department to additional vulnerabilities. OPDIVs being unaware of illegally copied or outdated software that was installed by its employees and/or contractors could occur.

Recommendations:

In order to move HHS toward an effective risk management domain, we recommend that the HHS OCIO continue to:

- ▶ Work with OPDIVs to enhance its enterprise risk management strategy and program to integrate governance functions for information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas. These enhancements should include the integration of threat modeling for dynamic risk assessments and appropriate reporting tools to timely respond to new threats as they arise.
- ▶ Develop an approach for the Department to ensure that CDM tools, Security Governance, Risk management, and Compliance (sGRC) tools, and associated processes are implemented at all OPDIVs for the integration of risk management programs at the enterprise, business process, and information system levels to ensure consistency with OMB, NIST, and Department guidelines and requirements.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. sGRC tool deployment is underway at the Department and the OPDIVs. The new CDM tools are being implemented to enhance security continuous monitoring efforts and achieve visibility into all HHS assets, vulnerabilities, and security threats. With the implementation of these new tools, relevant policies, procedures, and guidance would be updated to reflect the new processes and capabilities that are consistent with OMB, NIST and Department guidelines and requirements.

HHS OCIO is coordinating a review of the specific OPDIV findings. This will enable OCIO to track mitigation, evaluate trends, identify common issues and assess if configuration policies and/or procedures are adequate at the OPDIVs.

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 18 IG assessment
Protect	Configuration Management	Defined
	Identity and Access Management	Consistently Implemented
	Data Protection and Privacy	Consistently Implemented
	Security Training	Consistently Implemented

Identified below are the findings and recommendations associated with those domains.

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’s configuration management function has the following in place:

- ▶ Defined guidelines for the appropriate security configuration of information systems.
- ▶ Established roles and responsibilities to be implemented at the OPDIVs.

Each OPDIV is responsible for the development of product specific baselines, implementation of those baselines and monitoring to determine the appropriate response to misconfigurations. For these areas we noted that while HHS and its OPDIVs are in the process of deploying common toolsets and processes, they were not fully implemented to allow for a consistent implementation of the HHS configuration management guidelines.

Based on the complexity of the system and associated architectures, individual OPDIVs and system owners can make risk based decisions when implementing HHS requirements. OPDIV established programs range from being manual to automated to monitor compliance.

The following findings were identified with HHS’ configuration management activities:

- ▶ At one OPDIV, a large number of vulnerabilities, which had been identified were not being resolved within the timelines established by HHS guidelines.
- ▶ Platforms being utilized by one OPDIV did not have security configuration requirements evaluated against established standards to confirm they were secure before deployment.
- ▶ One OPDIV had numerous IT assets deployed with security configurations that were no longer being supported by the vendor to address emerging cyber threats.

OPDIVs that do not detect and resolve known security vulnerabilities will be left exposed, thus compromising their confidentiality, integrity, and availability of their information assets.

Recommendations:

In order to move HHS toward an effective configuration management domain, we recommend that the HHS OCIO continue to:

- ▶ Work with OPDIVs to leverage qualitative and quantitative performance measures to determine the effectiveness of OPDIVs' configuration management plans. These measures should be based on results from automated toolsets to determine security misconfigurations, unsupported information system components, and effectiveness of flaw remediation processes. Define the timeframe for OPDIV communication of the performance measures to the OCIO.
- ▶ Implement the approach for the Department to fully implement CDM tools, sGRC tools, and process tools to consistently record, implement, and maintain configuration controls, baseline configurations of its information systems, and an inventory of related components.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

HHS CIO concurred with our recommendations. Some OPDIVs are currently awaiting deployment of tools provided by DHS as part of the CDM program. These tools will assist in the effective management of configuration baselines, tracking hardware assets, managing patches, and tracking end of life maintenance support. sGRC tool deployment is underway at the Department and the OPDIVs. This tool will enhance the OCIO's ability to document, track and evaluate trends and common issues.

HHS OCIO is coordinating a review of the specific OPDIV findings. This will enable OCIO to track mitigation, evaluate trends, identify common issues and assess if configuration policies and/or procedures are adequate at the OPDIVs.

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's identity and access management function has the following in place:

- ▶ Has a defined identity, credential, and access management program with established roles and responsibilities.
- ▶ OPDIVs have implemented HHS requirements to establish identity and access management controls.
- ▶ OPDIVs are on track with the implementation of strategic guidance for their information systems.

However, HHS does not have a consistent toolset to conduct real time monitoring or measure effectiveness across OPDIVs.

The following findings were identified with HHS's identity and access management program:

- ▶ At one OPDIV, appropriate user agreements were not maintained for some of the selected users.
- ▶ At one OPDIV, the implementation of two factor authentication could not be verified for some of the selected systems.

Without properly maintaining user agreements, HHS may not be able to enforce legal responsibilities on users who violated security policies. The lack of two factor authentication for systems may increase the risk of inappropriate access to the HHS network, information systems, and data resulting in the potential loss, destruction or misuse of sensitive data and resources.

