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 2017

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

March 2018
A-18-17-11200

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 Web site.

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

February 15, 2018

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 2017 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, 2017. 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

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 2017 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, 2017, with the objective of assessing HHS' compliance with FISMA as defined in the FY 2017 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

February 15, 2018
Tysons, Virginia

Report in Brief

Date: March 2018
Report No. A-18-17-11200

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

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017

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, 2017 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 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.

What We Found

Overall, HHS has made improvements and continues to implement changes to strengthen its enterprise-wide information security program including adhering to security training procedures and updating policies and procedures. Further, HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program, coordinating with the Department of Homeland Security (DHS). CDM will allow for HHS to monitor personnel activity, networks, and information systems, as well as report progress through DHS dashboards.

While HHS continue to improve their information security program, opportunities to strengthen the overall information security program were identified which should allow HHS to achieve a higher level of maturity for its information security program. We continued to identify weaknesses in the following areas: risk management, configuration management, identity and access management, 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 configure newly implemented tools procured from DHS to address program missions and goals and address the root cause for risk, inventory, and continuous monitoring concerns and deficiencies. 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 and specific recommendations were also provided to the OPDIVs.

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

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181711200.

TABLE OF CONTENTS

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, 2017 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.

To comply with the FISMA, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2017 FISMA reporting metrics, issued April 17, 2017, 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 2017 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 2017 metrics also mark a continuation of the work that OMB, DHS, and CIGIE undertook in FY 2015 and FY 2016 to move the IG assessments to a maturity model approach. In previous years, CIGIE, in partnership with OMB and DHS, fully transitioned two of the NIST Cybersecurity Framework function areas, Detect and Respond, to maturity models, with other function areas utilizing maturity model indicators. The FY 2017 IG FISMA Reporting Metrics complete this work by not only transitioning the Identify, Protect, and Recover functions to full maturity models, but by reorganizing the models themselves to be more intuitive. This is the first year that all FISMA security domains were

assessed using a maturity model. Therefore, the FY 2017 IG FISMA metrics were assessed differently than the previous year's IG FISMA metrics.

The FY 2017 IG FISMA Reporting Metrics are grouped into seven 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	IG FISMA Domain
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Security Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Reporting Metrics

For FY 2017 IG FISMA Metrics, a series of metrics (or questions) were developed to assess the effectiveness of an agency's information security program as defined by FISMA and relevant guidelines. 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 strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
2. Level 2 (Defined): Policies, procedures, and strategy are formalized and documented but not consistently implemented.
3. Level 3 (Consistently implemented): Policies, procedures, and strategy 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 strategy are collected across the organization and used to assess them and make necessary changes.
5. Level 5 (Optimized): Policies, procedures, and strategy 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

HHS administers more than 100 programs across its operating divisions (OPDIVs) to protect the health of all Americans and provide essential health services, especially for those who are least able to help themselves. HHS' mission is to enhance and protect the health and well-being of all Americans and they fulfill that mission by providing for effective health and human services and

fostering advances in medicine, public health, and social services. 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. The program ensures compliance with federal mandates and legislation, including FISMA and the President's Management Agenda. 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 OPDIV's 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 Chief Information Security Officers 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.

We assigned a maturity level rating of 2, "Defined," for four of the five function areas (Identify, Protect, Detect, and Recover) and level 3 "Consistently Implemented" for the Respond function area. Within the Protect function area, we assigned level 2 to Configuration Management, level 3 to Identity and Access Management, and level 4 to Security Training. It should be noted that changes have been made to the reporting metrics used by IGs in recent years. These changes, together with differences in the scope of audit work performed each year, including the OPDIVs reviewed, make it difficult to compare this year's maturity level ratings to prior year ratings.

Continued improvements were made by HHS in their enterprise-wide security program including adhering to security training procedures and updating policies and procedures. Further, HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program coordinating with DHS. CDM will allow for HHS to monitor personnel activity, networks, and information systems, as well as report progress through DHS dashboards.

While HHS continue to improve their information security program, opportunities to strengthen the overall information security program were identified which should allow HHS to achieve a higher level of maturity for its information security program. We continued to identify weaknesses in the five Cybersecurity framework areas: Identify (Risk Management), Protect

(Configuration Management, Identity and Access Management, Security Training), Detect (ISCM), Respond (Incident Response), and Recover (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 Authorization to Operate (ATO). Additionally, the Department should configure newly implemented tools procured from DHS to address program missions and goals and address the root cause for risk, inventory, and continuous monitoring concerns and deficiencies. These steps will strengthen the program and further enhance the HHS mission.

SECTION III – FINDINGS AND RECOMMENDATIONS

This report consolidates findings identified at the Department level and each of the selected OPDIVs reviewed. Certain details of the vulnerabilities are not presented, because of sensitive information. Such detailed information was provided to HHS and OPDIV management to address the identified conditions.

We identified several reportable exceptions in HHS' security program. The exceptions have been consolidated into each of the five 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 it efforts with its risk management strategy and business needs. HHS and the OPDIVs currently have initiatives in place to implement CDM tools, RSA Archer, and an integrated risk management governance structure, processes, and reporting tools that will allow HHS to reduce the cybersecurity risk of the organization.

Risk Management

The Risk Management Framework, as 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. This year, the maturity model for risk management included metrics for plan of action & milestones (POA&M) management and contractor systems.

