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 2019

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

Amy J. Frontz
Deputy Inspector General
for Audit Services

April 2020
A-18-19-11200

# *Office of Inspector General*

https://oig.hhs.gov

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

## *Office of Audit Services*

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

## *Office of Evaluation and Inspections*

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

## *Office of Investigations*

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

## *Office of Counsel to the Inspector General*

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

# *Notices*

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

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

## OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

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

**Report in Brief**
Date: April 2020 Report
No. A-18-19-11200

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 2019

## Why We Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires Inspectors General to perform an annual independent evaluation of their agency's information security programs and practices to determine the effectiveness of those programs and practices. HHS OIG engaged Ernst & Young LLP (EY) to conduct this audit.

EY conducted a performance audit of HHS' compliance with FISMA as of September 30, 2019 based upon the FISMA reporting metrics defined by the Inspectors General.

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

## How We Did This Audit

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

## What We Found

Overall, HHS continues to implement changes to strengthen the maturity of its enterprise-wide cybersecurity program. Progress has been made to mature cybersecurity in the Configuration Management and Information Security Continuous Monitoring FISMA domains. Both domains were assessed at Consistently Implemented maturity in FY 2019, an improvement from Defined in FY 2018. Also notable was increased maturation of Incident Response. We identified opportunities where HHS can strengthen its overall information security program. Weaknesses continue to persist in Contingency Planning, which was the only domain assessed as Defined. Additionally, we identified weaknesses in each of the IG FISMA domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response and contingency planning.

## What We Recommend and HHS Comments

We recommend that HHS further strengthen its cybersecurity program and enhance information security controls at HHS. Specific recommendations were also provided to the HHS OPDIVs reviewed.

HHS should commit to creating and implementing a Cybersecurity Maturity Migration Strategy to advance the cybersecurity program from its current maturity state to Managed and Measurable across HHS. A progression road map and plan should be developed that includes specific, measurable, attainable, relevant and time-bound (SMART) milestones.

HHS' program should address current gaps between the current maturity levels to the level of Managed and Measurable. Roles and shared responsibilities should be articulated and implemented to meet the requirements for effective maturity, including whether requirements are to be implemented using centralized, federated, or hybrid controls.

HHS concurred with all of our recommendations. HHS also provided technical comments, which we addressed.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181911200.asp.

# Department of Health and Human Services (HHS)

## Federal Information Security Modernization Act (FISMA) report

March 19, 2020

Building a better working world

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

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

# Report of Independent Auditors on HHS' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2019 Based on a Performance Audit Conducted in Accordance with *Government Auditing Standards*

Ms. Tamara Lilly
Assistant Inspector General for Audit Services

We have conducted a performance audit of the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2019, with the objective of assessing HHS' compliance with FISMA as defined in the FY 2019 Inspector General FISMA Reporting Metrics.

We conducted this performance audit in accordance with generally accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To audit HHS' compliance with FISMA, we applied the FISMA reporting metrics for the Inspector General. The specific scope and methodology are defined in Appendix A of this report.

The conclusions in Section II and our findings and recommendations, as well as proposed alternatives for the improvement of HHS' compliance with FISMA in Section III, were noted as a result of our audit.

This report is intended solely for the information and use of HHS, the HHS Office of Inspector General (OIG), Department of Homeland Security (DHS), Office of Management and Budget (OMB), the appropriate committees of Congress and the Comptroller General and is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

March 19, 2020

# Contents

Section I

# Background

# Introduction

We conducted a performance audit of the Department of Health and Human Services' compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2019 based upon the questions outlined in the FISMA reporting metrics for the Inspectors General (IG).

# Section I: Background

On December 17, 2002, the President signed the FISMA into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provide a mechanism for improved oversight of Federal agency information security programs. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendments included the: (1) reestablishment of the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification or destruction of such information or information systems.

To comply with the FISMA, OMB, DHS and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2019 IG FISMA reporting metrics, issued April 9, 2019, in consultation with the Federal Chief Information Officers Council. These metrics leverage the *National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)* and are aligned with the five function areas: Identify, Protect, Detect, Respond and Recover. FISMA requires Inspectors General to perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of the information security program and practices of the agency. The FY 2019 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 2019 metrics also mark a continuation of the work that OMB, DHS and CIGIE undertook in the past (5) years to move the IG assessments to a maturity model approach. This is the third year that all FISMA security domains were assessed using a maturity model.

For FY 2019, updates were made to the IG FISMA questions, as reported in the FY 2019 IG FISMA Reporting Metrics Version 1.3, dated April 9, 2019, which include:

- The FY 2019 CIO FISMA Metrics, OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program, and DHS' Binding Operational Directive 18-02, Securing High Value Assets, have placed additional emphasis on the enhancement of the High Value Asset (HVA) program. As such, the FY 2019 IG FISMA Reporting Metrics include additional maturity indicators and criteria references regarding the evaluation of the effectiveness of agencies' HVA programs.
- On December 21, 2018, the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act of 2018 (SECURE Technology Act) established new requirements for supply chain risk management. The FY 2019 IG FISMA Metrics have been updated to gauge agencies' preparedness in addressing these new requirements while recognizing that specific guidance will be issued at a later date.

The FY 2019 IG FISMA Reporting Metrics are grouped into eight domains and organized around the five Cybersecurity Framework function areas:

*Table 1: Alignment of the Cybersecurity Framework with the IG FISMA Domains*

| Cybersecurity Framework Function Areas | IG FISMA Domains |
|---|---|
| **Identify** | Risk Management |
| **Protect** | Configuration Management<br>Identity and Access Management<br>Data Protection and Privacy<br>Security Training |
| **Detect** | Information Security Continuous Monitoring (ISCM) |
| **Respond** | Incident Response |
| **Recover** | Contingency Planning |

### *Reporting Metrics*

For the FY 2019 IG FISMA Metrics, a series of metrics (or questions) was developed for each IG FISMA domain (Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning) to assess the effectiveness of an agency's cybersecurity framework function areas (Identify, Protect, Detect, Respond and Recover).

### *Maturity Level Scoring*

The maturity level scoring was prepared by OMB and DHS. Level 1 (Ad-hoc) is the lowest maturity level and Level 5 (Optimized) is the highest maturity level. The details of the five maturity model levels are:

1. Level 1 (Ad-hoc): Policies, procedures and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
2. Level 2 (Defined): Policies, procedures and strategies are formalized and documented but not consistently implemented.
3. Level 3 (Consistently Implemented): Policies, procedures and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4. Level 4 (Managed and Measurable): Quantitative and qualitative measures on the effectiveness of policies, procedures and strategies are collected across the organization and used to assess them and make necessary changes.
5. Level 5 (Optimized): Policies, procedures and strategies are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

Per OMB and DHS, within the context of the maturity model, Level 4 (Managed and Measurable) represents an "effective" level of security.

### *HHS Shared Responsibility Model*

The HHS cybersecurity program follows a shared responsibility model that informally recognizes that the Department, the HHS OPDIVs and third-party stakeholders (including contractors) are critical to risk management. This model also recognizes that the responsibilities for certain aspects of risk management change between each stakeholder, depending upon the roles assigned to defining, implementing and overseeing the operation of any given control. Assignments for those activities can and do change over time, often in conjunction with changes implemented to increase control maturity and especially where control implementation strategies change among centralized, federated and hybrid implementation strategies.