Recommendations:

In order to move HHS toward an effective identity and access management domain, we recommend that the HHS OCIO continue to:

- ▶ Work with OPDIVs to determine the effectiveness of identity and access management processes. These measures should monitor OPDIVs' implementation of strong authentication techniques for all privileged and non-privileged users.
- ▶ Assist OPDIV implementation of "to-be" Identity, Credential, and Access Management (ICAM) architecture and integration of their ICAM strategy and activities within its enterprise and Federal ICAM segment architecture.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. OCIO is coordinating a review of the specific OPDIV findings. This will enable OCIO to track mitigation, evaluate trends, identify common issues and assess if enterprise identity and access management 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. The underlying principle of data privacy and protection controls are 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's data protection and privacy function has the following in place:

- ▶ HHS has a defined privacy program including a defined plan and guidelines.
- ▶ The guidelines have been communicated to the OPDIVs.
- ▶ The OPDIVs we reviewed had a process in place for the development of privacy impact assessments, standard controls to be implemented, and breach response processes, established roles and responsibilities, security requirements, and an enterprise breach response process for monitoring.
- ▶ 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.

- ▶ Each OPDIV had integrated privacy controls within their risk management process and reporting vulnerabilities and weaknesses accordingly.

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

- ▶ The Department did not document their review and updates for the guidance associated with the privacy based risk assessments to reflect the current environment.
- ▶ One OPDIV's guidance and requirements to address data protection and privacy controls was not updated within two years as required by HHS.
- ▶ Security requirements outlined in privacy impact assessments were outdated or incomplete.

Recommendation:

In order to move HHS toward an effective data protection and privacy domain, we recommend that the HHS OCIO continue to:

- ▶ HHS OCIO update relevant Department policies, procedures, and guidance.
- ▶ Work with the OPDIVs to measure the effectiveness of privacy specific controls and trainings through tracked breaches and maintain current privacy related documentation.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. OCIO is currently updating relevant policies and procedures to reflect any new terminology, processes and procedures.

HHS OCIO is coordinating a review of the specific OPDIV findings. 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 OPDIVs.

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 environments and secured physical locations without providing their personnel adequate security training.

HHS security training accomplishments:

- ▶ HHS has established security and training content, requirements for varying level of individuals based on their access, and completed workforce assessments.
- ▶ OPDIVs have a security and training program, which included monitoring and tracking of users who needed additional training to meet requirements.
- ▶ OPDIVs are responsible for reporting workforce shortfalls to HHS and discussing security training requirements and their associated training budget at the monthly CISO Council meetings.

The following findings were identified within HHS' security training program:

- ▶ At one OPDIV, guidance and requirements associated with training had not been defined, including a security training strategy. Specifically, some users had not completed the

required annual training to make them aware of current cyber threats, trends, and recommended actions.

Users who are unaware of their security responsibilities and/or have not received adequate security training may not be properly equipped to effectively perform their assigned duties which increases the risk of causing a computer security incident. This could lead to the loss, destruction, or misuse of sensitive Federal data.

Recommendation:

We recommend that HHS OCIO continue to work with the OPDIV to assign the necessary personnel to monitor compliance with the security awareness and training program.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. OCIO is coordinating a review of the specific OPDIV findings. 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 OPDIVs.

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) domain. Our overall assessment of this function was “Not Effective”. Identified below are the findings and recommendations associated with this domain.

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 18 IG assessment
Detect	Information Security Continuous Monitoring	Defined

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

- ▶ The “HHS Information Security Continuous Monitoring Strategy” was released in May 2017 to define and communicate the enterprise ISCM strategy.
- ▶ HHS has formalized its ISCM program through development of ISCM policies, procedures, and strategies.

The following findings were identified as they relate to HHS’s information security continuous monitoring program:

- ▶ The Department did not currently know the effectiveness of CDM tools leveraged by the OPDIVs to determine authorized assets on the network.
- ▶ At one OPDIV, some systems were operating with an expired Authorization to Operate (ATO).
- ▶ At one OPDIV, security control assessments were not always performed within the three (3) year HHS requirement.

Without a Department-wide, fully-implemented enterprise-level ISCM program, HHS and its OPDIVs do not have a complete list of required processes to protect their information assets. This includes current ATOs and completion of security control assessments. As a result, potential high-risk threats may not be detected. This security risk could lead to unauthorized access or changes to information systems, and misuse, compromise, or loss of confidential data and resources.