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

- At the OCIO and three of the selected OPDIVs, risk management policies and procedures were either not finalized, reviewed or updated per HHS OCIO requirements.
- At two of the selected OPDIVs, there was not an effective process to develop, maintain and report an inventory of software assets on the network.

- At one of the selected OPDIVs, there was not a defined information security architecture integrated into the OPDIV enterprise architecture to provide a disciplined and structured methodology for managing risk.
- At one of the selected OPDIVs, there was not an automated mechanism employed to help maintain an up-to-date, complete, accurate, and readily available inventory of information systems.
- At one of the selected OPDIVs, there were discrepancies for system categorizations between the system inventory and security documentation.
- At one of the selected OPDIVs, the network boundaries for FISMA systems were not defined in relevant documentation.

The review and approval processes for policies and procedures did not always incorporate the Department's requirements to update and review these documents every three years. The OPDIVs did not have an effective asset management program to identify all system software inventories. Additionally, new CDM tools being implemented in FY 2018 should improve the effectiveness of software scanning and inventory capabilities for the enterprise.

Outdated risk and security documentation may not provide the appropriate current guidance and protection techniques for information systems, leading to increased risks for HHS. Without an effective hardware management process, there could be misuse of hardware assets for malicious purposes, threatening the operations and missions for respective OPDIVs. Without an effective program to identify and define all system inventories, HHS and its OPDIVs may not be able to protect its information systems, exposing the Department to additional vulnerabilities. OPDIVs could be unaware of illegally copied or outdated software that was installed by its employees and contractors. Software assets may have legal or security implications if not properly managed or patched. With system boundaries not defined, there is an overall lack of accountability as to specific system owners that are responsible for OPDIV assets, producing additional attack vectors.

Recommendations:

We recommend that the HHS OCIO continue to:

- Update relevant policies, procedures, and guidance and implement CDM tools at all OPDIVs to enhance an integrated risk management program at the enterprise, business process, and information system levels that is consistent with OMB, NIST, and Department guidelines and requirements.

In addition, we provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address these specific findings.

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. According to HHS OCIO, the new CDM tools being implemented should improve the effectiveness of software scanning and inventory capabilities for the enterprise. 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 has received a copy of the OPDIV audit reports and will continue to track findings and report them to management officials.

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, and Security Training. HHS and the OPDIVs currently have initiatives in place to implement CDM tools, RSA Archer, and process tools to assess the effectiveness of information system configuration management activities and inventory related components. Further, HHS continues to implement their Identity Control and Access Management (ICAM) strategy. HHS has deployed performance measures to monitor and analyze the effectiveness of their security awareness training program.

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.

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

- Instances of non-compliance with finalized configuration management policies and procedures were noted at all four selected OPDIVs specific to patch management, up-to-date software maintenance, baseline configurations, and vulnerability scans performed through Security Content Automation Protocol (SCAP) tools.
- At two of the selected OPDIVs, operating systems no longer supported by the vendor (i.e., end-of-life) were installed on some assets. Approved waivers were not completed.
- At one of the selected OPDIVs, configuration management personnel were not tracking the approvals, testing results, and migration dates within change management tracking tools.

Some OPDIVs have not fully developed, defined, and/or implemented their configuration management policies and procedures. Additionally, some OPDIVs are currently awaiting to deploy the tools that are being provided by DHS which should be more effective in managing configuration baselines, tracking hardware assets, managing patches, and tracking end of life maintenance support.

Non-compliance with policies and procedures may lead to increased risks of its information systems. Without effective configuration management programs, HHS and its OPDIVs expose its operating systems to known vulnerabilities and exploitation. During May 2017, the WannaCry ransomware cyberattack targeted unpatched computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments. This could leave HHS data susceptible to unauthorized disclosure, modification or non-availability of data. Without managing the vulnerabilities identified during scans, OPDIVs may not be able to take action to

reduce the potential threats that these vulnerabilities are exploited and thereby reduce risk of compromise to the confidentiality, integrity, and availability of its information assets.

Recommendation:

We recommend that the HHS OCIO continue to:

- Implement CDM tools and RSA Archer at the Department level and at all OPDIVs to enhance its configuration management program in order to maintain and measure its configuration management activities at the enterprise, business process, and information system levels.

We have provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address their specific findings.

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO stated that some OPDIVs are currently awaiting the final 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. Once the deployment of RSA Archer is completed, it will enhance HHS OCIO's ability to document, track and evaluate trends and common issues. HHS OCIO has received a copy of the OPDIV audit reports and is coordinating a review of the specific findings.

Identity and Access Management

Federal agencies are required to establish procedures to limit information system access to authorized individuals and to limit the types of transactions and functions that authorized users are permitted to perform based on the concept of least privilege. Remote access provides the ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities. Remote access management refers to activities performed to establish a secure channel for users to remotely authenticate over open networks.

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

- At two of the selected OPDIVs, account management procedures were not followed; this included monitoring and maintaining active and shared accounts, periodically reviewing users, enforcing resets of active network user account passwords, removing inactive accounts in a timely manner, and disabling accounts of transferred and terminated personnel in a timely manner.
- At two of the selected OPDIVs, Personal Identification Verification (PIV) cards were either not issued to some personnel or implemented for logical access. One OPDIV's policies and procedures for identity and access management and remote access were not updated and reviewed per HHS OCIO requirements. The OPDIVs did not consistently comply with their procedures for managing user access, oversight of terminated users, and user account management.

