

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 2016**

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



Gloria L. Jarmon
Deputy Inspector General
for Audit Services

February 2017
A-18-16-30350

Office of Inspector General

<https://oig.hhs.gov>

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

Office of Audit Services

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

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Notices

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

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

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

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



Ernst & Young LLP
Westpark Corporate Center
8484 Westpark Drive
McLean, VA 22102

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

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

January 20, 2017

Dear Ms. Frontz:

Attached is our final report on the procedures conducted to evaluate the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) in accordance with the FY 2016 Inspector General FISMA Reporting Metrics (reporting metrics) provided by the Department of Homeland Security (DHS).

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

Our audit procedures were performed to provide our report as of September 30, 2016. The projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the information security program or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

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

Sincerely,

A handwritten signature in black ink that reads 'Ernst & Young LLP'. The signature is written in a cursive, flowing style.



Ernst & Young LLP
Westpark Corporate Center
8484 Westpark Drive
McLean, 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

Ms. Amy J. Frontz
Assistant Inspector General for Audit Services

We have conducted a performance audit of the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2016, with the objective of assessing HHS FISMA compliance as defined in the FY 2016 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 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.

To assess HHS FISMA compliance, we utilized 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 OIG, DHS, 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

January 20, 2017
McLean, Virginia

EXECUTIVE SUMMARY

We conducted a performance audit of the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2016 based upon the questions outlined in the FISMA reporting metrics for the Inspectors General.

BACKGROUND

On December 17, 2002, the President signed the FISMA into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and provide a mechanism for improved oversight of Federal agency information security programs. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendments included the: (1) reestablishment of the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

To comply with the FISMA, the OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FY 2016 FISMA reporting metrics in consultation with the Federal Chief Information Officer Council. FISMA requires Inspectors General to perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of such program and practices, including (1) testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems; and (2) an assessment of the effectiveness of the information security policies, procedures and practices of the agency. This 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*.

WHAT WE FOUND

Our conclusions relative to HHS compliance with the FISMA reporting metrics for the Inspectors General are presented in Appendix C. Overall, in comparison to the prior year's FISMA review, HHS has made improvements. Specifically, the number of findings have decreased from year to year. In addition, HHS and its OPDIVs have implemented continuous monitoring tools that have allowed them to gain more insight to the security compliance of their assets. HHS continues to implement changes to strengthen its enterprise-wide information security program. HHS has formalized its Information Security Continuous Monitoring (ISCM) program through development of ISCM policies, procedures, and strategies. DHS has put in place requirements that focus on "real-time" monitoring of systems controls. The Continuous Diagnostics and Mitigation (CDM) program - implemented by DHS - includes continuously monitoring its networks and systems, updating and finalizing policies and procedures, indicating how documenting OPDIVs'

progress to address and implement strategies, and reporting its progress through DHS dashboards. HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS. HHS and its OPDIVs have made progress by implementing these tools and are working on the “real-time” monitoring of their security controls.

However, despite the progress made to improve the HHS and its OPDIV’s information security program, opportunities to strengthen the overall information security program exist. We continued to identify weaknesses in the following areas: continuous monitoring, configuration management, identity and access management, risk management, incident response, security training, contingency planning, and contractor systems.

HHS needs to ensure that all OPDIVs consistently review and remediate or address the risk presented by vulnerabilities discovered, consistently implement account management procedures, and accurately track systems to ensure they are operating with a current and valid Authority to Operate. These steps will strengthen the program and further enhance the HHS mission.

Exploitation of weaknesses we identified could result in unauthorized access to, and disclosure of, sensitive information and disruption of critical operations at HHS. As a result, we believe the weaknesses could potentially compromise the confidentiality, integrity, and availability of HHS’ sensitive information and information systems.

Recommendations

HHS should further strengthen its information security program. We made a series of recommendations as described in Section III to enhance information security controls at HHS and specific controls at the OPDIVs.

HHS Comments

In written comments to our draft report, HHS concurred with all of our recommendations and described actions it has taken and plans to take to implement them.

Table of Contents

INTRODUCTION	1
SECTION I – BACKGROUND	1
SECTION II – CONCLUSION	2
SECTION III – FINDINGS AND RECOMMENDATIONS.....	2
Finding #1 – Continuous Monitoring Management.....	3
Finding #2 – Configuration Management.....	5
Finding #3 – Identity and Access Management.....	6
Finding #4 – Incident Response and Reporting.....	7
Finding #5 – Risk Management.....	8
Finding #6 – Security Training.....	10
Finding #7 – Plan of Action and Milestones (POA&M)	11
Finding #8 – Contingency Planning	12
Finding #9 – Contractor Systems.....	13
APPENDIX A: AUDIT SCOPE AND METHODOLOGY	14
APPENDIX B: FEDERAL REQUIREMENTS and GUIDANCE	15
APPENDIX C: FY 2016 INSPECTOR GENERAL FISMA REPORTING METRICS	16
APPENDIX D: HHS RESPONSE.....	56

INTRODUCTION

We conducted a performance audit of the Department of Health and Human Services' (HHS) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2016 based upon the questions outlined in the FISMA reporting metrics for the Inspectors General.

SECTION I – BACKGROUND

On December 17, 2002, the President signed the FISMA into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and provide a mechanism for improved oversight of Federal agency information security programs. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendments included the: (1) reestablishment of the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

To comply with the FISMA, the OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FY 2016 FISMA reporting metrics in consultation with the Federal Chief Information Officer Council. FISMA requires Inspectors General to perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of such program and practices, including (1) testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems; and (2) an assessment of the effectiveness of the information security policies, procedures and practices of the agency. The FY 2016 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*.

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

HHS administers more than 100 programs across its operating divisions (OPDIVs) to protect the health of all Americans and provide essential health services, especially for those who are least able to help themselves. HHS' mission is to enhance and protect the health and well-being of all Americans and they fulfill that mission by providing for effective health and human services and fostering advances in medicine, public health, and social services. The Office of the Chief Information Officer (OCIO) serves this mission by leading the development and implementation of an enterprise information technology (IT) infrastructure across HHS. The office establishes and provides support for: E-Government initiatives; IT operations management; IT investment analysis; IT security and privacy; performance measurement; policies to provide improved management of information resources and technology; strategic development and application of information systems and infrastructure; and technology supported business process reengineering.