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

The Office of the Chief Information Officer (OCIO) leads the development and implementation of enterprise information technology (IT) infrastructure across HHS. The office establishes and provides support for: e-government initiatives; IT operations management; IT investment analysis; cybersecurity and privacy; performance measurement; policies to provide improved management of information resources and technology; strategic development and implementation of information systems and infrastructure; and technology-supported business process reengineering.

The HHS Chief Information Security Officer (CISO) is responsible for developing and maintaining the Department's information security and privacy program. This enterprise-wide program is designed to help protect HHS against cybersecurity threats. The OCIO information security and privacy program plays an important role in protecting HHS' ability to provide mission-critical operations by issuing security and privacy policies, standards and guidance; overseeing the completion of privacy impact assessments; providing incident reporting policy and incident management guidelines; and promoting IT security awareness and training.

Each OPDIV's CIO is responsible for establishing, implementing and enforcing an OPDIV-wide framework to facilitate its cybersecurity program based on policies and standards provided by the HHS CIO and CISO. The OPDIV CISOs are responsible for implementing department and OPDIV cybersecurity policies and procedures.

Third-party stakeholders are responsible for executing the cybersecurity and privacy program as defined by HHS and each OPDIV on behalf of HHS.

Section II

# Conclusion and Enterprise-wide Recommendations

# Section II: Conclusion and Enterprise-wide Recommendations

### *Conclusion*

Our specific conclusions related to HHS' cybersecurity program for each of the FISMA domains are based on the FISMA reporting metrics in Appendix C.

Based on the results of our evaluation, we determined that HHS' cybersecurity program was "Not Effective", as it did not meet the criteria required to be assessed at a "Managed and Measurable" maturity level for any of the five function areas: Identify, Protect, Detect, Respond and Recover.

### *Progress for FY 2019*

Table 2 below provides a comparison from the FY 2018 and FY 2019 IG FISMA Metrics. For FY 2019, the HHS Security Program strengthened its controls maturity for several individual IG FISMA Metric questions.

*Table 2: FY 2018 and 2019 HHS Maturity Levels*

| Maturity Level | FY 2018 IG FISMA Metrics | FY 2019 IG FISMA Metrics |
|---|---|---|
| **Defined** | 21 | 17 |
| **Consistently Implemented** | 36 | 42 |
| **Managed and Measurable** | 2 | 0 |

IG FISMA Reporting Metrics are assessed based on a selection of HHS OPDIVs and the aggregation of their results. The FY 2018 and FY 2019 IG FISMA reporting metrics may not be comparable since the selection of OPDIVs to be assessed changes from year to year. Also, the scope of testing of some IG FISMA reporting metrics differed in each year of the assessment, which can affect the IG assessment of the individual metrics and the overall assessment of each FISMA domain and function area.

***Recommendations***

To strengthen HHS' enterprise-wide cybersecurity program and further enhance its mission, we recommend the following:

- HHS should commit to creating and implementing a Cybersecurity Maturity Migration Strategy to advance the cybersecurity program from its current maturity state to an effective state across HHS. This strategy should include the following:
  - Perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on your missions and risks faced, risk appetite, and risk tolerance level.
  - Identify gaps between the current state at each OPDIV and the criteria required to reach the optimal level across HHS' enterprise-wide cybersecurity program and develop security controls to implement effective security.
  - Ensure the requirements for all metrics is Consistently Implemented or higher are achieved.
  - Articulate roles and shared responsibilities needed to meet the requirements for effective maturity, including whether requirements are to be implemented through centralized, federated, or hybrid controls.
- HHS should continue to provide department-wide guidance and DHS-supplied Continuous Diagnostics and Mitigation (CDM) tools to each OPDIV for the implementation of their ISCM programs.
- The Information Security and Privacy Policy (IS2P) is HHS' primary policy document governing cybersecurity which is pending a rewrite to address the upcoming requirements in NIST 800-53 revision 5. When this update occurs to the IS2P, HHS should:
  - Specify required cybersecurity control maturity levels in addition to identifying the selection of NIST controls.
  - Describe HHS' Cybersecurity Shared Responsibility Model, including the key roles under centralized, federated and hybrid strategies for control implementation. Include responsibilities of the OCIO, the OPDIVs, and third-party stakeholders (including contractors).
  - Communicate that a Managed and Measurable or the optimal maturity level, based on HHS's risk assessment, be required to be deemed "Effective".

***HHS OCIO Response:***

HHS OCIO concurred with our recommendations. HHS OCIO is drafting the Cybersecurity Risk Management Memo, which will provide details into the risk management strategy and approach diagram. Details will include how HHS intends to assess risk, respond to risk, and monitor risk. The finalized memo will be transmitted to the HHS Division Heads and HHS Division CIO's and CISO. The HHS OCIO will also update the IS2P to address NIST 800-53 revision 5 once NIST issues the final publication.

Section III

# Department and OPDIV Findings and Recommendations

# Section III: Department and OPDIV Findings and Recommendations

This section consolidates findings identified at each of the selected OPDIVs reviewed. It also includes recommendations that should support the Department to achieve a higher maturity state. We identified several findings in HHS' security program and consolidated them into each of the eight domains below:

| *Function* | *Identify* | *Protect* | | | | *Detect* | *Respond* | *Recover* |
|---|---|---|---|---|---|---|---|---|
| **Domain** | **Risk Management** | **Configuration Management** | **Identity & Access Management** | **Data Protection & Privacy** | **Security Training** | **ISCM** | **Incident Response** | **Contingency Planning** |
| OIG Assessed Maturity | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Defined (Level 2) |
| Change FY 2019 Audit vs FY 2018 | No Change | Upgraded from Defined | No Change | No Change | No Change | Upgraded from Defined | Upgraded from Defined | No Change |

## Identify

The goal of the Identify function is to develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. This area is the foundation that allows an agency to focus and prioritize its efforts with its risk management strategy and business needs. Within this function, there is one domain, Risk Management, for evaluation within the IG metrics. Our overall assessment of this function was "Not Effective."

### Risk Management

The Risk Management Framework, developed by NIST, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. A risk management framework is the foundation on which an IT security program is developed and implemented by an entity. A risk management framework should include: an assessment of management's long-term plan, documented goals and objectives of the entity, clearly defined roles and responsibilities for security management personnel, and prioritization of IT needs.

| Cybersecurity Framework Function Area | IG FISMA Domain | FY 19 IG Assessment | Change from FY 18 IG Assessment |
|---|---|---|---|
| **Identify** | Risk Management | Consistently Implemented | No change |

HHS' risk management function has the following in place:

- Established a risk management framework for evaluating and reporting risks.
- Provided an overarching IT strategy to OPDIVs to guide leaders as they make risk decisions.
- HHS Office of the CISO hosts monthly meetings to communicate emerging risks and trends to individual OPDIVs.
- Selected OPDIVs followed the defined process for identification, assessment, response and monitoring of IT risks.
- Selected OPDIVs maintain inventories of their information systems.
- Uses 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.
- Categorization and communication of the importance/priority of information systems in enabling its missions and business functions.
- Establishment, communication and implementation of its risk management policies, procedures and strategy, including for supply chain risk management.
- Uses an information security architecture to provide a disciplined and structured methodology for managing risk.
- Defined and communicated roles and responsibilities of internal and external stakeholders involved in risk management processes.
- Plans of action and milestones (POA&Ms) are utilized for mitigating security weaknesses.
- Definition, communication and implementation of its policies and procedures for conducting system-level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework; (ii) internal and external asset vulnerabilities, including through vulnerability scanning; (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities; and (iv) security controls to mitigate system-level risks.
- Information about risks is communicated in a timely manner to all necessary internal and external stakeholders.
- 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.
- Technology is used to provide a centralized, enterprise-wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies and risk scores/levels.