Weaknesses in identity and access management and remote access management controls may increase the risk of inappropriate access to the HHS network, information systems and data. Identity access and remote access policies and procedures that are not updated, finalized, and distributed may result in a lack of clarity in the implementation and control of access, thereby leading to potentially unauthorized access to the network resulting in loss, destruction or misuse of sensitive data and resources.

Recommendation:

We have provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address their specific findings.

HHS OCIO Response:

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

Security Training

An effective IT security program cannot be established without significant attention given to training its information system users. Federal agencies and organizations cannot protect the confidentiality, integrity and availability of information in today's highly networked systems environment and secured physical locations without providing their personnel training to:
(a) understand their roles and responsibilities related to the organizational mission; (b) understand the organization's IT security policies, procedures, and practices; and; (c) have adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

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

- At three of the selected OPDIVs, the required new hire, annual and role-based trainings were not taken by some personnel. The total number of personnel that did not receive the training was minimal.
- At two of the selected OPDIVs, there was not an effective tracking of OPDIV personnel and contractors regarding their security training status.

Some OPDIVs lacked an effective process to monitor and enforce security training requirements for all employees and contractors. The OPDIVs continue to enhance their monitoring processes for completion of security training of their personnel and contractors.

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 and increase the risk of causing a computer security incident. This could lead to the loss, destruction or misuse of sensitive Federal data assets.

Recommendation:

We provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address their specific findings.

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS 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

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 as defined by the information security continuous monitoring domain. HHS released the *"HHS Information Security Continuous Monitoring Strategy"* in May 2017 to define and communicate the enterprise ISCM strategy. HHS and its OPDIVs currently have initiatives in place to implement CDM tools, RSA Archer, and process tools to assess the effectiveness of their ISCM program.

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 the system security plan, a security assessment report, and POA&Ms, which are the three principal documents in the security authorization package. OMB and DHS have updated the requirements to include documentation of an ISCM strategy, implementation of ISCM for information technology assets, incorporation of risk assessments to develop an ISCM strategy, and reporting of ISCM results in accordance with their strategy. HHS has formalized its ISCM program through development of ISCM policies, procedures, and strategies. DHS has put in place requirements that focus on "real-time" monitoring of systems controls. The CDM program - implemented by DHS - includes continuously monitoring of networks and systems, updating and finalizing policies and procedures, documenting OPDIVs' progress to address and implement strategies, and reporting its progress through DHS dashboards. HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS. HHS and its OPDIVs have made progress by implementing these tools and are working on the "real-time" monitoring of their security controls. 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 following findings were identified as they relate to HHS' continuous monitoring program:

- The OCIO does not currently know the effectiveness of software scanning tools that are leveraged by the OPDIVs to determine authorized software on the network.
- The OCIO does not currently know the full listing of systems that are operational across the HHS environment.
- At two of the selected OPDIVs, information system security control assessments for sampled information systems did not document all NIST 800-53 controls and include all of the testing results.
- At two of the selected OPDIVs, instances of operational non-compliance with the OPDIVs ISCM program requirements were identified. OPDIVs were not able to provide an inventory of authorized and unauthorized devices and software on the network or identified unauthorized software currently on the network. Additionally, discrepancies were found when reconciling hardware inventories and antivirus scanning software scanning results.
- At one of the selected OPDIVs, there are a small number of information systems that were operating without a current ATO.

Without a Department-wide, fully-implemented enterprise-level ISCM program, HHS and its OPDIVs do not have a complete list of processes that need to be performed in order to protect their information assets. This may result in potential high-risk threats not being detected, which may result in unauthorized access or changes to information systems leading to misuse, compromise, or loss of confidential data and resources.

Recommendation:

We recommend that the HHS OCIO continue to:

- Enhance the Department-wide ISCM program and continue to provide department-wide guidance and SCAP tools to each OPDIV for the implementation of their ISCM programs. This would also increase the Department's awareness of OPDIVs' software scanning capabilities.
- Implement and configure DHS' CDM inventory management tools and mechanisms to centrally track and report information systems from all OPDIVs.

In addition, we provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address these specific findings.

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO stated that HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS. However, additional guidance on ISCM elements and requirements from DHS is still outstanding in order for HHS OCIO to finalize and fully implement its continuous monitoring strategy. Once the implementation of RSA Archer is completed, it will enhance HHS OCIO's ability to centrally track and report information systems. HHS OCIO has received a copy of the OPDIV audit reports and is coordinating a review of the specific findings.

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. HHS consistently implemented, captured, and shared lessons on their incident response policies, procedures, plans, and strategies.

Incident Response

Incident response involves capturing general threats and incidents that occur in the HHS system 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.

The following findings were identified with HHS' incident response program:

- A small number of incidents were not reported to the United States Computer Emergency Response Team (US-CERT) by the HHS Computer Security Incident Response Center (CSIRC) within the required timeframe.
- At one of the selected OPDIVs, there was not a file integrity software program in its incident response software.
- At one of the selected OPDIVs, there was not a 24/7 monitoring capability.

In some cases, incidents were not being tracked accurately and reported to US-CERT within the required timeframe due to lack of OPDIVs management oversight or documentation errors. Resources were not allocated to provide 24/7 monitoring coverage which could result in delayed reporting of incidents.

Without tracking all incidents accurately and reporting incidents in a timely manner, HHS faces an increased exposure to security risks to its IT environment.