Recommendations:

In order to move HHS toward an effective ISCM domain, we recommend that the HHS OCIO continue to:

- ▶ Provide department-wide guidance and DHS-supplied CDM tools to each OPDIV for the implementation of their ISCM programs. This should include periodic reporting requirements and metrics to monitor real time threats identified by the Computer Security Incident Response Center (CSIRC) across the HHS enterprise.
- ▶ Enhance OPDIVs security continuous monitoring efforts to maintain visibility into IT assets, be aware of all vulnerabilities, be informed about security threats, and verify that all software assets are scanned on the network on a regular basis, as required.
- ▶ Assist OPDIVS in maintaining and managing system ATOs and security control assessments per the HHS policy and guidelines.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS. However, additional guidance from DHS is still outstanding on ISCM elements and requirements. This guidance is a critical input that will allow HHS to finalize and fully implement their continuous monitoring strategy. The implementation of the sGRC tool will enhance the OPDIVs' and OCIO's ability to centrally track and report information systems.

HHS OCIO is coordinating a review of the specific OPDIV findings. This will enable OCIO to track mitigation, evaluate trends, identify common issues and assess if ISCM policies and/or procedures are adequate at the OPDIVs.

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 their incident response program. The domain within this function is incident response. Our overall assessment of this

function was “Not Effective”. Identified below are the findings and recommendations associated with that domain.

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 areas	IG FISMA domain	FY 18 IG assessment
Respond	Incident Response	Defined

HHS’s incident response function has the following in place:

- ▶ HHS has established monitoring requirements for security incidents identified across the enterprise.
- ▶ The OPDIVs we reviewed utilized its common attributes to classify incidents and implement its processes for incident detection, analysis, and prioritization.

The following findings were identified with HHS’s incident response program:

- ▶ At one OPDIV, guidelines and requirements for reporting suspected security incidents to the HHS CSIRC did not include sufficient detail to validate timeliness of resolution.

Recommendation:

We recommend that the HHS OCIO work with the OPDIV to improve enforcement and communication of the incident response program organization wide. Improvements should focus on measuring consistent profiling techniques and improve communication between the CSIRC, OPDIVs, and components.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

HHS OCIO concurred with our recommendations. OCIO is coordinating a review of the specific findings. This will enable OCIO to track mitigation, evaluate trends, identify common issues and assess if incident response policies and/or procedures are adequate at the OPDIVs.

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”. Identified below are the findings and recommendations associated with that domain.

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 areas	IG FISMA domain	FY 18 IG assessment
Recover	Contingency Planning	Defined

HHS contingency planning function has the following in place:

- ▶ HHS has defined a continuity program, established roles and responsibilities, and contingency planning requirements.
- ▶ HHS has distributed their defined requirements to the OPDIVs for implementation at the system level.

Procedures related to recovery of mission essential and business functions are designated as the primary responsibility of the OPDIVs for implementation. Our analysis at select OPDIVs and systems identified the following findings:

- ▶ Three OPDIVs had not consistently implemented their information system contingency planning program through communication of current policies, procedures, and strategies to information system owners.
- ▶ Two OPDIVs had not updated their Continuity of Operations frameworks, policies, or procedures to reflect their current mission and business environment. This led to a lack of current policies and procedures being maintained by system owners.
- ▶ At one OPDIV, business impact analysis or adequate back up procedures were not completely documented for some of the selected FIPS 199 High or Moderate availability systems.
- ▶ Testing procedures related to contingency planning did not have adequate reconstitution activities documented or executed for some of the selected FIPS 199 High or Moderate availability systems.
- ▶ Adequate alternative processing sites with geographical dispersion were not implemented for some of the selected FIPS 199 High availability systems.

Without implementing effective security controls for the contingency planning process, critical data and operations may not be recoverable timely in the event of a true disaster or emergency. Without consistently updating the contingency planning functions, system owners and its users may be unaware and unprepared to address the current threats that may significantly impact the information system security.

Recommendations:

In order to move HHS toward an effective contingency planning domain, we recommend that the HHS OCIO continue to Assist OPDIVs in the implementation of a monitoring program that

identifies metrics based on defined mission and business risk. The program should validate OPDIVs implementation of contingency planning policies, procedures, and strategies in the following areas: conducting business impact analysis, conducting contingency plan testing, implementing information system backup and storage requirements, incorporating supply chain risks and the selection of alternative processing sites.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS OCIO Response:

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

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's compliance with FISMA. To assess HHS's 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 2018 IG FISMA reporting metrics were assessed at selected HHS OPDIVs and based on the aggregation of their results.

We performed our fieldwork at the HHS OCIO and four HHS OPDIVs during the FY 2018 performance audit:

- ▶ Centers for Medicare & Medicaid Services
- ▶ Food and Drug Administration (FDA)
- ▶ National Institutes of Health
- ▶ Office of the Secretary

The FY 2017 and FY 2018 IG FISMA reporting metrics may not be comparable since this year one of the OPDIVs reviewed (FDA) was not assessed in FY 2017. Also, the scope of testing of some of the FY 2018 IG FISMA reporting metrics differed from the testing in FY 2017, which can affect the IG assessment of the individual metrics and the overall assessment of each FISMA domain and function.

Additionally, we followed up with the Centers for Disease Control and Prevention on the status of FY 2018 Government Accountability Office report findings. We did not review the overall internal control structure for HHS.