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

***Risk Management Finding and Recommendations***

The following finding was identified with HHS' risk management program:

- The POA&Ms reported by the Department for one OPDIV and those reported by that OPDIV did not reconcile during our point-in-time test of the May 2019 Weakness Report. The OPDIV did not address the non-reconciling items within a timely manner.

  The absence of a complete and accurate list of POA&Ms at the Department level could lead to the OPDIV and HHS leadership placing reliance on inaccurate information when making risk decisions.

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

  - Review the monthly reconciliation report, currently provided by the HHS OCIO, to ensure that discrepancies on the POA&M exception report are corrected to enable accurate OPDIV and Department-level reporting.

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

***HHS OCIO Response:***

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

## Protect

The goal of the Protect function is to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event and incorporates the domains of Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training.

| Cybersecurity Framework Function Area | IG FISMA Domain | FY 19 IG Assessment | Change from FY 18 IG Assessment |
|---|---|---|---|
| **Protect** | Configuration Management | Consistently Implemented | Upgrade from Defined |
| **Protect** | Identity and Access Management | Consistently Implemented | No change |
| **Protect** | Data Protection and Privacy | Consistently Implemented | No change |
| **Protect** | Security Training | Consistently Implemented | No change |

### Configuration Management

Configuration management involves activities that pertain to the operations, administration, maintenance and configuration of networked systems and their security posture. Areas of configuration management include standard baseline configurations, anti-virus management and patch management.

HHS' configuration management function has the following in place:

- Defined guidelines for the appropriate security configuration of information systems.
- Established roles and responsibilities to be implemented at the OPDIVs.
- Definition of information system configuration management policies and procedures across the agency.
- Each OPDIV is responsible for the development of product-specific baselines, the implementation of those baselines and monitoring to determine the appropriate response to misconfigurations.
- Based on the complexity of the systems and associated architectures, each OPDIV and system owner can make risk-based decisions when implementing HHS requirements. When monitoring configuration management compliance, OPDIV programs range from manual to automated.
- Adoption of the Trusted Internet Connection (TIC) program to assist in protecting its network.
- Definition and implementation of configuration change control activities.

***Configuration Management Findings and Recommendations***

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

- An OPDIV's patches were not applied to address high-risk vulnerabilities within established time frames.

  Discovered vulnerabilities that are not patched timely increase risk of successful exploits from known threat actors.

- An OPDIV has not developed and documented an enterprise-wide configuration management plan.

  The absence of an enterprise-wide configuration management plan could lead to inconsistency in the configuration management principles, policies, standards and procedures across an OPDIV's technological landscape. Further, it increases the possibility that decisions made at the system level for an OPDIV's systems may not be consistent, compatible and in alignment with that OPDIV's strategic direction for its technology.

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

- Ensure that the OPDIVs cybersecurity management create and implement a patch management strategy to ensure that patches are installed timely as required by HHS and Federal requirements.
- Develop and document an enterprise-wide configuration management plan that allows for OPDIV-level and system-level configuration management plans to be created and implemented in alignment with the higher-level enterprise plans, to ensure that changes implemented at the system level are consistent with and made only after approval by the OPDIV, and that an HHS-level plan defines the role of the OPDIVs for the creation, implementation and execution of OPDIV-specific configuration management plans.
- Identify roles of stakeholders to ensure proper identification of responsibilities in a shared responsibility environment.
- Communicate the enterprise-wide configuration management plan to all HHS system owners and stakeholders.
- Implement the enterprise-wide configuration management plan, working with system owners to align system configuration management plans with the enterprise plan.

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

***HHS OCIO Response:***

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

### Identity and Access Management

Federal agencies are required to establish procedures to limit access to physical and logical assets and associated facilities to authorized users, processes and devices. An appropriate monitoring process should also be implemented to validate that information system access is limited to authorized transactions and functions for each user based on the concept of least privilege.

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

- A defined identity, credential and access management program with established roles and responsibilities.
- OPDIVs have implemented HHS requirements to establish identity and access management controls.
- Use of an Identity, Credential and Access Management (ICAM) strategy to guide its ICAM processes and activities.
- Defined and implemented ICAM policies and procedures.
- Use of 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.
- Implementation of strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks and systems, including for remote access.
- Appropriate configuration/connection requirements for remote access connections, including the use of appropriate cryptographic modules and system time-outs.

#### *Identity and Access Management Findings and Recommendations*

The following finding was identified with HHS' identify and access management program:

- At one OPDIV, not all selected personnel with privileged access to OPDIV systems had a current background investigation on file.

  If background investigations are not conducted on all individuals with privileged access to OPDIV information systems, there is a potential risk to the information systems and the information itself on these information systems these individuals can access.

- OPDIVs require privileged users to sign a "privileged user rules of behavior agreement" as part of the access request process. However, signed copies of the Rules of Behavior are neither being collected nor maintained for privileged users at one OPDIV.

  The lack of signed copies of Privileged Account Rules of Behavior being collected and maintained may leave HHS without assurance that individuals with privileged access understand their critical

cybersecurity responsibilities in safeguarding the OPDIV's assets against compromise to their confidentiality, integrity and availability.

- At one OPDIV, not all selected systems reviewed implemented a strong authentication mechanism (PIV or a Level of Assurance 4 credential) for privileged and non-privileged user access.

  A lack of strong authentication for privileged and non-privileged users could lead to unauthorized access, resulting in unauthorized changes being made to production data. Such changes could lead to disclosure of confidential information, diminished system integrity or the inability of a system to perform as needed to meet the needs of its intended users.

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

- Conduct background checks on all personnel with information system access before they are granted access. The OPDIV should also conduct reinvestigations on these individuals in accordance with current personnel security policy.
- Create and implement a process to require privileged users to sign a privileged user rules of behavior agreement for all systems prior to provisioning privileged access to those systems.
- Establish a repository to retain signed copies of privileged user rules of behavior agreements for holders of privileged access for all systems.
- Ensure implementation of strong authentication mechanisms for privileged and non-privileged users to all OPDIV systems using multifactor PIV credentials, NIST 800-63 Identity Assurance Level 3/Authenticator Assurance Level 3/Federated Assurance Level 3 credential or other strong authentication for non-privileged and privileged users.

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

***HHS OCIO Response:***

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

### Data Protection and Privacy

Federal agencies have unique access to personally identifiable information (PII) and personal health information (PHI) of US citizens. Many of HHS systems contain PII and PHI, including systems that support the Medicare program and its 60 million beneficiaries. The underlying principle of data privacy and protection controls is to protect the confidentiality of information stored on information systems. To protect this information, Federal regulations have been established requiring agencies to report when this information is stored, how it is protected, and when breaches occur.

HHS' data protection and privacy function has the following in place:

- HHS has a defined privacy program including a defined plan and guidelines.
- The guidelines have been communicated to the OPDIVs.
- The OPDIVs we reviewed had a process in place for the development of privacy impact assessments, standard controls to be implemented and breach response processes; established roles and responsibilities; security requirements; and an enterprise breach response process for monitoring.
- The OPDIVs we reviewed have tailored their own privacy programs to implement the broader HHS guidelines and have integrated their incident response and privacy breach response program.
- Privacy awareness training is provided to all individuals, including role-based privacy training.
- Each OPDIV had integrated privacy controls within its risk management process and reporting vulnerabilities and weaknesses accordingly.
- Each OPDIV followed a breach response plan to respond to privacy events.
- Privacy awareness training is provided.