Recommendations:

We recommend that the HHS OCIO continue to:

- Implement an adequate oversight protocol to monitor and ensure that all OPDIVs report incidents timely to the HHS CSIRC.

In addition, we provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address these specific exceptions.

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. In order to assist the OPDIVs in complying with US-CERT and HHS reporting requirements, CSIRC initiated a program to perform incident response plan tabletop exercises with each OPDIV. HHS OCIO will continue this program and determine if additional testing is needed during these exercises in order to meet all incident reporting requirements. HHS OCIO has received a copy of the OPDIV audit reports and is coordinating a review of the specific findings.

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. HHS has defined processes for information systems contingency plan development, maintenance, testing, and integration with other continuity areas.

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, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

The following findings were identified within HHS' contingency planning program:

- At three of the selected OPDIVs, a system level Business Impact Analysis, including all necessary elements based on NIST guidance, were not documented for some systems reviewed.
- At two of the selected OPDIVs, there were no results or an after-action report available to demonstrate that the contingency plans were tested on an annual basis for selected systems.
- At one of the selected OPDIVs, the Continuity of Operations (COOP) and information system contingency plan documentation was not complete and did not meet NIST guidance.
- At two of the selected OPDIVs, backup and restoration procedures were either not performed or not effective for some systems reviewed.

In some instances, OPDIVs have not documented or updated the COOP, contingency plans and related documentation in accordance with HHS requirements. Some OPDIVs did not have adequate oversight to ensure contingency planning efforts for all systems, including information system contingency plan testing, backups, and restorations, meet HHS and NIST standards to support the adequate recoverability and security of data.

Without maintaining an effective contingency planning process, the contingency plan might not provide adequate coverage of all system components, incorporate lessons learned from plan testing exercises, or address all potentially mission/business critical processes and their interdependencies in the event of a true disaster or emergency. Without conducting and documenting an enterprise-wide exercise on an annual basis, system owners and its users may be unaware and unprepared to address the current threats that may significantly impact the information system security.

Recommendation:

We provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so that they could address these specific findings.

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO has received a copy of the OPDIV audit reports and is coordinating a review of the specific findings. This will enable HHS 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.

HHS Comments

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

HHS' comments are included as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

In tandem with the work being undertaken for the Chief Financial Officer audit, we performed procedures to assess, based on OMB and DHS guidance, HHS' compliance with FISMA. To assess HHS' FISMA compliance, we leveraged the FISMA reporting metrics for the Inspector General. We developed an Objective Attribute Recap Sheet for each finding identified during the testing and provided to the OPDIV after review and concurrence by the OIG.

We performed our fieldwork at the HHS OCIO and four (4) HHS OPDIVs during the FY 2017 performance audit:

- Centers for Medicare & Medicaid Services (CMS)
- Indian Health Service (IHS)
- National Institutes of Health (NIH)
- Office of the Secretary (OS)

Additionally, we followed up with the Centers for Disease Control and Prevention (CDC) on the status of FY 2016 FISMA findings and with Food and Drug Administration (FDA) on the status of the FY 2015 Government Accountability Office FISMA 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 its self-assessment for each FISMA reporting metric.
- 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 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.

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* (Mar 9, 2006);
- *HHS Counterintelligence and Insider Threat Policy* (June 2015);
- 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);
- IHS *Indian Health Manual (IHM) Access Control - Chapter 21*
- 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* (February 2010);
- NIST SP 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013);
- NIST SP 800-61*, Section 2.4.2 Team Model Selection* (August 2012);
- Office of the Secretary's *Patch Management Standard Operating Procedures*;
- OS *Procedures Handbook for Information Security* (November 25, 2016);
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007);
- OMB M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements* (November 4, 2016);
- *US-CERT Federal Incident Notification Guidelines*

APPENDIX C: FY 2017 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 Office of Inspector General entered its FY 2017 FISMA audit results and narrative comments into the CyberScope system.

Inspector General

Section Report

2017

Annual FISMA Report

Department of Health and Human Services

For Official Use Only

Function 1: Identify - Risk Management

1 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 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4)?

Defined (Level 2)

Comments: Overall, HHS is at a defined maturity level for this question though two of the four OPDIVs reviewed were at the consistently implemented level with a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections. The Department did not have a systems inventory reconciliation process in place to determine completeness and accuracy of systems inventory and system interconnections at all OPDIVs. The OPDIVs have initiatives in the works such as implementing CDM tools, RSA Archer, and processes in order to move them to a consistently implemented maturity level.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets 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)?

Defined (Level 2)

Comments: Overall, HHS is at a defined maturity level for this question. Two of 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. Three of 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. The OPDIVs have initiatives in the works, such as implementing CDM tools and processes, in order to move them to a consistently implemented maturity 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: The four OPDIVs reviewed have defined, but not consistently implemented, a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting. Two OPDIVs did not ensure that the software assets on the network (and their associated licenses) are subject to the monitoring processes defined within the organization's ISCM strategy. The OPDIVs have initiatives in the works 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; and FIPS 199)?

Consistently Implemented (Level 3)

Comments: Information on the organization's defined importance/priority levels for its missions, business functions, and information is consistently implemented and integrated with other information security areas to guide risk management activities and investments in accordance with applicable requirements and guidance. Additionally, systems with significant financial investments receive additional scrutiny through the CPIC process, where security is integrated as a data point and supports risk management activities. The Department is rolling out additional reporting tools to enhance this process.