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's security program against HHS and selected OPDIV information security program policies, other standards and guidance issued by HHS management, and reporting metrics.
- ▶ Inspected 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 HHS and OPDIVs managements that had a similar scope to the FY 18 IG FISMA metrics. Incorporated the results as part of the FY 18 IG FISMA metrics.
- ▶ Inspected results from GAO and OIG audits and reports that had a similar scope to the FY 18 IG FISMA Metrics. Incorporated the results as part of the FY 18 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

The principal criteria used for this audit included:

- ▶ *CMS The Risk Management Handbook Volume 1 Chapter 1 Risk Management XLC* (November 8, 2012);
- ▶ 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 OCIO, *Information Systems Security and Privacy Policy* (July 30, 2014);
- ▶ HHS Standard for Plan of Action and Milestones (POA&M) Management & Reporting (September 4, 2013);
- ▶ 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 2015/April 2013);
- ▶ NIST SP 800-61, *Computer Security Incident Handling Guide* (August 2012);
- ▶ *OS Server Patch Management Process, Standard Operating Procedures* (June 16, 2017)
- ▶ *OS Procedures Handbook for Information Security* (June 29, 2017)
- ▶ 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*
- ▶ *FDA Information System Security and Privacy Policy (IS2P)* (September 13, 2017)
- ▶ *Information Security Services Continuity of Operations Handbook* (June 1, 2018)

Appendix C: FY 2018 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 2018 FISMA audit results and narrative comments into the CyberScope system.

Inspector General

Section Report

2018

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: CA-3, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. HHS has a process 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 connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2; FY 2018 CIO FISMA Metrics: 1.2)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. Three of the four OPDIVs reviewed 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. However, the four OPDIVs reviewed did not ensure that the hardware assets connected to the network are subject to the monitoring processes defined within the organization's ISCM strategy (Managed and Measurable level).

- 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: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. One OPDIV reviewed is at the Consistently Implemented 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. The four OPDIVs reviewed 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 (Managed and Measurable level). The OPDIVs have initiatives, such as implementing CDM tools and processes, in order to move them to a Consistently Implemented maturity level.

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 (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level 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 that 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: 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; FY 2018 CIO FISMA Metrics: 1.6)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. Two OPDIVs reviewed are at the Managed and Measurable level. Two OPDIVs did not monitor and analyze its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines. The continued rollout of RSA Archer should enable HHS to move all OPDIVs to a Managed and Measurable level for its risk assessment program.

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 (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. One OPDIV is at the Managed and Measurable level. 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.

Function 1: Identify - Risk Management

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: CA-5; OMB M-04-25)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. Each OPDIV uses specific tools in order to manage the tracking and mitigation of security weaknesses. Three OPDIVS reviewed are at the Managed and Measurable level using new CDM tools to monitor and analyze qualitative and quantitative performance measures.

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 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. Two OPDIVs reviewed were at the Managed and Measurable level. Two OPDIVs reviewed did not consistently monitor the effectiveness of risk responses to ensure that enterprise-wide risk tolerance is maintained at an appropriate level. The implementation of CDM tools will help with monitoring the effectiveness of risk responses across HHS.

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))?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed did not employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization (Managed and Measurable level). The implementation of dashboards and reporting tools will help facilitate a portfolio view of interrelated risks across HHS in order to reach a managed and measurable maturity level.

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 (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at the Consistently Implemented maturity level. Two OPDIVs are at the Managed and Measurable level.

- 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)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at the Consistently Implemented maturity level. The OPDIVs reviewed 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 (Managed and Measurable level). HHS has invested in RSA Archer to provide a centralized, enterprise wide view of risks across the organization.

- 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 maturity 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 risk management it is not at a 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 all of 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: CM-1; NIST SP 800-128: Section 2.4)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. Two OPDIVs reviewed are at the Consistently Implemented level for ensuring that stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities. HHS is implementing CDM tools and RSA Archer so that metrics can be maintained on the effectiveness of information systems 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: CM-9)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. HHS has not consistently implemented an enterprise wide configuration management plan to monitor, analyze, and report to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan. HHS is implementing CDM tools and RSA Archer at all OPDIVs that should enable HHS to reach at least the Consistently Implemented maturity level.

- 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: CM-1; NIST SP 800-128: 2.2.1)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. One OPDIV is at the Consistently Implemented level. Three OPDIVs reviewed did not consistently implement its policies and procedures for managing the configurations of its information systems. The four OPDIVs reviewed did not monitor, analyze, and report on the qualitative and quantitative performance measures on 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 (Managed and Measurable level). The ODPIVs are implementing CDM tools, RSA Archer, and process tools in order to consistently record, implement, and maintain configuration control, baseline configurations of its information systems, and an inventory of related components.

Function 2A: Protect - Configuration Management

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: CM-2 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. The four OPDIVs reviewed did not employ automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its networks and then take immediate actions to limit any security impact (Managed and Measurable level).