#### *Data Protection and Privacy Findings and Recommendations*

The following finding was identified with HHS' Data Protection and Privacy Program:

- At one ODPDIV, not all selected systems had Privacy Impact Assessments (PIA) completed and evidenced by signature within the three-year renewal time frame required by the HHS-OCIO Policy for PIA.

  Changes within systems, and to the internal and external environments in which they exist, may occur that directly, or indirectly, affect the risk profile of those systems over time. The absence of a timely PIA may result in increased risk. The public entrusts HHS with a wide array of personal information ranging from basic identifiers, such as name and Social Security number, to more complex data, such as an individual's genomic sequence or medical history. This public trust carries with it a corresponding responsibility that HHS protect and safeguard the information while it is being stored, transmitted and shared by HHS. Given that HHS handles a large amount of PII, it is critical that HHS protects PII and retains the public's trust.

We recommend that the HHS OCIO:

- Periodically sample systems to ensure that PIAs are created and maintained for all systems that require one.
- Work with the OPDIVs to ensure that all PIAs are reviewed, approved and signed by the appropriate HHS personnel at a minimum within three (3) years of the last PIA approval date.

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

***HHS OCIO Response:***

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

### Security Training

An effective IT security program cannot be established and maintained without giving a sufficient amount of training to its information system users. Federal agencies and organizations cannot protect the confidentiality, integrity and availability of information in today's highly networked systems environment and secured physical locations without providing their personnel adequate security training.

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

- Established security and training content, requirements for varying levels of individuals based on their access and completed workforce assessments.
- OPDIVs have a security and training program, which includes monitoring and tracking of users who needed additional training to meet requirements.
- OPDIVs report workforce shortfalls to HHS and discuss security training requirements and their associated training budget at the monthly CISO Council meetings.
- Use of a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to the HHS culture.
- Definition and implementation of security awareness and specialized security training policies and procedures.
- Providing security awareness training to all system users that is tailored based on its organizational requirements, culture and types of information systems.
- Providing specialized security training to all individuals with significant security responsibilities.

#### *Security Training Findings and Recommendations*

The following findings were identified with HHS' security awareness training program:

- One OPDIV did not have processes sufficiently defined and implemented to oversee and manage the completion of required security awareness training by users of contractor-owned and contractor-operated OPDIV systems.

  Without obtaining training completion certificates, ensuring that the training was successfully completed, the OPDIV presents an opportunity for untrained users to make security-related errors or mistakes that are avoidable through training, resulting in a decrease in the confidentiality, integrity or availability of one or more OPDIV systems.

- One OPDIV could not provide evidence that all users with significant security responsibilities had completed the annual Role-Based Training (RBT) and were in compliance with the requirements set forth by HHS.

  The lack of role-based training/specialized training for users with significant security responsibilities presents an opportunity for information systems to be accessed without collection, maintenance or dissemination during that three-year period that impacts the system's privacy posture.

We recommend that the HHS OCIO work with the ODPIVs ensure that:

- OPDIVs' security management improve their processes to consistently and accurately track training to ensure that everyone has taken the training prior to granting them system access. Obtain and retain training certificates as evidence of completed training.
- Role-based training is obtained for all users with significant security responsibilities before granting access to the system and annually thereafter.
- A process be designed and implemented that ensures the collection and maintenance of artifacts evidencing the successful completion of annual RBT for all users with significant security responsibilities.

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

***HHS OCIO Response:***

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

## Detect

The goal of the Detect function is to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events. The domain within this function is Information Security Continuous Monitoring (ISCM). Our overall assessment of this function was "Not Effective".

### Information Security Continuous Monitoring

An ISCM program allows an organization to maintain the security authorization of an information system over time in a dynamic environment of operations with changing threats, vulnerabilities, technologies and business processes. The implementation of a continuous monitoring program results in ongoing updates to system security plans, a periodic security assessment and POA&Ms, which are three principal documents in a security authorization package.

| Cybersecurity Framework Function Area | IG FISMA Domain | FY 19 IG Assessment | Change from FY 18 IG Assessment |
|---|---|---|---|
| **Detect** | ISCM | Consistently Implemented | Upgrade from Defined |

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

- "HHS Information Security Continuous Monitoring Strategy" was released in May 2017 to define and communicate the enterprise ISCM strategy.
- Formalization of its ISCM program through development of ISCM policies, procedures and strategies.
- An ISCM strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM.
- ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy.
- Defined ISCM roles, responsibilities, levels of authority and dependencies have been communicated across the organization.

***ISCM Findings and Recommendations***

The following findings were identified with HHS' ISCM program:

- Systems owners at selected OPDIVs did not renew their Authority to Operate (ATO) on a timely basis. Additionally, some Security Control Assessments (SCA) for systems were past due.

  Failure to renew ATOs for systems that continue to operate in the production environment resulted in the OPDIV allowing unauthorized systems to operate in its environment without the assurance that system security plans identify risks currently facing those applications, controls are in place and operating effectively in mitigating those risks, and that overall system risk profiles are within OPDIV tolerances and accepted by management.

- Although progress is being made to implement CDM, HHS is still working to operationalize CDM at select OPDIVs. Changes to support CDM are needed to both technology and processes. The Department is constrained in what it can drive for implementation by the following, all of which are controlled at the OPDIV level: budget, authority, schedule, integration, speed and priority.

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

  We recommend that the HHS OCIO work with the OPDIVs to ensure that they:

  - Plan and execute resource staffing such that ATOs are kept up to date without a lapse of authorization.
  - Obtain waiver or acceptances of risk approved by senior OPDIV management for those systems continuing to operate in the production environment without authorization.
  - Plan and execute resource staffing such that SCAs are kept up to date as needed to support the ATO process.

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

  ***HHS OCIO Response:***

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

## Respond

The goal of the Respond function is to develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity event and is defined by the incident response program. The domain within this function is incident response. Our overall assessment of this function was "Not Effective".

### Incident Response

Incident response involves capturing general threats and incidents that occur in the HHS systems and physical environment. Incidents are captured by systematically scanning IT network assets for any potential threats, or they are reported by affected persons to the appropriate personnel.

| Cybersecurity Framework Function Area | IG FISMA Domain | FY 19 IG Assessment | Change from FY 18 IG Assessment |
|---|---|---|---|
| **Respond** | Incidence response | Consistently implemented | Upgrade from Defined |

HHS' incident response function has the following in place:

- Established monitoring requirements for security incidents identified across the enterprise.
- Use of common attributes to classify incidents and implement its processes for incident detection, analysis and prioritization.
- Defined and implemented incident response policies, procedures, plans and strategies, as appropriate, to respond to cybersecurity events.
- Defined and communicated incident response team structures/models, stakeholders and their roles, responsibilities, levels of authority and dependencies.
- Implemented processes for incident detection and analysis.
- Implemented processes for incident handling.
- Timely sharing of incident response information with individuals with significant security responsibilities and reporting to external stakeholders.
- Collaboration with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents.
- Use of technology to support its incident response program.