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include 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 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

Defined (Level 2)

Comments: While some OPDIVs are using RSA Archer's dashboards and reports to present an enterprise security posture view with the capability to drill down through the data to identify key security weaknesses, not all OPDIVs are consistently implementing its risk management program at the enterprise, business process, and information system levels. The continued rollout of RSA Archer should enable HHS to consistently implement and possibly move to a managed and measurable maturity level for its risk management program.

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Defined (Level 2)

Comments: Overall, HHS has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture for risk management. Security architecture reviews are consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment. The OPDIVs are in the process of consistently implementing its security architecture across the enterprise, business processes, and system levels.

Function 1: Identify - Risk Management

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, 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 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Consistently Implemented (Level 3)

Comments: For the four OPDIVs reviewed, roles and responsibilities of stakeholders have been defined and communicated across the organization. Three OPDIVs have consistently implemented these procedures and one OPDIV is already at a managed and measurable maturity level. The Department's Office of the Chief Information Officer (OCIO) and the OPDIVs are implementing an integrated risk management governance structure for implementing and overseeing an enterprise risk management capability that will help HHS move to a managed and measured maturity level.

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: At the Department level and for the four OPDIVs reviewed, the POA&M process is consistently implemented. Each of the four OPDIVs use specific tools in order to manage the tracking and mitigation of security weaknesses. The Department's OCIO and the four OPDIVs are moving towards establishing a managed and measurable maturity level with implementation of 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) selecting and implementing security controls to mitigate system-level risks (NIST 800--37; NIST 800-39; NIST 800--53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?

Consistently Implemented (Level 3)

Comments: The Department and the four OPDIVs reviewed have consistently implemented a system level risk assessment program with one OPDIV already at a managed and measurable maturity level. The OPDIVs use various vulnerability management tools to achieve this goal. The implementation of tools such as CDM will help monitor the effectiveness of risk responses across HHS.

Function 1: Identify - Risk Management

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)?

Consistently Implemented (Level 3)

Comments: The Department and three OPDIVs have consistently implemented a system level risk assessment program. The current implementation of dashboards and reporting tools will help facilitate a portfolio view of interrelated risks across HHS to reach a managed and measurable maturity level.

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, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8)?

Defined (Level 2)

Comments: Overall, HHS has defined a process and consistently implemented it at two OPDIVs reviewed to include information security and other business areas as appropriate for ensuring that contracts and other agreements for third party systems and services include appropriate clauses to monitor the risks related to such systems and services. The OCIO issued policies in the fourth quarter of FY2017 covering contracting language to be implemented at all OPDIVs. This should help HHS move towards a consistently implemented maturity 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)?

Defined (Level 2)

Comments: The four OPDIVs reviewed have identified and defined and two of those OPDIVs have consistently implemented their requirements for an automated solution that provides a centralized, enterprise wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. HHS has invested in RSA Archer to provide a centralized, enterprise wide view of risks across the organization. This should help HHS move towards a consistently implemented maturity level.

Function 1: Identify - Risk Management

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

Defined (Level 2)

Comments: Overall the Department and its OPDIVs have initiatives and processes to implement its Risk Management program. However, all OPDIVs are not consistently implementing its risk management programs. With the full implementation of the CDM tools at the Department and OPDIV level, HHS should have the capability to consistently implement and have an effective 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?

Since HHS is at the Defined maturity level for its risk management program and level 4 (Managed and Measureable) is deemed to be effective, HHS's risk management program is currently not effective.

Comments:

Calculated Maturity Level - Defined (Level 2)

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; SP 800-128: Section 2.4)?

Defined (Level 2)

Comments: The four OPDIVs reviewed have identified and defined its requirements for an automated solution that provides a centralized, enterprise wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. One OPDIV is at a consistently implemented maturity level and one OPDIV is at the managed and measureable level. HHS is implementing CDM tools and RSA Archer so that metrics can be maintained on the effectiveness of information system configuration management activities.

Function 2A: Protect - Configuration Management

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 location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800--128: Section 2.3.2; NIST 800--53: CM-9)?

Defined (Level 2)

Comments: The four OPDIVs reviewed have developed an organization wide configuration management plan that includes the necessary components and two OPDIVs have consistently implemented it and one OPDIV also monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan to reach a managed and measurable maturity level. HHS is implementing CDM tools and RSA Archer that should enable HHS to reach 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 800-128: 2.2.1)

Defined (Level 2)

Comments: The four OPDIVS reviewed have developed, documented, and disseminated comprehensive policies and procedures for managing the configurations of its information systems. This process has been consistently implemented by one OPDIV who conducts lessons learned activities with the CIOs, ISSOs, and security staff at established monthly meetings. Opportunities for improvement are incorporated into information security 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, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?

Defined (Level 2)

Comments: Overall, HHS has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures. The OPDIVs 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

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 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Defined (Level 2)

Comments: The four OPDIVs reviewed have developed, documented, and disseminated its policies and procedures in this area and developed common secure configurations (hardening guides) that are tailored to its environment. One OPDIV is at a managed and measured maturity level by employing Tenable Security Center to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.

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

Defined (Level 2)

Comments: The four OPDIVS reviewed have developed, documented, and disseminated its policies and procedures for flaw remediation, including patch management, to manage software vulnerabilities. One OPDIV has consistently implemented these procedures. HHS has CDM initiatives and Information Security Modernization initiative in order to automate and manage the flaw remediation, patch management, and software vulnerabilities and gain qualitative and quantitative reports that help generate effective solutions.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

Consistently Implemented (Level 3)

Comments: HHS has consistently implemented its TIC approved connections and critical capabilities that it manages internally. HHS has implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST 800-53: CM--2, CM-3)?