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. One OPDIV is at the Managed and Measurable level and one OPDIV is at the Consistently Implemented level. Three OPDIVs reviewed 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 (Managed and Measurable level).

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. One OPDIV is at the Consistently Implemented level. The four OPDIVs reviewed did not centrally manage its flaw remediation process and utilize automated patch management and software update tools for operating systems, where such tools are available and safe. HHS has initiatives in order to automate and manage flaw remediation and patch management (Managed and Measurable level).

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Consistently Implemented (Level 3)

Comments:

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

Function 2A: Protect - Configuration Management

- 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: CM-2 and CM-3)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at the Consistently Implemented maturity level. The four OPDIVs reviewed did not monitor, analyze, and report on the qualitative and quantitative performance measures on the effectiveness of its change control activities and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format (Managed and Measurable level). The OPDIVs are implementing CDM tools and processes which should allow them to reach a Managed and Measurable maturity level.

- 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 at the Defined maturity level, therefore is not currently effective across HHS.

Calculated Maturity Level - Defined (Level 2)

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: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. The OCIO and OPDIVs reviewed have defined and communicated roles and responsibilities at the organizational and information systems levels for stakeholders involved in ICAM. One OPDIV is at the Consistently Implemented level since they ensure that stakeholders have adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities.

Function 2B: Protect - Identity and Access Management

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

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. One OPDIV reviewed is at the Consistently Implemented level and one OPDIV is at the Managed and Measurable level. The four OPDIVs reviewed have not transitioned to its desired or "to-be" ICAM architecture and has not integrated its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture (Managed and Measurable level).

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: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3).

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed 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 (Managed and Measurable level). The OCIO and OPDIVs are implementing tools and processes in order to reach the Managed and Measurable maturity level.

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: PS-2 and PS-3; National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. The OPDIVs are implementing CDM tools and RSA Archer in order to achieve automation to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate (Managed and Measurable level).

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: AC-8, PL-4, and PS-6)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level where access agreements for individuals are completed prior to access being granted. However the OPDIVs reviewed did not centrally manage user access agreements for privileged and non-privileged users (Managed and Measurable level).

Function 2B: Protect - Identity and Access Management

- 28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed did not ensure that all non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems (Managed and Measurable level).

- 29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. One OPDIV is at the Managed and Measurable level. Three OPDIVs reviewed did not ensure that all privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

- 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 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), and AC-17; CSIP)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. Two OPDIVs are at the Consistently Implemented level. Four OPDIVs reviewed 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 (Managed and Measurable level).

Function 2B: Protect - Identity and Access Management

- 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: AC-17 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at the Consistently Implemented maturity level. One OPDIV is at the Managed and Measurable level. Three OPDIVs reviewed did not ensure that end user devices have been appropriately configured prior to allowing remote access and restrict the ability of individuals to transfer data accessed remotely to non-authorized devices (Managed and Measurable level).

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

Calculated Maturity Level - Consistently Implemented (Level 3)

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; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at the Consistently Implemented maturity level for its privacy program.

Function 2C: Protect - Data Protection and Privacy

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; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

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 though two OPDIVs are at the Consistently Implemented level. The four OPDIVs reviewed did 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 (Managed and Measurable level).

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. One OPDIV reviewed measures 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: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. The OCIO has defined and communicated its Data Breach Response Plan. While one OPDIV has consistently implemented the Plan and one OPDIV is at the Managed and Measureable level, it is not consistently implemented across HHS.

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: 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 the Consistently Implemented maturity level. Two OPDIVs reviewed are at the Managed and Measurable level. Some OPDIVs 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 (Managed and Measurable level).

- 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: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at the Consistently Implemented maturity level. HHS has assigned responsibility for monitoring and tracking the effectiveness of its security awareness and training program.

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: 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. Two OPDIVs are at the Consistently Implemented level since they have conducted an assessment of the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and have identified its skills gaps.

- 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: AT-1; NIST SP 800-50: Section 3).

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at Consistently Implemented maturity level. Two OPDIVs are at the Managed and Measurable level and one OPDIV is at the Defined level.

- 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: AT-1 through AT-4; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at the Consistently Implemented maturity level. While the OCIO and three OPDIVs reviewed were at the Managed and Measurable level, one OPDIV was at the Defined level since they relied on the Department's policies and procedures for security awareness and had not developed their own.

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: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Managed and Measurable (Level 4)

Comments:

Overall, HHS is at the Managed and Measurable maturity level. While the OCIO and three OPDIVs reviewed measures the effectiveness of its security awareness program, one OPDIV did not.

- 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: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Managed and Measurable (Level 4)

Comments:

Overall, HHS is at the Managed and Measurable maturity level. However, one OPDIV did not obtain feedback on its security training content and make updates to its 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 the Protect function. HHS and its OPDIVs have defined, and in many cases consistently implemented or managed and measured its configuration management, identity and access management, data protection and privacy, and security training programs. Due to the federated nature of HHS, not all OPDIVs are at the same maturity level for each of the Protect domains.