### *Incident Response Findings and Recommendations*

The following finding was identified with HHS' incident response program:

- One OPDIV has not implemented incident profiling techniques to predict and categorize the potential for attacks on OPDIV assets, based on observed behaviors, to provide attack defenders with analysis of probable attackers' profiles, identification of their most desirable asset targets and the most probable attack vector scenarios that could be used to exploit them.

Without incident profiling techniques, HHS does not have the ability to make the most effective risk-based decisions regarding what assets are most in need of protection, the identification of those who could be most interested in adversely controlling them, and the scenarios and attack vectors the attacker is most likely to use to exploit weaknesses and impact the confidentiality, integrity and availability of those assets.

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

- Define a threat profiling framework that structures and standardizes threat profiling at the OPDIV.
- Implement threat profiling techniques within the defined framework that helps management understand where the OPDIV's high-value assets are located, who could be interested in taking control of them, and what attack vectors and under which scenarios they would likely be used to exploit vulnerabilities to succeed in their pursuits.

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

***HHS OCIO Response:***

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

## Recover

The goal of the Recover function is to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. The domain that was assessed within this function is contingency planning. Our overall assessment of this function was "Not Effective".

### Contingency Planning

Contingency planning refers to a coordinated strategy involving plans, procedures and technical measures that enable the recovery of business operations, information systems and data after a disruption. Information system contingency planning is unique to each system. Each contingency plan should provide preventive measures, recovery strategies and technical considerations that are in accordance with the system's information confidentiality, integrity and availability requirements and the system impact level.

| Cybersecurity Framework Function Area | IG FISMA Domain | FY 19 IG Assessment | Change from FY 18 IG Assessment |
|---|---|---|---|
| **Recover** | Contingency planning | Defined | No change |

HHS' contingency planning function has the following in place:

- HHS has distributed its defined requirements to the OPDIVs for implementation at the system level.
- HHS communicates information on the planning and performance of recovery activities to internal stakeholders and executive management teams that is used to make risk-based decisions.
- Procedures related to the recovery of mission-essential and business functions are designated as the primary responsibility of the OPDIVs for implementation.

***Contingency Planning Findings and Recommendations***

- At one OPDIV, not all systems were in compliance with the requirement to perform contingency plan testing at least annually.

The lack of contingency plan testing could result in insufficient preparedness needed to respond to an actual contingency event, and ultimately risk failure to meet system-established recovery point and recovery time objectives.

We recommend that the HHS OCIO:

- Require each OPDIV to develop a POA&M to implement activities required to achieve an effective maturity level for contingency planning, pending HHS risk assessment.
- Work with the OPDIVs to monitor and validate each OPDIV's implementation progress, which should include periodically sampling HHS systems to ensure the effectiveness of contingency plans, including adequate testing based on system categorization.

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

***HHS OCIO Response:***

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

# Appendices

# Appendix A: Audit Scope and Methodology

### *Scope*

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

The FY 2019 IG FISMA reporting metrics were assessed at selected HHS OPDIVs and based on the aggregation of their results.

We performed our fieldwork at the HHS OCIO and four HHS OPDIVs during the FY 2019 performance audit:

- Centers for Disease Control and Prevention
- Centers for Medicare & Medicaid Services (CMS)
- Health Resources and Services Administration
- Office of the Secretary (OS)

The FY 2018 and FY 2019 IG FISMA reporting metrics may not be comparable since some of the OPDIVs reviewed are different in each assessment year. Also, the scope of testing of some of the FY 2019 IG FISMA reporting metrics differed from the testing in FY 2018, which can affect the IG assessment of the individual metrics and the overall assessment of each FISMA domain and function.

### *Methodology*

To accomplish our objective, we:

- Reviewed applicable Federal laws, regulations and guidance.
- Gained an understanding of the current security program at HHS and selected OPDIVs.
- Inquired of OCIO and OPDIV personnel their self-assessment for each FISMA reporting metric.
- Assessed the status of HHS' security program against HHS and selected OPDIV cybersecurity program policies, other standards and guidance issued by HHS management, and reporting metrics.
- Inspected and analyzed selected artifacts including but not limited to: system security plans, evidence to support testing of security controls, POA&M records, security training records, asset compliance reports, system inventory reports and account management documentation.
- Inspected internal assessments performed on behalf of HHS and OPDIVs' managements that had a similar scope to the FY19 IG FISMA metrics. Incorporated the results as part of the FY19 IG FISMA metrics.

- Inspected results from GAO and OIG audits and reports that had a similar scope to the FY19 IG FISMA metrics. Incorporated the results as part of the FY19 IG FISMA metrics.

We conducted these procedures in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix B: Federal Requirements and Guidance

The principal criteria used for this audit included:

- Assistant Secretary for Administration Office of Security and Strategic Information (ASA OSSI), *HSPD-12 Implementation Policy for the Use of the Personal Identity Verification (PIV) Card for Strong Authentication* (January 13, 2017).
- ASA OSSI Cybersecurity, Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response (April 5, 2010).
- CMS The Risk Management Handbook Volume 1 Chapter 1 Risk Management XLC (November 8, 2012).
- DHS Binding Operational Directive 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems, (April 29, 2019).
- Federal Information Security Modernization Act of 2014 (December 2014).
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (February 2004).
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006);
- HHS Cybersecurity Program, Standard for Encryption of Computing Devices and Information (December 14, 2016).
- HHS Office of Information Security, High Value Asset Program Policy (March 2018).
- HHS OCIO, Information Systems Security and Privacy Policy (July 30, 2014).
- HHS OCIO, HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII) (June 29, 2017).
- HHS OCIO, HHS Policy for Enterprise Architecture (EA) (August 07, 2008).
- HHS OCIO, HHS Policy for Privacy Impact Assessments (PIA) (June 4, 2019).
- HHS OCIO, HHS System Inventory Management Standard (December 27, 2018).
- HHS OCIO, Minimum Security Configuration Standards Guidance (October 5, 2017).
- HHS OCIO, Policy for Information Technology (IT) Enterprise Performance Life Cycle (EPLC) (November 30, 2016).
- HHS OCIO, HHS Policy for Privacy Impact Assessments (PIA) (June 4, 2019).
- HHS Standard for Plan of Action and Milestones (POA&M) Management & Reporting (September 4, 2013).
- Homeland Security Presidential Directive 12 (HSPD 12): Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004).
- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems (May 2010).
- NIST SP 800-37, revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (June 2014).
- NIST SP 800-53, revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (January 22, 2015).
- NIST SP 800-61, Computer Security Incident Handling Guide (August 2012).
- OS Server Patch Management Process, Standard Operating Procedures (June 16, 2017).
- OS Procedures Handbook for Information Security (June 29, 2017).

- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).
- OMB M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements (October 16, 2017).
- US-CERT Federal Incident Notification Guidelines.

# Appendix C: FY 2019 Inspector General FISMA Reporting Metrics

Appendix C contains a system-generated report exported from the CyberScope FISMA Reporting Application. CyberScope is maintained by DHS and OMB. The HHS OIG entered its FY 2019 FISMA audit results and narrative comments into the CyberScope system. The report begins on the following page.

# Inspector General

Section Report

2019

Annual FISMA Report

## Department of Health and Human Services

## Function 1: Identify - Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800- 53. Rev. 4: CA-3, PM-5, and CM8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

**Consistently Implemented (Level 3)**

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

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1).