The OCIO is responsible for the Department's information security and privacy program. The HHS enterprise-wide information security and privacy program is designed to help protect HHS against potential IT threats and vulnerabilities. The program ensures compliance with federal mandates and legislation, including FISMA and the President's Management Agenda. This program plays an important role in protecting HHS' ability to provide mission-critical operations by providing a baseline for security and privacy policies and guidance; overseeing the guidance and completion of privacy impact assessments, providing incident reporting, policy and incident management guidelines, and promoting IT security awareness and training.

Each OPDIV's CIO is responsible for establishing, implementing, and enforcing an OPDIV-wide framework to facilitate its information security program based on guidance provided by the HHS CIO. The OPDIV Chief Information Security Officers are responsible for implementing Department and OPDIV IT security policies and procedures.

SECTION II – CONCLUSION

Our conclusions related to HHS' information security program are contained within the FISMA reporting metrics in Appendix C. Overall, in comparison to the prior year's FISMA review, HHS has made improvements. Specifically, the number of findings have decreased from year to year. In addition, HHS and its OPDIVs have implemented continuous monitoring tools that have allowed them to gain more insight to the security compliance of their assets. HHS continues to implement changes to strengthen its enterprise-wide information security program.

However, despite the progress made to improve the HHS and its OPDIV's information security program, opportunities to strengthen the overall information security program were identified. We continued to identify weaknesses in the following areas: continuous monitoring, configuration management, identity and access management, risk management, incident response, security training, and contractor systems.

HHS needs to ensure that all OPDIVs address all identified findings to include consistently review and remediate or address the risk presented by vulnerabilities discovered, consistently implement account management procedures, and accurately track systems to ensure they are operating with a current and valid Authority to Operate. These steps will strengthen the program and further enhance the HHS mission.

SECTION III – FINDINGS AND RECOMMENDATIONS

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

We identified several reportable exceptions in HHS' security program. The exceptions have been consolidated into nine findings for management consideration. Areas for improvement were identified in HHS' Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response, Risk Management, Security Training, Plan of Action and Milestones (POA&M), Contingency Planning, and Contractor Systems.

Finding #1 – Continuous Monitoring Management

An Information Security Continuous Monitoring (ISCM) program allows an organization to maintain the security authorization of an information system over time in a dynamic environment of operations with changing threats, vulnerabilities, technologies, and business processes. The implementation of a continuous monitoring program results in ongoing updates to the system security plan, the security assessment report, and the POA&M, which are the three principal documents in the security authorization package. OMB and DHS have updated the requirements to include documentation of an ISCM strategy, implementation of ISCM for information technology assets, incorporation of risk assessments to develop an ISCM strategy, and reporting of ISCM results in accordance with their strategy. HHS has formalized its ISCM program through development of ISCM policies, procedures, and strategies. DHS has put in place requirements that focus on “real-time” monitoring of systems controls. The Continuous Diagnostics and Mitigation (CDM) program - implemented by DHS - includes continuously monitoring its networks and systems, updating and finalizing policies and procedures, documenting OPDIVs’ progress to address and implement strategies, and reporting its progress through DHS dashboards. HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS. HHS and its OPDIVs have made progress by implementing these tools and are working on the “real-time” monitoring of their security controls. However, additional guidance from DHS is still outstanding on ISCM elements and requirements. This guidance is a critical input that will allow HHS to finalize and fully implement their continuous monitoring strategy.

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

- For one of the selected OPDIVs, policies and procedures were not updated and finalized for vulnerability management, patch management, asset management, and security management.
- For one of the selected OPDIVs, antivirus scanning did not include all workstations that were associated to the OPDIV’s workstation inventory.
- For one of the selected OPDIVs, instances of operational non-compliance with the OPDIV’s ISCM program requirements were identified. Specifically, the computers were not continuously monitored for prohibited software and a reconciliation was not performed to monitor its hardware assets.

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

Recommendation:

We recommend that the HHS OCIO continue to:

- Enhance the Department-wide ISCM program and continue to provide department-wide guidance and tools to each OPDIV on the implementation of their ISCM programs.

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendation. As noted in the report, HHS OCIO is awaiting additional guidance from DHS on ISCM elements and requirements. HHS OCIO is overseeing the process to implement new continuous monitoring tools across all the OPDIVs. Once the new tools are in place, many of the existing findings can be mitigated and security will be strengthened.

Finding #2 – Configuration Management

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

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

- One of the selected OPDIVs' and the Department's configuration management policies and procedures were not updated, reviewed, and finalized per HHS OCIO requirements.
- Instances of non-compliance with configuration management policies and procedures were noted for all four selected OPDIVs specific to patch management, up-to-date software maintenance, baseline configurations, and vulnerability scans performed through Security Content Automation Protocol (SCAP) tools.
- Some configuration changes at three of the selected OPDIVs were not approved by the Change Control Board before implementation.

Some OPDIVs have not fully developed, defined, and/or implemented their configuration management policies and procedures. Without a fully developed configuration management process, HHS's information systems may be exposed to vulnerabilities and exploitation. Also, the OPDIVs' management may not receive accurate information about its systems to make decisions related to information security.

Recommendation:

We recommend that the OCIO ensure that all Department and OPDIV policies and guidance are updated in accordance with its requirements.

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO has developed a plan to update the Department security policies and will be working with the OPDIVs to make sure they have similar plans in place. HHS OCIO has obtained a new electronic Governance, Risk and Compliance (eGRC) tool that will be implemented enterprise wide at HHS and will enhance their ability to document, track and evaluate trends and common issues.

Finding #3 – Identity and Access Management

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

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

- Account management procedures were not followed by two of the selected OPDIVs. This included monitoring and maintaining active and shared accounts, enforcing resets of active network user accounts passwords, removing inactive accounts in a timely manner and disabling accounts of transferred and terminated personnel in a timely manner.
- One OPDIV's policies and procedures for identity and access management and remote access were not updated and reviewed per HHS OCIO requirements.
- One OPDIV's Privileged Account Standard Operating Procedures was not reviewed and updated in the last three years.

OPDIVs did not consistently comply with their procedures for managing user access, oversight of terminated users, and user account management. Weaknesses in identity and access and remote access management controls may increase the risk of inappropriate access to the HHS network, information systems and data. Identity access and remote access policies and procedures that are not updated, finalized and distributed may result in a lack of clarity in the implementation and control of access, thereby leading to potentially unauthorized access to the network resulting in loss, destruction or misuse of sensitive data and resources.

Recommendation:

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO is coordinating a review of the specific OPDIV findings. This will enable HHS OCIO to track mitigation, evaluate trends, identify common issues, and assess adequacy of policies and procedures at the Department and the OPDIV level.