- 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 at HHS is effective.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 3: Detect - ISCM

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 organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. The OCIO and one OPDIV reviewed are at the Defined level, while two OPDIVS reviewed were at the Consistently Implemented level and one OPDIV was at the Managed and Measurable level. Three OPDIVs did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of the ISCM strategy (Managed and Measurable level).

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: CA-7) (Note: The overall maturity level should take into consideration the maturity of question 49)?

Defined (Level 2)

Comments:

Overall, HHS is at the Defined maturity level. HHS has defined and communicated ISCM policies and procedures. Two OPDIVs are further ahead - one OPDIV is at the Consistently Implemented level and one OPDIV is at the Managed and Measurable level. Three OPDIVs did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of the ISCM policies and procedures (Managed and Measurable level).

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: CA-1; NIST SP 800-137; and FY 2018 CIO FISMA Metrics)?

Defined (Level 2)

Comments:

Overall, HHS is at the Defined maturity level. HHS has defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders and levels of authority and dependencies. Two OPDIVs are further ahead - one at the Consistently Implemented level and one at the Managed and Measurable level.

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: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Defined (Level 2)

Comments:

Overall, HHS is at the Defined maturity level. While two OPDIVs reviewed are at the Consistently Implemented level, at the other two OPDIVs reviewed, security control assessments have not been consistently implemented for all systems. The OCIO uses quarterly reports and dashboard reports to view the progress of information security administration at the OPDIVs.

Function 3: Detect - ISCM

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 the Defined maturity level. HHS has identified and defined the performance measures and requirements that are used to assess the effectiveness of its ISCM program. HHS has defined the format and frequency of reports and the tools used to provide information to individuals with significant security responsibilities. One OPDIV is further ahead at the Managed and Measurable level. The implementation of CDM tools and RSA Archer at all OPDIVs should help move HHS to the next maturity level.

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

Defined (Level 2)

Comments:

Since HHS and its OPDIVs reviewed are not consistently implementing its ISCM program, the ISCM program is at the Defined maturity level.

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?

While HHS has defined its ISCM processes, not all OPDIVs are consistently implementing them. Therefore, overall, the HHS ISCM program is not effective.

Calculated Maturity Level - Defined (Level 2)

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: 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: 4.1, 4.3, 4.6, and 5.3; 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. Three OPDIVs reviewed are at the Managed and Measurable level in implementing its incident response policies and procedures.

Function 4: Respond - Incident Response

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: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. One OPDIV is further along at the Managed and Measurable level. Three OPDIVs have not assigned responsibility for monitoring and tracking the effectiveness of incident response activities (Managed and Measurable level).

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; and US-CERT Incident Response Guidelines)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. One OPDIV is further along at the Managed and Measurable level. At most OPDIVs reviewed, they consistently utilize its threat vector taxonomy to classify incidents and implement its processes for incident detection, analysis, and prioritization. However, they 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 (Managed and Measurable level).

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?

Consistently Implemented (Level 3)

Comments:

Overall, HHS is at a Consistently Implemented maturity level. HHS consistently implements its incident handling with the Department's Computer Security Incident Response Center (CSIRC) that all OPDIVs report incidents to.

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: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. While one OPDIV is at the Consistently Implemented level and one OPDIV is at the Managed and Measurable level, at some OPDIVs there was not a consistent method of OPDIV communication with CSIRC or consistently shared information with all of its internal stakeholders.

Function 4: Respond - Incident Response

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 (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. One OPDIV is at the Consistently Implemented level and one OPDIV is at the Managed and Measurable level. HHS utilizes DHS's Einstein program for intrusion detection/prevention capabilities.

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)

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. Two OPDIVs reviewed are at the Defined maturity level and two OPDIVs are at the Managed and Measurable level.

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

Defined (Level 2)

Comments:

While HHS's CSIRC manages and measures security incidents from all HHS OPDIVs, not all OPDIVs are consistently implementing its incident response program. Therefore the incident response program is at a Defined 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?

The HHS incident response program is not effective due to the fact that not all HHS OPDIVs are consistently implementing its incident response program.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

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: 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. HHS has defined roles and responsibilities and communicated them across the organization.

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; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. The four OPDIVs reviewed did not consistently implement its contingency planning policies, procedures, and strategies. HHS also did not manage their information and communications technology 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: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. One OPDIV is further along at the Consistently Implemented level. Three OPDIVs did not incorporate the results of organizational and system level BIAs into strategy and did not plan development efforts consistently (Consistently Implemented level).

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: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Defined (Level 2)

Comments:

Overall, HHS is at a Defined maturity level. Two OPDIVs are at the Consistently Implemented level. The four OPDIVs reviewed did not integrate metrics on the effectiveness of their information system contingency plans with information on the effectiveness of related plans (Managed and Measurable level).