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. Two OPDIVs have a Consistently Implemented process, one OPDIV has a Managed and Measurable process, and one OPDIV has a Defined 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.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level. Two OPDIVs reviewed are at the Defined level, one OPDIV reviewed is at the Consistently Implemented level, and one OPDIV is at the Managed and Measurable level for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting. The four OPDIVs reviewed did not ensure that the software assets on the network (and their associated licenses) are subject to the monitoring processes defined within the organization's ISCM strategy (Managed and Measurable level).

## Function 1: Identify - Risk Management

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03)?

**Consistently Implemented (Level 3)**

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

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. One OPDIV is at the Managed and Measurable level. Three OPDIVs did not monitor and analyze its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and collect, analyze and report information on the effectiveness of its risk management program (Managed and Measurable level).

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at the Defined level. The four OPDIVs reviewed did not integrate its security architecture with its systems development lifecycle and define and direct implementation of security methods, mechanisms, and capabilities to both the information and communications technology supply chain and the organization's information systems (Managed and Measurable level).

## Function 1: Identify - Risk Management

7 To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M19-03)?

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV reviewed at the Managed and Measurable level. Three OPDIVs did not utilize an integrated risk management governance structure for implementing and overseeing an enterprise risk management capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas (Managed and Measurable 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 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2); OMB M-19-03, CSF v1.1, ID.RA-6)?

**Consistently Implemented (Level 3)**

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

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

**Consistently Implemented (Level 3)**

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

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed did not employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization (Managed and Measurable level).

## Function 1: Identify - Risk Management

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at the Managed and Measurable level. Three OPDIVs did not use qualitative and quantitative performance metrics to measure, report on, and monitor information security performance of contractor-operated systems and services (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed did not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at the Consistently Implemented maturity level for its risk management program.

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

**The HHS risk management program is not effective since all aspects of its program are not at the Managed and Measurable maturity level. With full implementation of the CDM tools at the Department and OPDIV level, HHS should have the capability to move to a managed and measurable risk management program which should be effective across HHS.**

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## Function 2A: Protect - Configuration Management

## Function 2A: Protect - Configuration Management

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

**Consistently Implemented (Level 3)**

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

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with one OPDIV at the Consistently Implemented level. The four OPDIVs reviewed did not monitor, analyze, and report to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, use this information to take corrective actions when necessary, and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format (Managed and Measurable 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 REV. 4: CM-1; NIST SP 800-128: 2.2.1).?

**Consistently Implemented (Level 3)**

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

## Function 2A: Protect - Configuration Management

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2019CIO FISMA Metrics: 1.1,2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7and PR.IP-1)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level. For one OPDIV, baselines were not developed for platforms. The four OPDIVs reviewed did not employ automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact (Managed and Measurable level).

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, and SI-2; FY 2019CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1and DE.CM-8)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with two OPDIVs at the Consistently Implemented level. The four OPDIVs reviewed did not employ automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network (Managed and Measurable level).

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20,Control 4.5; FY 2019CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive(BOD)15-01; DHS BOD 18-02)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level, while two OPDIVs were at the Managed and Measurable level. Two of four OPDIVs reviewed did not centrally manage its flaw remediation process and utilize automated patch management and software update tools for operating systems (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

## Function 2A: Protect - Configuration Management

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2 and CM-3; CSF: PR.IP-3).?

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed did not monitor, analyze, and report on the qualitative and quantitative performance measures on the effectiveness of its change control activities and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format (Managed and Measurable level).

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

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

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## Function 2B: Protect - Identity and Access Management

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at the Defined level. The four OPDIVs reviewed did not ensure resources were allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

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

## Function 2B: Protect - Identity and Access Management

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

**Consistently Implemented (Level 3)**

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

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with two OPDIVs at the Consistently Implemented level. The four OPDIVs reviewed did not employ automation to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate (Managed and Measurable level).

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800- 53 REV. 4: AC-8, PL-4, and PS6)?

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level, with one OPDIV at the Defined level and one OPDIV at the Managed and Measurable level. Three OPDIVs reviewed did not use automation to centrally manage user access agreements for privileged and non-privileged users (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

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

## Function 2B: Protect - Identity and Access Management

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. Two OPDIVs reviewed were at the Managed and Measurable level, one OPDIV was at the Consistently Implemented level and one OPDIV did not ensure that all privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and therefore was at the Defined level.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level, with one OPDIV at the Consistently Implemented level, one OPDIV at the Managed and Measurable level and two OPDIVs at the Defined level. Three OPDIVs did not employ automated mechanisms to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate (Managed and Measurable level).

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10)?.

**Consistently Implemented (Level 3)**

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

## Function 2B: Protect - Identity and Access Management

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

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

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## Function 2C: Protect - Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at the Managed and Measurable level. Three OPDIVs reviewed did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and use that information to make appropriate adjustments as needed (Managed and Measurable level).

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

- Encryption of data at rest
- Encryption of data in transit
- Limitation of transfer to removable media
- Sanitization of digital media prior to disposal or reuse

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level, with two OPDIVs at the Consistently Implemented level. The four OPDIVs reviewed did not ensure that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy (Managed and Measurable level).

## Function 2C: Protect - Data Protection and Privacy

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with two OPDIVs reviewed at the Consistently Implemented level. The four OPDIVs reviewed did not measure the effectiveness of its data exfiltration and enhanced network defenses by conducting exfiltration exercises (Managed and Measurable level).

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at the Managed and Measurable level. Three OPDIVs reviewed did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan (Managed and Measurable level).

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs at the Managed and Measurable level and one OPDIV at the Defined level. Two OPDIVs reviewed did not measure the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII (Managed and Measurable level).

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

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

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## Function 2D: Protect - Security Training

## Function 2D: Protect - Security Training

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at the Consistently Implemented level with one OPDIV at the Managed and Measurable level.

40 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800- 50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with two OPDIVs at the Consistently Implemented level. All four OPDIVs reviewed have not addressed all of their identified knowledge, skills, and abilities gaps through the training or hiring of additional staff/contractors (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

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

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

**Consistently Implemented (Level 3)**

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

## Function 2D: Protect - Security Training

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs at the Managed and Measurable level. Two OPDIVs reviewed did not measure the effectiveness of its awareness training program (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

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

45.1 Please provide the assessed maturity level for the agency's Protect Function.

**Consistently Implemented (Level 3)**

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

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

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

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## Function 3: Detect - ISCM

## Function 3: Detect - ISCM

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at the Managed and Measurable level. Three OPDIVs reviewed did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of the ISCM strategy (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of the ISCM policies and procedures (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

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

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800- 137: Section 2.2; NIST SP 800- 53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with one OPDIV at the Consistently Implemented level. The four OPDIVs reviewed did not consistently utilize the results of security control assessments and monitoring to maintain ongoing authorizations of information systems (Managed and Measurable level).

## Function 3: Detect - ISCM

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

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with two OPDIVs at the Consistently Implemented level. The four OPDIVs reviewed did not integrate metrics on the effectiveness of the ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

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

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

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

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## Function 4: Respond - Incident Response

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with three OPDIVs reviewed at the Managed and Measurable level. One OPDIV did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of incident response policies, procedures, plans, and strategies (Managed and Measurable level).

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs reviewed at the Managed and Measurable level.

## Function 4: Respond - Incident Response

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; and US-CERT Incident Response Guidelines)

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with one OPDIV at the Managed and Measurable level. Three OPDIVs reviewed did not utilize profiling techniques to measure the characteristics of expected activities on their networks and systems so that they can more effectively detect security incidents (Managed and Measurable level).