Finding #4 – Incident Response and Reporting

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

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

- For two of the selected OPDIVs, incidents were not reported to the HHS Computer Security Incident Response Center (CSIRC) within the appropriate timeframe.
- One of the selected OPDIVs failed to document the accurate closure dates of some incidents.
- One of the selected OPDIVs did not update their incident response policies and procedures as required by the HHS OCIO.

Policies and procedures were not updated timely and incidents were being tracked accurately and reported to US-CERT within the timeframe prescribed by HHS due to OPDIV management oversight and limited resources.

Without updating incident response policies and procedures, tracking incidents accurately, and reporting incidents in a timely manner to US-CERT, HHS faces an increased exposure to security risks to its IT environment.

Recommendations:

We recommend that the HHS OCIO continue to:

- Implement an adequate oversight protocol to monitor and ensure that the OPDIVs report incidents timely to the CSIRC.
- Ensure timely updates to the incident response and reporting policies and procedures.

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. In order to assist the OPDIVs in complying with US-CERT and HHS reporting requirements, CSIRC initiated a new program in 2016 to perform incident response plan tabletop exercises with each OPDIV. HHS OCIO will continue this program and determine if additional testing is needed during these exercises in order to meet all incident reporting requirements.

Finding #5 – Risk Management

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

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

- The Department-managed systems inventory did not reconcile to the OPDIV-managed systems inventory for three selected OPDIVs.
- For one of the selected OPDIV, Risk Management policies and procedures were not reviewed and updated per HHS OCIO requirements.
- One of the selected OPDIV did not fully establish an insider threat detection and prevention program.
- For the systems selected for review at one of the selected OPDIVs, security controls selected for testing were either not effective or were not fully implemented.
- For two of the selected OPDIVs, some systems were operating without a current and valid Authorization to Operate (ATO).

The OPDIVs did not consistently implement the HHS OCIO enterprise-wide and NIST risk management framework. Each selected OPDIV used different tools to track its system inventories. This resulted in differences in the inventories between the OPDIVs and HHS OCIO. HHS does not have an adequate mechanism to determine whether system authorizations are conducted in a timely manner, policies are updated periodically and that the insider threat detection and prevention program is established in a timely manner.

Without establishing a consistent security authorization process that meets minimum IT security requirements, HHS management will not be able to evaluate and determine whether appropriate security measures are in place for its IT systems and operations. This could lead to inadequate controls across systems that could compromise the security of the systems and lead to unauthorized access and manipulation of data. Without reconciling systems inventories, HHS might not have full awareness of all applicable FISMA systems for tracking, reporting, and security authorization purposes. Operating information systems with expired ATOs may increase the risk that information security controls are not operating effectively and do not meet current minimum baseline control requirements, which could place HHS data and operations at risk.

Recommendations:

We recommend that the HHS OCIO continue to:

- Perform detailed reconciliation of HHS systems inventory to each OPDIV's systems inventory on a monthly basis to ensure the HHS system inventory is accurate.
- Provide updated guidance to the OPDIVs specific to implementing its risk management program that is consistent with HHS and NIST guidelines.

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO has continued to enhance the HHS Data Warehouse (HSDW) reports that are issued to the OPDIVs both during submission of system inventory data and on a monthly basis. HHS OCIO will be implementing a new eGRC tool across the enterprise in conjunction with the DHS supplied CDM tools in order to facilitate system inventory and security authorization tracking and enable OPDIVs to implement an improved risk management program. As new tools are implemented, OCIO will update policies, standards and guidance related to improved implementation and tracking.

Finding #6 – Security Training

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

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

- Required new hire, annual and role-based trainings were not taken by personnel at two of the selected OPDIVs.
- Security training policies and procedures at the Department were not reviewed and updated in the last three years.

HHS does not have an adequate mechanism to enforce the timely review of policies and procedures. HHS does not have an effective process to monitor and enforce users to complete security trainings in the required timeframe.

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

Recommendation:

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO has implemented a new Department level process for writing and updating security policies and procedures in a timely manner. HHS OCIO is coordinating a review of the specific OPDIV findings.

Finding #7 – Plan of Action and Milestones (POA&M)

The POA&M process facilitates the remediation of information security program and system-level weaknesses and provides a means for planning and monitoring corrective actions, defining roles and responsibilities for weakness resolution, assisting in identifying the resource requirements necessary to mitigate weaknesses, tracking and prioritizing resources, and informing decision makers. An effective risk management program cannot be established without significant attention focused on the POA&M.

The following findings were identified within HHS' POA&M management program:

- For all four of the selected OPDIVs, some POA&M records had estimated completion dates that were past due and some POA&M records were missing cost requirements in terms of hours or dollars as well as point of contacts assigned for ownership for weaknesses remediation.
- For two of the selected OPDIVs, POA&M records tracked and monitored by the OPDIVs did not match the POA&M records tracked and monitored by the Department.
- For one of the selected OPDIVs, findings noted in a prior FISMA audit and a Security Assessment Report were not included in the POA&M records.
- The Department's POA&M policies and procedures have not been reviewed and updated per HHS OCIO requirements.

While the OCIO has developed reports and processes to reconcile and ensure that Department and OPDIV POA&Ms reflect accurate information, differences and incomplete or inaccurate POA&M records remain. In addition, OPDIVs did not always adequately document and track POA&M records and did not verify remediation by the estimated completion dates.

Without an effective POA&M process for managing security weaknesses, HHS management has no assurance that information system security weaknesses have been identified and adequately resolved. This could lead to inadequate resource allocation and corrective actions that do not adequately address the identified weaknesses and could compromise the overall information security posture at HHS.

Recommendation:

We recommend that the HHS OCIO continue to:

- Perform a formal reconciliation between Department POA&M records and OPDIV POA&M records on a monthly basis.

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO has continued to enhance the HSDW reports that are issued to the OPDIVs both during submission of POA&M data and on a monthly basis. HHS OCIO will be implementing a new eGRC tool across the enterprise in conjunction with the DHS supplied CDM tools that will standardize the collection and reporting mechanisms related to POA&Ms and enable OPDIVs to implement an improved risk management program.

Finding #8 – Contingency Planning

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

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

- For three of the selected OPDIVs, the Continuity of Operations (COOP) and Business Impact Analysis (BIA) documentation was not complete and did not meet NIST guidance. Additionally, the results of the BIA were not incorporated into the COOP to reflect the current environment.
- For two of the selected OPDIVs, for some systems, there were no results or an after-action report available to demonstrate that the Contingency Plans were tested on an annual basis.
- For one of the selected OPDIVs, for one system, the alternative processing site was in close proximity to the primary site.