Function 5: Recover - Contingency Planning

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: CP-3 and CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. The OPDIVs did not consistently implement contingency plan testing and exercises.

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: 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 2018 CIO FISMA Metrics: 5.4; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: Overall, HHS is at a Defined maturity level. 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: CP-2 and IR-4)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is at a Consistently Implemented maturity level. For the four OPDIVs reviewed, metrics on the effectiveness of recovery activities were not communicated to relevant stakeholders and the OPDIVs had not ensured that the data supporting the metrics was obtained accurately, consistently, and in a reproducible format (Managed and Measurable).

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.

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 it 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, HHS continues to implement changes to strengthen its enterprise-wide information security program. Based on the results of our evaluation, we determined that HHS' information security program was 'Not Effective' since it was not at a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover functional areas. HHS continues to be aware of the opportunities to strengthen its overall information security program to ensure that its policies and procedures at all Operating Divisions (OPDIVs) are consistently implemented in all areas of its security program. HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program in coordination with DHS to include continuous monitoring of its networks and systems, documenting OPDIVs' progress to address and implement strategies, and reporting its progress through DHS dashboards. The CDM program is in the final stages of being fully implemented at all OPDIVs. Additionally, HHS needs to ensure that there is effective contingency planning, identity and access management, configuration management, and incident response through the use of appropriate tools, processes, and controls at all OPDIVs. HHS also needs to continue to build towards a working model where all the functional areas interact with each other in real-time and provide holistic and coordinated responses to security events helping to strengthen all aspects of its information security program. These steps will help HHS achieve its mission through an effective and coordinated information security program.

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.

In order 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 for the Inspector General. We assessed the maturity levels and effectiveness across the Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, Data Protection & Privacy, and Security Training), Detect (Information Security Continuous Monitoring (ISCM)), Respond (Incident Response), and Recover (Contingency Planning) functional areas. In addition to the HHS Office of the CIO, the following four HHS OPDIVs were in-scope for this assessment: Centers for Medicare & Medicaid Services, Food & Drug Administration, National Institutes of Health, and Office of the Secretary. Additionally, follow-up was conducted with Centers for Disease Control and Prevention on the status of FY 2017 Government Accountability Office FISMA related findings. We also incorporated results from other IT audits and assessments. We performed an inspection of HHS' and OPDIVs' policies, procedures, standards and other guidance, as well as inspection of corresponding artifacts.

APPENDIX A: Maturity Model Scoring**Function 1: Identify - Risk Management**

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	11
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	6
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	0

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2C: Protect - Data Protection and Privacy

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

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	3
Managed and Measurable	2
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

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

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	0

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 maturity 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 the Protect function. HHS and its OPDIVs have defined, and in many cases consistently implemented or managed and measured its configuration management, identity and access management, data protection and privacy, and security training programs. Due to the federated nature of HHS, not all OPDIVs are at the same maturity level for each of the Protect domains.
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	Since HHS and its OPDIVs reviewed are not consistently implementing its ISCM program, the ISCM program is at the Defined maturity level.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Defined (Level 2)	While HHS's CSIRC manages and measures security incidents from all HHS OPDIVs, not all OPDIVs are consistently implementing its incident response program. Therefore the incident response program is at a Defined 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	

Appendix D: HHS Comments




DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the Chief Information Officer
Assistant Secretary for Administration
Washington, DC 20201

DATE: February 4, 2019

TO: Gloria L. Jarmon
Deputy Inspector General for Audit Services

FROM: Edwin Simcox
Chief Technology Officer and Acting Chief Information Officer 
Edwin Simcox (Feb 25, 2019)

SUBJECT: Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018 (A-18-18-11200)

The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) thanks the Office of the Inspector General (OIG) for their review of the HHS security program for fiscal year (FY) 2018. 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 Acting Chief Information Security Officer, Janet Vogel at Janet.Vogel@hhs.gov or 202-774-2446.

Attachment

TAB 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 (ISCM) Act of 2014 for Fiscal Year 2018 (A-18-18-11200)*

CC:

Janet Vogel, Acting Chief Information Security Officer
Christopher Bollerer, Deputy Chief Information Security Officer
Jeffrey Arman, OIG Information Technology Audit Manager

TAB 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 (ISCM) Act of 2014 for Fiscal Year 2018 (A-18-18-11200)*

Identity - Risk Management

OIG Recommendation:

In order to move HHS toward an effective risk management domain, we recommend that the HHS OCIO continue to:

- ▶ Work with OPDIVs to enhance its enterprise risk management strategy and program to integrate governance functions for information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas. These enhancements should include the integration of threat modeling for dynamic risk assessments and appropriate reporting tools to timely respond to new threats as they arise.
- ▶ Develop an approach for the Department to ensure that CDM tools, Security Governance Risk Compliance (sGRC) tools, and associated processes are implemented at all OPDIVs for the integration of risk management programs at the enterprise, business process, and information system levels to ensure consistency with OMB, NIST, and Department guidelines and requirements.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

HHS OCIO is currently updating relevant policies and procedures to reflect any new terminology, processes and procedures.

sGRC tool deployment is underway at the Department and the OpDivs. This tool will enhance our ability to document, track and evaluate trends and common issues.