Consistently Implemented (Level 3)

Comments: The Department and the four OPDIVs reviewed have developed, documented, and disseminated its policies and procedures for managing configuration change control. Three OPDIVs have consistently implemented their change control policies, procedures, and processes, including explicitly consideration of security impacts prior to implementing changes. The OPDIVs are implementing CDM tools, RSA Archer, and processes in order to reach a managed and measurable maturity level.

Function 2A: Protect - Configuration Management

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

Since overall, HHS is only at the Defined level for its configuration management program, it is not 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 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Defined (Level 2)

Comments: The OCIO and the four OPDIVs reviewed have defined and communicated roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM. While overall HHS is at the defined level, one OPDIV is at a managed and measurable maturity level.

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 implementing its ICAM strategy and is on track to meet milestones though some OPDIVs have not consistently implemented the strategy.

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 27 through 31) (NIST 800-53: AC-1 and IA--1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

Consistently Implemented (Level 3)

Comments: Overall, HHS is consistently implementing its policies and procedures for ICAM, including account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. The OCIO and the OPDIVs are implementing tools and processes in order to reach the managed and measurable maturity level.

Function 2B: Protect - Identity and Access Management

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2, PS- 3; and National Insider Threat Policy)?

Consistently Implemented (Level 3)

Comments: Three of the four OPDIVs reviewed are at a consistently implemented maturity level and one OPDIV is at an optimized 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.

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: The four OPDIVS reviewed are at a consistently implemented maturity level where access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800--53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: Overall, HHS has consistently implemented strong authentication mechanisms for non- privileged users of the organization's facilities and networks, including for remote access. One OPDIV is further along at a managed and measurable maturity level where non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800--53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a managed and measurable maturity level where privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

Function 2B: Protect - Identity and Access Management

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Defined (Level 2)

Comments: The OCIO and the four OPDIV reviewed have defined processes for provisioning, managing, and reviewing privileged accounts. One OPDIV is further along at a consistently implemented maturity level.

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, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

Consistently Implemented (Level 3)

Comments: The four OPDIVS reviewed are at a consistently implemented maturity level by implementing FIPS 140-2 validated cryptographic modules for remote access connection, remote access sessions time out after 30 minutes, and remote users' activities being logged and reviewed based on risk.

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?

HHS's identity and access management program is not effective since it is not at the managed and measureable level across the Department.

Comments:

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2C: Protect - Security Training

Function 2C: Protect - Security Training

33 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 800-53: AT-1; and NIST SP 800-50)?

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a managed and measurable maturity level. HHS has assigned responsibility for monitoring and tracking the effectiveness of security awareness and training activities.

34 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 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

Defined (Level 2)

Comments: Two of the OPDIVs reviewed have conducted an assessment of the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. Further, they periodically update its assessment to account for a changing risk environment. However, the other two OPDIVs reviewed have not completed the assessments.

35 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 800--53: AT-1; NIST 800-50: Section 3))

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a managed and measurable maturity level. HHS monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans.

36 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 questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a managed and measurable maturity level. HHS monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures.

Function 2C: Protect - Security Training

37 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 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a managed and measurable maturity level since HHS measures the effectiveness of the awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and disciplinary action.

38 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 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Managed and Measurable (Level 4)

Comments: Overall, HHS is at a managed and measurable maturity level. HHS obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, HHS measures the effectiveness of its specialized security training program with phishing exercises and follow-up.

39.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).

Defined (Level 2)

Comments: While HHS and its OPDIVs have defined and in many areas consistently implemented its configuration management, identity and access management, and security training programs, due to the federated nature of HHS, not all OPDIVs are all at the same maturity levels. Therefore, overall HHS is at the Defined level for the Protect function.

39.2 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.

Comments:

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 3: Detect - ISCM

Function 3: Detect - ISCM

40 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: Three of the OPDIVs reviewed consistently implemented the ISCM strategy at the OPDIV level and information system levels supporting clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. However, one of the OPDIVs reviewed have not consistently implemented it at the organization and information systems levels. To help this goal across all of OPDIVs, HHS released the 'HHS Information Security Continuous Monitoring Strategy' in May 2017.

41 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; collecting 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 43)

Defined (Level 2)

Comments: Overall, HHS has defined and communicated ISCM policies and procedures. To help this goal, HHS released the 'HHS Information Security Continuous Monitoring Strategy' in May 2017. One OPDIV is further ahead and is at a consistently implemented maturity level and another OPDIV is even further ahead at a managed and measurable maturity level.

42 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 2017 CIO FISMA Metrics)?

Defined (Level 2)

Comments: Overall, HHS has defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies. To help this goal, HHS released the 'HHS Information Security Continuous Monitoring Strategy' in May 2017. One OPDIV is further ahead and is at a consistently implemented maturity level and another OPDIV is even further ahead at a managed and measurable maturity level.

Function 3: Detect - ISCM

43 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: While the OCIO and OPDIVs have defined it processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls to provide a view of the organizational security posture as well as each system's contribution to said security posture, two of the four OPDIVs reviewed have consistently implemented its processes (test all appropriate security controls). The OCIO uses quarterly reports and dashboard reports to view the progress of information security administration at the OPDIVs.