In some instances, OPDIVs have not documented or updated the COOP, contingency plans and related documentation in accordance with HHS requirements. Some OPDIVs did not have adequate oversight to ensure it meets HHS and NIST standards to support the adequate recoverability and security of data.

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

Recommendation:

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO is coordinating a review of the specific OPDIV findings. This will enable HHS OCIO to track mitigation, evaluate trends, identify common issues, and assess adequacy of policies and procedures at the Department and OPDIV level.

Finding #9 – Contractor Systems

Contractor oversight is necessary to assess that companies and individuals working with Federal government agencies and information are following the same security requirements as Federal government agencies and employees.

The following findings were identified within HHS' contractor systems program:

- For one of the selected OPDIVs, the required security controls for two sampled contractor systems were not tested.

The OPDIV did not have sufficient oversight on the security authorization process of contractor systems to determine whether security controls had been adequately tested and documented.

Failure to exercise proper oversight over the security controls implemented and maintained by contractor systems could expose systems to unmitigated vulnerabilities and foster a false sense of security that invites service interruptions, jeopardizes the availability and reliability of data, and could expose sensitive information.

Recommendation:

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

HHS OCIO Response:

HHS OCIO concurred with the findings and the recommendations. HHS OCIO is coordinating a review of the specific OPDIV findings. This will enable HHS OCIO to track mitigation, evaluate trends, identify common issues, and assess adequacy of policies and procedures at the OPDIV level.

HHS Comments

In written comments to our draft report, HHS concurred with all of our recommendations and described actions it has taken and plans to take to implement them. HHS's comments are included in their entirety as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed HHS' compliance with FISMA as prescribed in the metrics outlined in the FY 2016 Inspector General FISMA Reporting Metrics. We did not review the overall internal control structure for HHS.

To respond to the metrics, we performed audit procedures, including inquiry of HHS and OPDIV personnel about their security program and inspection of HHS and OPDIVs policies, procedures, standards and other guidance, as well as inspection of corresponding artifacts.

We performed our fieldwork from April 2016 through September 2016 at HHS OCIO and selected OPDIVs as listed below.

- Centers for Disease Control and Prevention (CDC)
- Centers for Medicare & Medicaid Services (CMS)
- National Institutes of Health (NIH)
- Office of the Secretary (OS)

In addition, we followed up on the remediation status of the prior year findings identified during the FISMA performance audit at Indian Health Service (IHS), Administration for Children and Families (ACF), and Food & Drug Administration (FDA).

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal and State laws, regulations, and guidance.
- Gained an understanding of the current security program at HHS and selected OPDIVs.
- Assessed the status of HHS' security program against HHS and selected OPDIV information security program policies, other standards and guidance issued by HHS management, and DHS-prescribed performance measures.
- Inquired of personnel to gain an understanding of the FISMA reporting metric areas.
- Inspected selected artifacts including, but not limited to, system security plans, evidence to support testing of security controls, POA&M records, security training records, asset compliance reports, system inventory reports and account management documentation.

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

APPENDIX B: FEDERAL REQUIREMENTS and GUIDANCE

The principal criteria used for this audit included:

- Federal Information Security Modernization Act of 2014 (December 2014);
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004);
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* (Mar 9, 2006);
- HHS OCIO, *Information Systems Security and Privacy Policy* (July 30, 2014);
- HHS Standard for Plan of Action and Milestones (POA&M) Management & Reporting (September 4, 2013);
- Homeland Security Presidential Directive 12 (HSPD 12): *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004);
- NIH *Continuity of Operations Plan (COOP)* (March 3, 2014);
- NIH *Information Technology (IT) Security Incident Response Plan* (June 18, 2013);
- NIST SP 800-34 *Contingency Planning Guide for Federal Information Systems* (May 2010);
- NIST SP 800-37, revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010);
- NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security* (June 2009);
- NIST SP 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013);
- OMB Circular A-130, *Management of Federal Information Resources, Appendix III, "Security of Federal Automated Information Resources"* (Revised, Transmittal Memorandum No. 4, November 28, 2000);
- OMB M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006);
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007);
- OMB Memo M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12* (February 3, 2011);
- OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems* (November 18, 2013);
- OMB M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements* (October 30, 2015);
- OS *Program Guide for Security Training and Awareness*

APPENDIX C: FY 2016 INSPECTOR GENERAL FISMA REPORTING METRICS

Appendix C contains a system-generated report exported from the CyberScope FISMA Reporting Application. CyberScope is maintained by DHS and OMB. The HHS Office of Inspector General entered its FY 2016 FISMA audit results and narrative comments into the CyberScope system. However, the numerical scores throughout the report were automatically generated by the system.

For Official Use Only

Inspector General

Section Report

2016

Annual FISMA
Report

Department of Health and Human Services

For Official Use Only

Section 0: Overall

0.1 Please provide an overall narrative assessment of the agency's information security program. 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 this response to conform with the grammatical and narrative structure of the Annual Report.

Overall, HHS has made improvements, in comparison to the prior year's Inspectors General FISMA reporting metrics and continues to implement changes to strengthen its enterprise-wide information security program. HHS is aware of the opportunities to strengthen their overall information security program in the areas of continuous monitoring, configuration management, identity and access management, risk management, incident response, security training, and contingency planning. HHS has formalized its Information Security Continuous Monitoring (ISCM) program through development of ISCM policies, procedures, and strategies. HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program in coordination with DHS. This CDM program - implemented by DHS - includes continuously monitoring its networks and systems, updating and finalizing policies and procedures, indicating how documenting OPDIVs' progress to address and implement strategies, and reporting its progress through DHS dashboards. HHS also needs to ensure that all OPDIVs consistently review and remediate or address the risk presented by vulnerabilities discovered, consistently implement account management procedures, and accurately track systems to ensure they are operating with a current and valid Authority To Operate. These steps will strengthen the program and further enhance the HHS mission.

Section 1: Identify

Risk Management (Identify)

1.1	Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Met	Defined
1.1.1	Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) 1D.AM.1, NIST 800-53: PM-5) Met	Defined
1.1.2	Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) Met	Consistently Implemented
1.1.3	Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) Met	Consistently Implemented
1.1.4	Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3) Met	Consistently Implemented
1.1.5	Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization. Met	Managed and Measureable
1.1.6	Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments) Met	Consistently Implemented
1.1.7	Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation.	Defined

Section 1: Identify

	Met	
1.1.8	Implements the tailored set of baseline security controls as described in 1.1.7.	Consistently Implemented
	Met	
1.1.9	Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3)	Managed and Measureable
	Met	
1.1.10	Continuously assesses the security controls, including hybrid and shared controls, using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Consistently Implemented
	Met	
1.1.11	Maintains ongoing information system authorizations based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization).	Managed and Measureable
	Not Met	
	Comments:	Some OPDIVs had systems without current ATO's.
1.1.12	Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37)	Managed and Measureable
	Met	
1.1.13	POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses.	Consistently Implemented
	Not Met	
	Comments:	We noted at 2 OPDIVs reviewed, some weaknesses did not have a POA&M or POA&Ms had outdated estimated completion dates.
1.1.14	Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 :CA-5; OMB M-04-25)	Managed and Measureable
	Not Met	

Section 1: Identify

Comments:

We noted POA&Ms that had outdated estimated completion dates at some OPDIVs.