As noted in the report, the new CDM tools being implemented to enhance its security continuous monitoring efforts and achieve visibility into all HHS assets, vulnerabilities, and security threats. With the implementation of these new tools, relevant policies, procedures, and guidance would be updated to reflect the new processes and capabilities that are consistent with OMB, NIST and Department guidelines and requirements.

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

Protect - Configuration Management

OIG Recommendation:

In order to move HHS toward an effective configuration management domain, we recommend that the HHS OCIO continue to:

- ▶ Work with OPDIVs to leverage qualitative and quantitative performance measures to determine the effectiveness of OPDIVs' configuration management plans. These measures should be based on results from automated toolsets to determine security misconfigurations, unsupported information system components, and effectiveness of flaw remediation processes. Define the timeframe for OPDIV communication of the performance measures to the OCIO.
- ▶ Implement the approach for the Department to fully implement CDM tools, SGRC tools, and process tools to consistently record, implement, and maintain configuration controls, baseline configurations of its information systems, and an inventory of related components.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

As noted in the report, some OpDivs are currently awaiting deployment of tools provided by DHS as part of the CDM program. These tools will assist in the effective management of configuration baselines, tracking hardware assets, managing patches, and tracking end of life maintenance support.

sGRC tool deployment is underway at the Department and the OpDivs. This tool will enhance our ability to document, track and evaluate trends and common issues.

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

Protect - Identity and Access Management

OIG Recommendation:

In order to move HHS toward an effective identity and access management domain, we recommend that the HHS OCIO continue to:

- ▶ Work with OPDIVs to determine the effectiveness of identity and access management processes. These measures should monitor OPDIVs' implementation of strong authentication techniques for all privileged and non-privileged users.
- ▶ Assist OPDIV implementation of "to-be" Identity, Credential, and Access Management (ICAM) architecture and integration of their ICAM strategy and activities within its enterprise and Federal ICAM segment architecture.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

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

Data Protection & Privacy

OIG Recommendation:

In order to move HHS toward an effective data protection and privacy domain, we recommend that the HHS OCIO continue to:

- ▶ HHS OCIO update relevant Department policies, procedures, and guidance.
- ▶ Work with the OPDIVs to measure the effectiveness of privacy specific controls and trainings through tracked breaches and maintain current privacy related documentation.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

HHS OCIO is currently updating relevant policies and procedures to reflect any new terminology, processes and procedures.

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings. 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 OpDivs.

Protect - Security Training

OIG Recommendation:

We recommend that HHS OCIO continue to work with the OPDIV to assign the necessary personnel to monitor compliance with the security awareness and training program.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings. 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 OpDivs.

Detect - Information Security Continuous Monitoring

OIG Recommendation:

In order to move HHS toward an effective ISCM domain, we recommend that the HHS OCIO continue to:

- ▶ Provide department-wide guidance and DHS-supplied CDM tools to each OPDIV for the implementation of their ISCM programs. This should include periodic reporting requirements and metrics to monitor real time threats identified by the Computer Security Incident Response Center (CSIRC) across the HHS enterprise.
- ▶ Enhance OPDIVs security continuous monitoring efforts to maintain visibility into IT assets, be aware of all vulnerabilities, be informed about security threats, and verify that all software assets are scanned on the network on a regular basis, as required.
- ▶ Assist OPDIVS in maintaining and managing system ATOs and security control assessments per the HHS policy and guidelines.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

As noted in the report, HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS. However, additional guidance from DHS is still outstanding on ISCM elements and requirements. This guidance is a critical input that will allow HHS to finalize and fully implement their continuous monitoring strategy. The implementation of the sGRC tool will enhance the OpDivs' and OCIO's ability to centrally track and report information systems.

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

Respond - Incident Response

OIG Recommendations

We recommend that the HHS OCIO work with the OPDIV to improve enforcement and communication of the incident response program organization wide. Improvements should focus on measuring consistent profiling techniques and improve communication between the CSIRC, OPDIVs, and components.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

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

Recover – Contingency Planning

OIG Recommendation:

In order to move HHS toward an effective contingency planning domain, we recommend that the HHS OCIO continue to Assist OPDIVs in the implementation of a monitoring program that identifies metrics based on defined mission and business risk. The program should validate OPDIVs implementation of contingency planning policies, procedures, and strategies in the following areas: conducting business impact analysis, conducting contingency plan testing, implementing information system backup and storage requirements, incorporating supply chain risks and the selection of alternative processing sites.

In addition, to ensure vulnerabilities were timely addressed, we provided detailed findings and recommendations that were specific to the OPDIVs.

HHS Response: Concur

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