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs reviewed at the Managed and Measurable level. Two OPDIVs reviewed did not manage and measure the impact of successful incidents in order to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability (Managed and Measurable level).

56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)

**Consistently Implemented (Level 3)**

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

57 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800- 86; NIST SP 800-53 REV. 4: IR- 4; OMB M-18-02; PPD-41).

**Consistently Implemented (Level 3)**

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

## Function 4: Respond - Incident Response

58 To what degree does the organization utilize the following technology to support its incident response program?

·Web application protections, such as web application firewalls

·Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools

·Aggregation and analysis, such as security information and event management (SIEM) products

Malware detection, such as antivirus and antispam software technologies

·Information management, such as data loss prevention

·File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level with two OPDIVs reviewed at the Managed and Measurable level. Two OPDIVs reviewed did not use technologies for monitoring and analyzing qualitative and quantitative performance across the organization and were not collecting, analyzing, and reporting data on the effectiveness of their technologies for performing incident response activities (Managed and Measurable level).

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

**Consistently Implemented (Level 3)**

**Comments:** HHS is at the Consistently Implemented maturity level.

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

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

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## Function 5: Recover - Contingency Planning

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

**Consistently Implemented (Level 3)**

**Comments:** Overall, HHS is at a Consistently Implemented maturity level. The four OPDIVs reviewed have not allocated resources in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are not held accountable for carrying out their roles and responsibilities effectively (Managed and Measurable level).

## Function 5: Recover - Contingency Planning

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

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level while two OPDIVs reviewed are at the Consistently Implemented level. The four OPDIVs reviewed did not manage their information and communications technology supply chain risks related to contingency planning activities (Managed and Measurable level).

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

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level. The four OPDIVs reviewed did not incorporate the results of organizational and system level BIAs into strategy and plan development efforts consistently (Consistently Implemented level).

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800- 53 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

**Defined (Level 2)**

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

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

**Defined (Level 2)**

**Comments:** Overall, HHS is at a Defined maturity level with two OPDIVs reviewed at the Consistently Implemented level. The four OPDIVs reviewed did not employ automated mechanisms to thoroughly and effectively test system contingency plans (Managed and Measurable level).

## Function 5: Recover - Contingency Planning

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?

**Defined (Level 2)**

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

66 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?

**Consistently Implemented (Level 3)**

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

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

**Defined (Level 2)**

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

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

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

**Calculated Maturity Level - Defined (Level 2)**

## Function 0: Overall

## Function 0: Overall

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

**Not Effective**

**Comments:**

Overall, HHS made strides within their organization by implementing changes which strengthened the enterprise-wide information security program. Through the evaluation of FISMA metrics, we determined that the HHS' information security program was 'Not Effective' since it was not at a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover functional areas. HHS's maturity level for Identify, Protect, Detect, and Respond were "Consistently Implemented", and Recover was "Defined". HHS is cognizant of opportunities which arise to strengthen the overall information security program which should help ensure that policies and procedures in place at all Operating Divisions (OPDIVs) are consistently implemented and in line with the requirements across their security programs. HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program in coordination with DHS with the ultimate goals of: 1.) Continuous monitoring of HHS networks and systems, 2.) Real-time reporting of OPDIVs status and progress to help address and implement strategies to combat risk, 3.) Prioritization of issues based on established risk criteria, and 4.) Improving federal cybersecurity response capabilities. Based on our assessment, the HHS CDM program has matured towards the last stages of being fully implemented at assessed OPDIVs. HHS needs to ensure that there is effective contingency planning, identity and access management, configuration management, and incident response using appropriate tools, processes, and controls at all OPDIVs. HHS should also continue to build towards a working model where all the functional areas interact with each other in real-time and provide holistic and coordinated responses to security events helping to strengthen all aspects of its information security program. These steps will help HHS achieve its mission through an effective and coordinated information security program.

## Function 0: Overall

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

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

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

**To assess and determine the effectiveness of HHS' information security program, we executed an assessment plan that helped determine the maturity level for the questions listed in the FISMA reporting metrics. We assessed the maturity levels and effectiveness across the Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, Data Protection & Privacy, and Security Training), Detect (Information Security Continuous Monitoring (ISCM)), Respond (Incident Response), and Recover (Contingency Planning) functional areas. In scope this year was the HHS Office of the CIO, and the following four HHS OPDIVs: Centers for Medicare & Medicaid Services, Centers for Disease Control and Prevention, Health Resources and Services Administration, and the Office of the Secretary. Two of the four OPDIVs in-scope this year were not reviewed last year. We also incorporated results from other IT audits and assessments. We reviewed HHS' and OPDIVs' policies, procedures, standards and other guidance, as well as examined corresponding artifacts.**

## APPENDIX A: Maturity Model Scoring

### Function 1: Identify - Risk Management

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

### Function 2A: Protect - Configuration Management

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

### Function 2B: Protect - Identity and Access Management

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

## Function 2C: Protect - Data Protection and Privacy

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

## Function 2D: Protect - Security Training

| Function | Count |
|---|---|
| Ad-Hoc | 0 |
| Defined | 1 |
| Consistently Implemented | 5 |
| Managed and Measurable | 0 |
| Optimized | 0 |
| **Function Rating: Consistently Implemented (Level 3)Not Effective** | |

## Function 3: Detect - ISCM

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

## Function 4: Respond - Incident Response

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

## Function 5: Recover - Contingency Planning

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

## Maturity Levels by Function

| Function | Calculated Maturity Level | Assessed Maturity Level | Explanation |
|---|---|---|---|
| Function 1: Identify - Risk Management | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Overall, HHS is at the Consistently Implemented maturity level for its risk management program. |
| Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Overall, HHS is at the Consistently Implemented level for Protect function. |
| Function 3: Detect - ISCM | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Overall, HHS is at the Consistently Implemented maturity level for the Detect function. |
| Function 4: Respond - Incident Response | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | HHS is at the Consistently Implemented maturity level. |
| Function 5: Recover - Contingency Planning | Defined (Level 2) | Defined (Level 2) | HHS and its OPDIVs have not consistently implemented its contingency planning functions, therefore HHS is at the Defined level. |

| | | | |
|---|---|---|---|
| Overall | Not Effective | Not Effective | Overall, HHS made strides within their organization by implementing changes which strengthened the enterprise-wide information security program. Through the evaluation of FISMA metrics, we determined that the HHS' information security program was 'Not Effective' since it was not at a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover functional areas. HHS's maturity level for Identify, Protect, Detect, and Respond were "Consistently Implemented", and Recover was "Defined". HHS is cognizant of opportunities which arise to strengthen the overall information security program which should help ensure that policies and procedures in place at all Operating Divisions (OPDIVs) are consistently implemented and in line with the requirements across their security programs. HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program in coordination with DHS with the ultimate goals of: 1.) Continuous monitoring of HHS networks and systems, 2.) Real-time reporting of OPDIVs status and progress to help address and implement strategies to combat risk, 3.) Prioritization of issues based on established risk criteria, and 4.) Improving federal cybersecurity response capabilities. Based on our assessment, the HHS CDM program has matured towards the last stages of being fully implemented at assessed OPDIVs. HHS needs to ensure that there is effective contingency planning, identity and access management, configuration management, and incident response using appropriate tools, processes, and |

| | | | |
|---|---|---|---|
| | | | controls at all OPDIVs. HHS should also continue to build towards a working model where all the functional areas interact with each other in real-time and provide holistic and coordinated responses to security events helping to strengthen all aspects of its information security program. These steps will help HHS achieve its mission through an effective and coordinated information security program. |

# Appendix D: HHS Comments

**DEPARTMENT OF HEALTH & HUMAN SERVICES** Office of the Secretary

Office of the Chief Information Officer
Washington, D.C. 20201

**DATE:** March 16, 2020

**TO:** Tamara Lilly, Assistant Inspector General for Audit Services

**FROM:** José L. Arrieta, Chief Information Officer

**SUBJECT:** Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2019 (A-18-19-11200)

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) 2019. We welcome the opportunity to respond to the report developed by Ernest & Young on your behalf.