- 1.1.15 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. **Managed and Measureable**
Met
- 1.1.16 Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (PMC; NIST SP 800-53: PM-12) **Consistently Implemented**
Met
- 1.1.17 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. Based on all testing performed, is the Risk Management program effective? **Effective**

Contractor Systems (Identify)

- 1.2 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**
Met
- 1.2.1 Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices) **Consistently Implemented**
Met
- 1.2.2 Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35) **Consistently Implemented**
Met

Section 1: Identify

1.2.3 Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)

Consistently Implemented

Met

1.2.4 Provide any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective?

Effective

Comments:

The Department has a FISMA working group, led by the OCIO's FISMA team, which includes representatives from all OPDIVs, who meet monthly to discuss relevant security related topics, requirements and concerns.

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 2: Protect

Configuration Management (Protect)

2.1	Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	Defined
	Met	
2.1.1	Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF 1D.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8)	Defined
	Not Met	
	Comments:	
	In some instances, a complete hardware assets listing could not be provided or reconciliations between property management systems and asset tracking systems were not performed to ensure its hardware inventory is accurate.	
2.1.2	Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF 1D.AM-2)	Defined
	Met	
2.1.3	Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.1P-1)	Consistently Implemented
	Not Met	
	Comments:	
	In some instances, baseline configurations were not documented.	
2.1.4	Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3)	Consistently Implemented
	Met	
2.1.5	Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.1P-3)	Managed and Measureable
	Not Met	
	Comments:	
	We noted instances where configuration changes were not approved before moving into production.	
2.1.6	Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7)	Managed and Measureable

Section 2: Protect

Met

- 2.1.7 Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI-2; CIO 2016 FISMA Metrics 2.2, CIS 4.1) **Managed and Measureable**

Met

- 2.1.8 Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2) **Consistently Implemented**

Not Met

Comments:

- 2.1.9 Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01) **Managed and Measureable**

Not Met

Comments:

One OPDIV has not fully implemented a patch management process. We noted at 1 OPDIV that 2 critical patches were not deployed and patched to all workstations.

- 2.1.10 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. Based on all testing performed, is the Configuration Management Program effective?

Not Effective

Identity and Access Management (Protect)

- 2.2 Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

- 2.2.1 Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6) **Consistently Implemented**

Met

Section 2: Protect

2.2.2	Ensures that all users are only granted access based on least privilege and separation-of-duties principles.	Consistently Implemented
	Met	
2.2.3	Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and IP phones).	Consistently Implemented
	Met	
2.2.4	Implements PIV for physical access in accordance with government policies. (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)	Consistently Implemented
	Met	
2.2.5	Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.5.1)	Consistently Implemented
	Met	
2.2.6	Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1)	Consistently Implemented
	Met	
2.2.7	Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2)	Managed and Measureable
	Met	
2.2.8	Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy.	Managed and Measureable
	Met	
2.2.9	Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2)	Consistently Implemented
	Met	
2.2.10	All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63)	Consistently Implemented

Section 2: Protect

Met

- | | | |
|--------|--|---------------------------------|
| 2.2.11 | Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (CIS 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1) | Consistently Implemented |
|--------|--|---------------------------------|

Met

- | | | |
|--------|--|--------------------------------|
| 2.2.12 | Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16 | Managed and Measureable |
|--------|--|--------------------------------|

Met

- | | | |
|--------|---|---------------------------------|
| 2.2.13 | Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7) | Consistently Implemented |
|--------|---|---------------------------------|

Met

- | | | |
|--------|--|---------------------------------|
| 2.2.14 | Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13) | Consistently Implemented |
|--------|--|---------------------------------|

Met

- | | | |
|--------|--|--|
| 2.2.15 | 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. Based on all testing performed is the Identity and Access Management Program effective? | |
|--------|--|--|

Effective**Security and Privacy Training (Protect)**

- | | | |
|-----|--|----------------|
| 2.3 | Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? | Defined |
|-----|--|----------------|

Met

- | | | |
|-------|--|---------------------------------|
| 2.3.1 | Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National Insider Threat Policy (NITP)) | Consistently Implemented |
|-------|--|---------------------------------|

Met

- | | | |
|-------|--|---------------------------------|
| 2.3.2 | Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50) | Consistently Implemented |
|-------|--|---------------------------------|

Section 2: Protect

Met

2.3.3 Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2)

Consistently Implemented

Not Met

Comments:

2.3.4 Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training.

Consistently Implemented

Met

2.3.5 Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55)

Managed and Measureable

Met

2.3.6 Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective?

Effective

Level	Score	Possible Score
LEVEL 2: Defined	7	20

Section 3: Detect

Level 1

Definition

- 3.1.1 ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

- 3.1.1.1 ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **Ad Hoc**
Met
- 3.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **Ad Hoc**
Met
- 3.1.1.3 The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. **Ad Hoc**
Met
- 3.1.1.4 The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. **Ad Hoc**
Met

Processes

- 3.1.1.5 ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Ad Hoc**
Met
- 3.1.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Ad Hoc**
Met
- 3.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. **Ad Hoc**

Section 3: Detect

Met

3.1.1.8 The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes.

Ad Hoc

Met

Technology

3.1.1.9 The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc.

Ad Hoc

- Patch management
- License management
- Information management
- Software assurance
- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Met

3.1.1.10 The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

Ad Hoc

Met

Level 2

Definition

3.2.1 The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.

People

3.2.1.1 ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders

Defined

Section 3: Detect

may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities.

Met

- 3.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **Defined**

Met

- 3.2.1.3 The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. **Defined**

Met

- 3.2.1.4 The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. **Defined**

Met

Processes

- 3.2.1.5 ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. **Defined**

Met

- 3.2.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Defined**

Met

- 3.2.1.7 The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Defined**

Met

- 3.2.1.8 The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements **Defined**

Section 3: Detect

to the ISCM program.

Met

Technology

3.2.1.9 The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology in these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable.