44 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 has identified and defined the performance measures and requirements that are used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, HHS has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities. The implementation of CDM tools and RSA Archer will help move HHS to the next maturity level of consistently implemented.

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

Defined (Level 2)

Comments: Since HHS and the OPDIVs reviewed are not consistently implementing its ISCM program, overall HHS' ISCM program is at the Defined level.

45.2 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 and at some OPDIVs consistently implemented them, overall the ISCM program at HHS is not effective.

Calculated Maturity Level - Defined (Level 2)

Function 4: Respond - Incident Response

Function 4: Respond - Incident Response

46 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 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)

Consistently Implemented (Level 3)

Comments: Overall, HHS consistently implements its incident response policies, procedures, plans, and strategies. Further, HHS is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy and processes to update the program. The Department's Computer Security Incident Response Center (CSIRC) and two OPDIVs reviewed are further along at a managed and measurable maturity level.

47 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; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: Overall, HHS has defined incident response roles and responsibilities and teams have adequate resources (people, processes, and technology) to consistently implement incident response activities. The Department's CSIRC and two OPDIVs reviewed are further along at a managed and measurable maturity level.

48 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; US- CERT Incident Response Guidelines)?

Consistently Implemented (Level 3)

Comments: Overall, HHS consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, HHS consistently implements and analyzes precursors and indicators generated by technologies such as the intrusion detection/prevention system, Security Information and Event Management (SIEM), antivirus and antispam software.

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

Consistently Implemented (Level 3)

Comments: Overall, HHS consistently implements its incident handling with a centralized incident response center (CSIRC) that all OPDIVs report incidents to. The CSIRC is responsible for consistently implementing its containment strategies, incident eradication processes and processes to remediate vulnerabilities.

Function 4: Respond - Incident Response

50 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-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

Defined (Level 2)

Comments: The Department's CSIRC shares information on incident activities with internal stakeholders and consistently implements the process whereby security incidents are reported to US-CERT, law enforcement, the OIG, and Congress (for major incidents) in a timely manner. However, three OPDIVs reviewed have not consistently shared information on incident activities with all its internal stakeholders.

51 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 and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

Consistently Implemented (Level 3)

Comments: Overall, HHS consistently utilizes on-site technical assistance and surge capabilities for incident response. HHS utilizes DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its network and has several tools implemented at the OPDIVs.

52 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)

Consistently Implemented (Level 3)

Comments: Overall, HHS consistently implements its defined incident response technologies. In addition, the technologies utilized are interoperable and cover the organization's network, and have been configured to collect and retain relevant and meaningful data. Two OPDIVs are further along at a managed and measurable maturity level.

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

Consistently Implemented (Level 3)

Comments: While the Department's CSIRC is managing and measuring security incidents (tracks, reports, assists in remediation of incidents) across the Department, and the OPDIVs are consistently implementing incident response and handling, some of the OPDIVs have not implemented processes that rise to the managed and measurable level.

Function 4: Respond - Incident Response

53.2 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?

While at the Department level there is an effective process in place to manage security incidents, not all OPDIVs have effective incident response programs in place (not at the managed and measurable level), therefore overall HHS' incident response function is not effective.

Comments:

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

54 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 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Defined (Level 2)

Comments: Overall, HHS has defined roles and responsibilities of stakeholders and communicated them across the organization, including appropriate delegations of authority. In addition, HHS has designated appropriate teams to implement its contingency planning strategies. Two OPDIVs reviewed are further along at a consistently implemented maturity level.

55 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 56-60) (NIST SP 800-34; NIST SP 800--161).

Defined (Level 2)

Comments: Overall, HHS has defined its policies, procedures, and strategies, for information system contingency planning, including technical contingency planning considerations for different types of systems. This includes roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance schedules, backups and storage, and use of alternate processing and storage sites. One OPDIV is further along at a consistently implemented maturity level.

56 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800--34, Rev. 1, 3.2, FIPS 199, FCD--1, OMB M-17-09)?

Defined (Level 2)

Comments: Overall, HHS has defined processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts. OPDIVs are working on implementing these defined processes to take them to the next maturity level of consistently implemented.

Function 5: Recover - Contingency Planning

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

Defined (Level 2)

Comments: Overall, HHS has defined processes for information system contingency plan development, maintenance, and integration with other continuity areas. One OPDIV is further ahead and is at a consistently implemented maturity level and another OPDIV is even further ahead at a managed and measurable maturity level.

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

Defined (Level 2)

Comments: Overall, HHS has defined processes for information system contingency plan testing and exercises for tabletop and functional exercises. Two OPDIVs reviewed are further ahead and are at a consistently implemented maturity level.

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800--53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: HHS and its OPDIVs have defined its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites but have not consistently implemented them across all of its OPDIVs and its systems.

60 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 800-53: CP-2, IR-4)?

Defined (Level 2)

Comments: Overall, HHS has defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams. Two OPDIVs are further ahead and are at a consistently implemented maturity level.

61.1 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 is contingency planning functions, therefore HHS is at the Defined level.

Function 5: Recover - Contingency Planning

61.2 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 is contingency planning functions, therefore it is not effective.

Comments:

Calculated Maturity Level - Defined (Level 2)

Function 0: Overall

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

Not Effective

Function 0: Overall

1.2 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.