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

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

Attachment A: Response from the Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2019 (A-18-19-11200)***

cc:
Janet Vogel, HHS Chief Information Security Officer
Christopher Bollerer, Acting HHS Deputy Chief Information Security Officer
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 2019 (A-18-19-11200)***

**Enterprise-wide Recommendations**

**OIG Recommendation:**

To strengthen HHS' enterprise-wide cybersecurity program and further enhance its mission, we recommend the following:

- HHS should commit to creating and implementing a Cybersecurity Maturity Migration Strategy to advance the cybersecurity program from its current maturity state to an effective state across HHS. This strategy should include the following:
  - Perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on your missions and risks faced, risk appetite, and risk tolerance level.
  - Identify gaps between the current state at each OPDIV and the criteria required to reach the optimal level across HHS' enterprise-wide cybersecurity program and develop security controls to implement effective security.
  - Ensure the requirements for all metrics is Consistently Implemented or higher are achieved.
  - Articulate roles and shared responsibilities needed to meet the requirements for effective maturity, including whether requirements are to be implemented through centralized, federated, or hybrid controls.

- The Information Security and Privacy Policy (IS2P) is HHS' primary policy document governing cybersecurity which is pending a rewrite to address the upcoming requirements in NIST 800-53 revision 5. For this update of the IS2P, HHS should:
  - Specify required cybersecurity control maturity levels in addition to identifying the selection of NIST controls.
  - Describe HHS' Cybersecurity Shared Responsibility Model, including the key roles under centralized, federated and hybrid strategies for control implementation. Include responsibilities of the OCIO, the OPDIVs, and third-party stakeholders (including contractors).
  - Communicate that a Managed and Measurable or the optimal maturity level, based on HHS's risk assessment, be required to be deemed "Effective".

**HHS Response: Concur**

HHS OCIO is drafting the Cybersecurity Risk Management Memo, which will provide details into the risk management strategy and approach diagram. Details will include how HHS intends to assess risk, respond to risk, and monitor risk. The intent is to transmit the finalized memo to the HHS Division Heads and HHS Division CIOs and CISOs. It will be aligned to the HHS ERM Framework and the HHS Office of Information Security (OIS) Strategic Plan. We will review the recommendations made by OIG and made appropriate updates to the OIS Strategic Plan and Cybersecurity Risk Management Memo.

In addition, HHS OCIO will update the IS2P to address NIST 800-53 revision 5. HHS OCIO is waiting on NIST to issue the final publication.

**Identity - Risk Management**

**OIG Recommendation:**

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

- Review the monthly reconciliation report, currently provided by the HHS OCIO, to ensure that discrepancies on the POA&M exception report are corrected to enable accurate OPDIV and Department-level reporting.

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

**HHS Response: Concur**

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

**Protect - Configuration Management**

**OIG Recommendation:**

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

- Ensure that the OPDIVs cybersecurity management create and implement a patch management strategy to ensure that patches are installed timely as required by HHS and Federal requirements.
- Develop and document an enterprise-wide configuration management plan that allows for OPDIV-level and system-level configuration management plans to be created and implemented in alignment with the higher-level enterprise plans, to ensure that changes implemented at the system level are consistent with and made only after approval by the OPDIV, and that an HHS-level plan defines the role of the OPDIVs for the creation, implementation and execution of OPDIV-specific

configuration management plans.

- Identify roles of stakeholders to ensure proper identification of responsibilities in a shared responsibility environment.
- Communicate the enterprise-wide configuration management plan to all HHS system owners and stakeholders.
- Implement the enterprise-wide configuration management plan, working with system owners to align system configuration management plans with the enterprise plan.

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

**HHS Response: Concur**

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

**Protect - Identity and Access Management**

**OIG Recommendation:**

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

- Conduct background checks on all personnel with information system access before they are granted access. The OPDIV should also conduct reinvestigations on these individuals in accordance with current personnel security policy.
- Create and implement a process to require privileged users to sign a privileged user rules of behavior agreement for all systems prior to provisioning privileged access to those systems.
- Establish a repository to retain signed copies of privileged user rules of behavior agreements for holders of privileged access for all systems.
- Ensure implementation of strong authentication mechanisms for privileged and non-privileged users to all OPDIV systems using multifactor PIV credentials, NIST 800-63 Identity Assurance Level 3/Authenticator Assurance Level 3/Federated Assurance Level 3 credential or other strong authentication for non-privileged and privileged users.

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

**HHS Response: Concur**

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

**Data Protection & Privacy**

**OIG Recommendation:**

We recommend that the HHS OCIO:

- Periodically sample systems to ensure that PIAs are created and maintained for all systems that require one.
- Work with the OPDIVs to ensure that all PIAs are reviewed, approved and signed by the appropriate HHS personnel at a minimum within three (3) years of the last PIA approval date.

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

**HHS Response: Concur**

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

**Protect - Security Training**

**OIG Recommendation:**

We recommend that the HHS OCIO work with the ODPIVs ensure that:

- OPDIVs' security management improve their processes to consistently and accurately track training to ensure that everyone has taken the training prior to granting them system access. Obtain and retain training certificates as evidence of completed training.
- Role-based training is obtained for all users with significant security responsibilities before granting access to the system and annually thereafter.
- A process be designed and implemented that ensures the collection and maintenance of artifacts evidencing the successful completion of annual RBT for all users with significant security responsibilities.

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

**HHS Response: Concur**

HHS OCIO received a copy of the OpDiv audit reports and is coordinating a review of the 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 work with the OPDIVs to ensure that they:

- Plan and execute resource staffing such that ATOs are kept up to date without a lapse of authorization.
- Obtain waiver or acceptances of risk approved by senior OPDIV management for those systems continuing to operate in the production environment without authorization.
- Plan and execute resource staffing such that SCAs are kept up to date as needed to support the ATO process.

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

**HHS Response: Concur**

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

**Respond - Incident Response**

**OIG Recommendations**

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

- Define a threat profiling framework that structures and standardizes threat profiling at the OPDIV.
- Implement threat profiling techniques within the defined framework that helps management understand where the OPDIV's high-value assets are located, who could be interested in taking control of them, and what attack vectors and under which scenarios they would likely be used to exploit vulnerabilities to succeed in their pursuits.

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

**HHS Response: Concur**

HHS OCIO received a copy of the OpDiv audit reports and is coordinating a review of the 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 recommend that the HHS OCIO:

- Require each OPDIV to develop a POA&M to implement activities required to achieve an effective maturity level for contingency planning, pending HHS risk assessment.
- Work with the OPDIVs to monitor and validate each OPDIV's implementation progress, which should include periodically sampling HHS systems to ensure the effectiveness of contingency plans, including adequate testing based on system categorization.

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

**HHS Response: Concur**

OCIO has received a copy of the OpDiv audit 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.