Defined

Met

3.2.1.10 The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

Defined

Met

Level 3

Definition

3.3.1 In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

3.3.1.1 ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities.

Consistently Implemented

Not Met

Comments:

We noted at some OPDIVs that stakeholders and their responsibilities have not been identified and communicated across the organization.

Section 3: Detect

3.3.1.2	The organization has fully implemented its plans to close any gaps in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. Met	Consistently Implemented
3.3.1.3	ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. Met	Consistently Implemented
3.3.1.4	ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. Met	Consistently Implemented
Processes		
3.3.1.5	ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. Met	Consistently Implemented
3.3.1.6	The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. Met	Consistently Implemented
3.3.1.7	The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. Met	Consistently Implemented
3.3.1.8	The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. Met	Consistently Implemented
3.3.1.9	The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. - Patch management	Consistently Implemented

Section 3: Detect

- License management
- Information management
- Software assurance
- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Not Met

Comments: At some OPDIVs, the OPDIV did not consistently implement its technologies in all of the key ISCM automation areas.

Technology

3.3.1.10 The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

Consistently Implemented

Not Met

Comments: Some OPDIVs could not produce an accurate point in time inventory of authorized and unauthorized devices an software on its network.

Level 4

Definition

3.4.1 In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

People

3.4.1.1 The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program.

Managed and Measureable

Not Met

Section 3: Detect

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, it has not been consistently implemented across the entire HHS organization.

3.4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **Managed and Measureable**
Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, skilled personnel have not been hired/trained across the entire organization.

3.4.1.3 Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. **Managed and Measureable**
Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, staff responsibilities have not been assigned fully across the entire HHS organization.

Processes

3.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **Managed and Measureable**
Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, processes for consistently implementing, monitoring, and analyzing qualitative and quantitative measures across the entire HHS organization.

3.4.1.5 Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **Managed and Measureable**
Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, data supporting ISCM metrics are not consistently obtained across the entire HHS organization.

3.4.1.6 The organization is able to integrate metrics on the effectiveness of its 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 **Managed and Measureable**

Section 3: Detect

of operations and security domains.

Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, it has not been able to integrate metrics on the effectiveness of its ISCM program across the entire HHS organization.

3.4.1.7 The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer.

Managed and Measureable

Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, ISCM metrics are not used consistently across the entire HHS organization for determining risk response actions.

3.4.1.8 ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities.

Managed and Measureable

Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, all ISCM metrics are not consistently reported to organizations officials charged with correlating and analyzing metrics across the entire HHS organization.

3.4.1.9 ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis.

Managed and Measureable

Met

Technology

3.4.1.10 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM.

Managed and Measureable

Not Met

Section 3: Detect

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the entire HHS organization has not been fully implemented.

3.4.1.11 The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations.

Managed and Measureable

Not Met

Comments: Since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, performance measures for all sections of the HHS network have not been fully developed across the entire HHS organization.

3.4.1.12 The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk

Managed and Measureable

Not Met

Comments: All OPDIVs have not fully implemented the use of a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk.

Level 5

Definition

3.5.1 In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.

People

3.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements.

Optimized

Not Met

Section 3: Detect

Comments: While we did not specifically test this metric during the FISMA audit, since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, the ISCM program is not at the Optimized level of institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape across the entire HHS organization.

Processes

3.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **Optimized**

Not Met

Comments: While we did not specifically test this metric during the FISMA audit, since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, the ISCM program is not at the Optimized level of institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape across the entire HHS organization.

3.5.1.3 On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **Optimized**

Not Met

Comments: While we did not specifically test this metric during the FISMA audit, since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, the ISCM program is not at the level of institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape across the entire HHS organization.

3.5.1.4 The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **Optimized**

Not Met

Section 3: Detect

Comments: While we did not specifically test this metric during the FISMA audit, since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, the ISCM program is not at the Optimized level of institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape across the entire HHS organization.

3.5.1.5 The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.

Optimized

Not Met

Comments: While we did not specifically test this metric during the FISMA audit, since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, the ISCM program is not at the Optimized level of institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape across the entire HHS organization.

Technology

3.5.1.6 The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time.

Optimized

Not Met

Comments: While we did not specifically test this metric during the FISMA audit, since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, the ISCM program is not at the Optimized level of institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape across the entire HHS organization.

3.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program.

Optimized

Not Met

For Official Use Only

Section 3: Detect

Comments:

While we did not specifically test this metric during the FISMA audit, since the Department and its OPDIVs are still in the process of implementing its ISCM program, collaborating with DHS, the ISCM program is not at the Optimized level of institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape across the entire HHS organization.

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 4: Respond

Level 1

Definition

- 4.1.1 Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines).

People

- 4.1.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. **Ad Hoc**

Met

- 4.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. **Ad Hoc**

Met

- 4.1.1.3 The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. **Ad Hoc**

Met

- 4.1.1.4 The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Ad Hoc**

Met

Processes

- 4.1.1.5 Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. **Ad Hoc**

Met

- 4.1.1.6 The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical **Ad Hoc**

Section 4: Respond

assistance/surge resources/special capabilities for quickly responding to incidents.

Met

- 4.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk.

Ad Hoc

Met

- 4.1.1.8 The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes.

Ad Hoc

Met

Technology

- 4.1.1.9 The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc.

Ad Hoc

- 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 anti-virus and antispyware software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

Met

- 4.1.1.10 The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.

Ad Hoc

Met

- 4.1.1.11 The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.

Ad Hoc

Met

- 4.1.1.12 The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems.

Ad Hoc

Met

Level 2

Section 4: Respond

Definition

- 4.2.1 The organization has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide.

People

- 4.2.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. **Defined**

Met

- 4.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. **Defined**

Met

- 4.2.1.3 The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. **Defined**

Met

- 4.2.1.4 The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas. **Defined**

Met

Processes

- 4.2.1.5 Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, **Defined**

Section 4: Respond

and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization.

Met

- 4.2.1.6 The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents.

Defined

Met

- 4.2.1.7 The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization.

Defined

Met

- 4.2.1.8 The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program.

Defined

Met

Technology

- 4.2.1.9 The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas:

Defined

- 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. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors.
- Malware detection such as Anti-virus and antispam software technologies
- Information management such as data loss prevention
- File integrity and endpoint and server security tools

However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.

Met

Section 4: Respond

- 4.2.1.10 The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the TIC 2.0 provider and agency managed capabilities are consistently implemented. **Defined**
Met
- 4.2.1.11 The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. **Defined**
Met
- 4.2.1.12 The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. **Defined**
Met

Level 3

Definition

- 4.3.1 In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.