Overall, HHS has made improvements and 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' level for Identify, Protect, Detect, Respond, and Recover functional areas. HHS is 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 continuously monitoring of its networks and systems, documenting OPDIVs' progress to address and implement strategies, and reporting its progress through DHS dashboards. Additionally, HHS needs to makes sure that there is effective vulnerability management, patch management, and access management through the use of appropriate tools and processes at all OPDIVs. HHS also needs to continue to build towards an operational environment where all the functional areas interact with each other in real time and provide holistic and coordinated responses to security events helping strengthen all aspects of the information security program. These steps will strengthen the program and further enhance the HHS mission.

Comments:

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 released by the DHS. We assessed the maturity levels and effectiveness across the Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, 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 Operating Divisions (OPDIVs) were in-scope for this assessment: Centers for Medicare & Medicaid Services, Indian Health Service, 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 FY2016 FISMA findings and with the Food and Drug Administration on the status of the FY2015 Government Accountability Office FISMA related findings. 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	7
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	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)	0

Function 2B: Protect - Identity and Access Management

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

Function 2C: Protect - Security Training

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

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	0

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Defined (Level 2)	Defined (Level 2)	Overall the Department and its OPDIVs have initiatives and processes to implement its Risk Management program. However, all OPDIVs are not consistently implementing its risk management programs. With the full implementation of the CDM tools at the Department and OPDIV level, HHS should have the capability to consistently implement and have an effective risk management program.
Function 2: Protect - Configuration Management / Identity Management / Security Training	Defined (Level 2)	Defined (Level 2)	While HHS and its OPDIVs have defined and in many areas consistently implemented its configuration management, identity and access management, and security training programs, due to the federated nature of HHS, not all OPDIVs are all at the same maturity levels. Therefore, overall HHS is at the Defined level for the Protect function.
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	Since HHS and the OPDIVs reviewed are not consistently implementing its ISCM program, overall HHS' ISCM program is at the Defined level.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	While the Department's CSIRC is managing and measuring security incidents (tracks, reports, and assists in remediation of incidents) across the Department and the OPDIVs are consistently implementing incident response and handling, some of the OPDIVs have not implemented processes that rise to the managed and measurable level.

Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	HHS and its OPDIVs have not consistently implemented is 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, D.C. 20201

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

FROM: Beth Killoran
Chief Information Officer
Department of Health and Human Services

DATE: February 5, 2018

SUBJECT: Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017 (A-18-17-11200)

The Department of Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) thanks the Office of the Inspector General (OIG) for your review of the HHS security program for fiscal year (FY) 2017. We welcome the opportunity to respond to the report developed by Ernst & Young on your behalf.

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

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

Regards,

/Beth Killoran/

Beth Killoran
HHS Chief Information Officer

Attachment A

CC:
Christopher Wlaschin, HHS Chief Information Security Officer
Christopher Bollerer, HHS Deputy Chief Information Security Officer (Acting)
Jeffrey Arman, OIG Information Technology Audit Manager

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017 (A-18-17-11200)***

Identity - Risk Management

OIG Recommendation:

We recommend that the HHS OCIO continue to:

- Update relevant policies, procedures, and guidance and implement CDM tools at all OPDIVs to enhance an integrated risk management program at the enterprise, business process, and information system levels that is consistent with OMB, NIST, and Department guidelines and requirements.

In addition, we provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address these specific findings.

HHS Response: Concur

As noted in the report, the new CDM tools being implemented in FY 2018 should improve the effectiveness of software scanning and inventory capabilities for the enterprise. 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 will continue to track findings and report them to management officials.

Protect - Configuration Management

OIG Recommendation:

We recommend that the HHS OCIO continue to:

- Implement CDM tools and RSA Archer at the Department level and at all OPDIVs to enhance its configuration management program in order to maintain and measure its configuration management activities at the enterprise, business process, and information system levels.

We have provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address their specific findings.

HHS Response: Concur

As noted in the report, some OpDivs are currently awaiting the final 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.

RSA Archer 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:

- We have provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address their specific findings.

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.

Protect - Security Training

OIG Recommendation:

- We have provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address their specific findings.

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:

We recommend that the HHS OCIO continue to:

- Enhance the Department-wide ISCM program and continue to provide department-wide guidance and SCAP tools to each OPDIV for the implementation of their ISCM

programs. This would also increase the Department's awareness of OPDIVs' software scanning capabilities.

- Implement and configure DHS CDM inventory management tools and mechanisms to centrally track and report information systems from all OPDIVs.

In addition, we provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address these specific findings.

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 RSA Archer 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 continue to:

- Implement an adequate oversight protocol to monitor and ensure that all OPDIVs report incidents timely to the HHS CSIRC.

In addition, we provided detailed information and recommendations that were specific to the OPDIVs' findings to management officials so they could address these specific exceptions.

HHS Response: Concur

In order to assist the OpDivs in complying with US-CERT and HHS reporting requirements, CSIRC initiated a program to perform incident response plan tabletop exercises with each OpDiv. During the exercise, policies, procedures and plans are tested to ensure that they are up-to-date, effective, and in compliance with US-CERT, OCIO, and other federal guidelines (including the timeliness and completeness of reported data). OCIO will continue this program and determine if additional testing is needed during these exercises in order to meet all incident reporting 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 incident response policies and/or procedures are adequate at the OpDivs.

Recover – Contingency Planning

OIG Recommendation:

- We provided detailed information and recommendations that were specific to the OPDIV's findings to OPDIV management officials so that they could address these specific findings.

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.