People

- 4.3.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. **Consistently Implemented**
Met
- 4.3.1.2 The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. **Consistently Implemented**
Not Met

Section 4: Respond

Comments: We did not specifically test this metric during the FISMA audit so we could not determine if this metric was met across HHS and its OPDIVs.

4.3.1.3 The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. **Consistently Implemented**

Met

4.3.1.4 Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Consistently Implemented**

Not Met

Comments: HHS and its OPDIVs have not fully integrated its incident response activities with organizational risk management, continuous monitoring, continuity of operations and other mission/business areas.

Processes

4.3.1.5 Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. **Consistently Implemented**

Met

4.3.1.6 The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. **Consistently Implemented**

Met

4.3.1.7 The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. **Consistently Implemented**

Not Met

Comments: We did not specifically test this metric during the FISMA audit so we could not determine if this metric was met across HHS and its OPDIVs.

Section 4: Respond

4.3.1.8 The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. **Consistently Implemented**

Not Met

Comments: We did not specifically test this metric during the FISMA audit so we could not determine if this metric was met across HHS and its OPDIVs.

4.3.1.9 The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. **Consistently Implemented**

Not Met

Comments: We did not specifically test this metric during the FISMA audit so we could not determine if this metric was met across HHS and its OPDIVs.

Technology

4.3.1.10 The organization has consistently implemented its defined incident response technologies in the following areas: **Consistently Implemented**

- 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. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors
- Malware detection, such as anti-virus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.

Not Met

Comments: We did not specifically test this metric during the FISMA audit so we could not determine if this metric was met across HHS and its OPDIVs.

Section 4: Respond

4.3.1.11	The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.	Consistently Implemented
	Met	
4.3.1.12	The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks.	Consistently Implemented
	Met	
4.3.1.13	The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems.	Consistently Implemented
	Met	

Level 4

Definition

4.4.1 In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities.

People

4.4.1.1	Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program.	Managed and Measurable
---------	---	-------------------------------

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

4.4.1.2	Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program.	Managed and Measurable
---------	---	-------------------------------

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

4.4.1.3	Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program.	Managed and Measurable
---------	---	-------------------------------

Section 4: Respond

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

Processes

4.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response.

Managed and Measurable

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

4.4.1.5 Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format.

Managed and Measurable

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

4.4.1.6 Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations

Managed and Measurable

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

4.4.1.7 Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities.

Managed and Measurable

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

Technology

Section 4: Respond

4.4.1.8 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. **Managed and Measureable**

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

4.4.1.9 The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. **Managed and Measureable**

Not Met

Comments: We determined that HHS is not at the Managed and Measurable level for its Incident Response program across the Department.

Level 5

Definition

4.5.1 In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements, and a changing threat and technology landscape.

People

4.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. **Optimized**

Not Met

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

Processes

4.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. **Optimized**

Not Met

Section 4: Respond

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

4.5.1.3 On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. **Optimized**

Not Met

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

4.5.1.4 The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Optimized**

Not Met

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

4.5.1.5 The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. **Optimized**

Not Met

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

Technology

4.5.1.6 The organization has institutionalized the implementation of advanced incident response technologies in near real-time. **Optimized**

Not Met

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

4.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. **Optimized**

Not Met

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

4.5.1.8 The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT **Optimized**

For Official Use Only

Section 4: Respond

assets and adjusts incident response processes and security measures accordingly.

Not Met

Comments: We determined that HHS is not at the Optimized level for its Incident Response program across the Department.

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 5: Recover

Contingency Planning (Recover)

5.1	Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Met	Defined
5.1.1	Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53) Met	Consistently Implemented
5.1.2	Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34) Not Met	Consistently Implemented
	Comments: In some instances, BIA's were not considered when developing contingency plans.	
5.1.3	Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34) Met	Consistently Implemented
5.1.4	BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC) Met	Consistently Implemented
5.1.5	Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4) Met	Managed and Measureable
5.1.6	Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) Met	Consistently Implemented
5.1.7	Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) Met	Managed and Measureable

Section 5: Recover

- 5.1.8 Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7)

Met

Consistently Implemented
- 5.1.9 Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records)

Met

Managed and Measureable
- 5.1.10 Contingency planning that considers supply chain threats.

Met

Defined
- 5.1.11 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. Based on all testing performed is the Contingency Planning Program effective?

Effective

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

For Official Use Only

APPENDIX A: Maturity Model Scoring

Maturity Levels by Section

Section	Level	Score	Possible Score
Section 1: Identify	LEVEL 3: Consistently Implemented	13	20
Section 2: Protect	LEVEL 2: Defined	7	20
Section 3: Detect	LEVEL 3: Consistently Implemented	13	20
Section 4: Respond	LEVEL 3: Consistently Implemented	13	20
Section 5: Recover	LEVEL 3: Consistently Implemented	13	20
TOTAL		59	100

Section 1: Identify

Model Indicator	Met	Not Met	Total	○	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	4	0	4	100%	4	4
Consistently Implemented	10	1	11	91%	6	6
Managed and Measureable	4	2	6	67%	0	5
Optimized	0	0	0	100%	0	2

Section 2: Protect

Model Indicator	Met	Not Met	Total	○	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	4	1	5	80%	4	4
Consistently Implemented	15	3	18	83%	0	6
Managed and Measureable	6	2	8	75%	0	5
Optimized	0	0	0	100%	0	2

Section 3: Detect

Model Indicator	Met	Not Met	Total	○	Points Assigned	Possible Points
Ad-Hoc	10	0	10	100%	3	3
Defined	10	0	10	100%	4	4
Consistently Implemented	7	3	10	70%	6	6
Managed and Measureable	1	11	12	8%	0	5
Optimized	0	7	7	0%	0	2

For Official Use Only

For Official Use Only

Section 4: Respond

Model Indicator	Met	Not Met	Total	○	Points Assigned	Possible Points
Ad-Hoc	12	0	12	100%	3	3
Defined	12	0	12	100%	4	4
Consistently Implemented	7	6	13	54%	6	6
Managed and Measureable	0	9	9	0%	0	5
Optimized	0	8	8	0%	0	2

Section 5: Recover

Model Indicator	Met	Not Met	Total	○	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	2	0	2	100%	4	4
Consistently Implemented	5	1	6	83%	6	6
Managed and Measureable	3	0	3	100%	0	5
Optimized	0	0	0	100%	0	2

APPENDIX D: HHS RESPONSE




DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

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

TO: Amy J. Frontz
Assistant Inspector General for Audit Services

FROM: Beth Killoran 
Deputy Assistant Secretary for Information Technology
and Chief Information Officer

DATE: January 3, 2017

SUBJECT: Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2016 (A-18-16-30350)

Ms. Frontz,

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) 2016. We welcome the opportunity to respond to the report developed by Ernest & Young on your behalf.

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

If you have any questions or need additional information, please reach out to the Leo Scanlon, Chief Information Security Officer (Acting), at leo.scanlon@hhs.gov or 202-260-6058.

Attachment A

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

ATTACHMENT A: Response from the Office of the Chief Information Officer (OCIO) regarding the *Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization (ISCM) Act of 2014 for Fiscal Year 2016 (A-18-16-30350)*

Finding #1 – Continuous Monitoring Management

OIG Recommendation:

We recommend that the HHS OCIO continue to:

- Enhance the Department-wide ISCM program and continue to provide department-wide guidance and tools to each OPDIV on the implementation of their ISCM programs.

OCIO Response: Concur

As noted in the report, OCIO is awaiting additional guidance from the Department of Homeland Security (DHS) on ISCM elements and requirements. Without this information OCIO cannot finalize an enterprise-level program. Some OpDivs have implemented more cross-cutting tools with the help of the Continuous Diagnostic and Mitigation (CDM) integrator, but this process is not fully incorporated at all OpDivs. A schedule is in place and OCIO is overseeing the process to ensure that the timeline is adhered to in the upcoming months. Once these new tools are in place, many of the existing findings can be mitigated and security will be strengthened.

Finding #2 – Configuration Management

Recommendation:

- We recommend that the OCIO ensure that all Department and OPDIV policies and guidance are updated in accordance with its requirements.
- In addition, we provided detailed information and recommendations that were specific to the Department and OPDIV's findings to management officials so they could address these specific findings.

HHS Response: Concur

OCIO has developed a plan to update Department security policies and will be working with the OpDivs to ensure that they have similar plans in place.

OCIO has received a copy of the OpDiv audit reports and will continue to track findings and report them to management officials. In addition, OCIO has purchased a new electronic Governance, Risk and Compliance (eGRC) tool that will be implemented enterprise wide in 2017 that will enhance our ability to document, track and evaluate trends and common issues.

Finding #3 – Identity and Access Management

OIG Recommendation:

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

HHS Response: Concur

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

Finding #4 – Incident Response and Reporting

OIG Recommendations

We recommend that the HHS OCIO continue to:

- Implement an adequate oversight protocol to monitor and ensure that the OPDIVs report incidents timely to the Computer Incident Response Center (CSIRC).
- Ensure timely updates to the incident response and reporting policies and procedures.
- In addition, we provided detailed information and recommendations that were specific to the OPDIV's findings to OPDIV management officials so they could address these specific findings.

HHS Response: Concur

OCIO appreciates the acknowledgement that our CSIRC continues to adhere to all U.S. Computer Emergency Readiness Team (US-CERT) reporting requirements and reviews OpDiv tickets for data quality and completion. Per the *HHS Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response*, the OpDivs are responsible for reporting incidents to CSIRC, who then reports on behalf of the Department.

In order to assist the OpDivs in complying with US-CERT and HHS reporting requirements, CSIRC initiated a new program in 2016 to perform incident response plan tabletop exercises with each OpDiv. During the exercise, policies, procedures and plans are tested to ensure that they are up-to-date, effective, and in compliance with US-CERT, OCIO, and other federal guidelines (including the timeliness and completeness of reported data). OCIO will continue this program and determine if additional testing is needed during these exercises in order to meet all incident reporting requirements.

Finding #5 – Risk Management

OIG Recommendations:

We recommend that the HHS OCIO continue to:

- Perform detailed reconciliation of HHS systems inventory to each OPDIV's systems inventory on a monthly basis to ensure the HHS system inventory is accurate.
- Provide updated guidance to the OPDIVs specific to implementing its risk management program that is consistent with HHS and National Institute of Standards guidelines.
- In addition, we provided detailed information and recommendations that were specific to the OPDIV's findings to OPDIV management officials so they could address these specific findings.

HHS Response: Concur

OCIO has continued to enhance the HHS Data Warehouse (HSDW) reports that are issued to the OpDivs both during submission of system inventory data and on a monthly basis.

In 2017, OCIO will be implementing a new eGRC tool across the enterprise in conjunction with the DHS supplied CDM tools in order to facilitate system inventory and security authorization tracking. This will standardize the collection and reporting mechanisms related to system data and also improve OpDiv and OCIO oversight of security control implementation and risk management. By linking the data in this new tool with other CDM tools, OpDivs and OCIO will have the ability to do further analysis of system information, associate vulnerabilities and incidents with systems and security controls, and enable OpDivs to implement an improved risk management program. As these new tools are implemented, OCIO will be updating policies, standards and/or guidance related to improved security implementation and tracking.

Finding #6 – Security Training

OIG Recommendation:

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

HHS Response: Concur

OCIO has implemented a new Department level development and update process for security policies and procedures to ensure that they are written and/or updated in a timely manner.

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings. This will enable us to identify common issues with OpDiv security training and assess if policies and/or procedures are adequate at both the Department and OpDiv level.

Finding #7 – Plan of Action and Milestones (POA&M)

OIG Recommendation:

We recommend that the HHS OCIO continue to:

- Perform a formal reconciliation between Department POA&M records and OPDIV POA&M records on a monthly basis.
- In addition, we provided detailed information and recommendations that were specific to the Department and OPDIV's findings to management officials so that they could address these specific findings.

HHS Response: Concur

OCIO has continued to enhance the HSDW reports that are issued to the OpDivs both during submission of POA&M data and on a monthly basis. These enhanced reports were developed to assist OpDivs identify incomplete or inaccurate POA&M records. It is the OpDiv's responsibility to ensure that the data supplied to the Department is accurate and complete.

In 2017 OCIO will be implementing a new eGRC tool across the enterprise in conjunction with the DHS supplied (CDM) tools. This will standardize the collection and reporting mechanisms related to POA&Ms and also improve OpDiv and Department oversight of security control implementation and risk management. By linking the data in this new tool with other CDM tools, OpDivs and the Department will have the ability to do further analysis of POA&M information, associate vulnerabilities and incidents with systems and security controls and enable OpDivs to implement an improved risk management program. As these new tools are implemented, the Department will be updating policies, standards and/or guidance related to improved security implementation and tracking.

Finding #8 – Contingency Planning

Recommendation:

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

HHS Response: Concur

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

Finding #9 – Contractor Systems

Recommendation:

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

HHS Response: Concur

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