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 2015

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

Thomas M. Salmon
Assistant Inspector General
for Audit Services

March 2016
A-18-15-30300

Office of Inspector General

http://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 http://oig.hhs.gov

Section 8L 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

Building a better working world

January 14, 2016

Mr. Thomas Salmon
Assistant Inspector General for Audit Services
Office of the Inspector General
Wilbur J. Cohen Building
330 Independence Avenue, SW
Washington, D.C. 20201

Dear Mr. Salmon:

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 2015 Inspector General FISMA Reporting Metrics (reporting metrics) provided by the Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C).

Our procedures were designed to respond to the questions outlined in the DHS CS&C reporting metrics for the Inspectors General 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, 2015. 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,

Ernst & Young LLP

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

Mr. Thomas Salmon
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, 2015, with the objective of assessing HHS FISMA compliance as defined in Office of Management and Budget (OMB) and U.S. Department of Homeland Security (DHS) guidance.

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 questions outlined in the DHS Office of Cybersecurity and Communications (CS&C) reporting metrics for the Inspector General. The specific scope and methodology are defined in Section II of this report.

The conclusions in Section III and our findings and recommendations, as well as proposed alternatives for the improvement of HHS' compliance with FISMA in Section IV, 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 14, 2016
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, 2015 based upon the questions outlined in the U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) 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 DHS to administer the implementation of such policies and practices for information systems.

To comply with the FISMA, the DHS CS&C prescribed reporting requirements for agencies and Inspectors General. FISMA authorizes 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 representative 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 questions outlined in the DHS CS&C reporting metrics for the Inspectors General are presented in Appendix A. Overall, in comparison to the prior year's Inspectors General FISMA reporting metrics, HHS has made improvements. However, opportunities to strengthen the overall information security program exist.

Overall Issues to Be Addressed

Despite the progress made to improve the HHS and its operating divisions' (OPDIV) information security program, opportunities to strengthen the program exist. We identified areas for improvement. The issues have been consolidated into ten findings for HHS' consideration. The ten findings are classified into the following areas:

1. **Continuous Monitoring Management** – HHS has formalized its Information Security Continuous Monitoring (ISCM) program through development of ISCM policies, procedures, and strategies. However, HHS has not implemented a Department-wide fully-implemented continuous monitoring program which includes continuously monitoring, updating and finalizing policies and procedures indicating how OPDIVs address, implement strategies and report on DHS metrics. This includes vulnerability management, software assurance, information management, patch management, license management, event management, malware detection, asset management, and network management.
2. **Configuration Management –** Some OPDIVs did not consistently review and remediate or address the risk presented by vulnerabilities discovered in configuration baseline compliance and vulnerability scans performed through Security Content Automation Protocol tools.
3. **Identity and Access Management** – Some OPDIVs did not consistently implement account management procedures for shared accounts, new personnel, transferred personnel and terminated personnel.
4. **Incident Response and Reporting** – Oversight processes had not been implemented by HHS to enforce incident response and reporting procedures at the OPDIVs.
5. **Risk Management** – HHS did not implement procedures to oversee that system inventories are complete, accurate and effectively managed, including reconciling to the OPDIV-managed system inventory tools.
6. **Security Training** – Some OPDIVs did not monitor the completion of role-based training for significant security responsibilities and other security training for personnel using IT systems.
7. **Plan of Action and Milestones –** Plan of Action & Milestones (POA&Ms) were not consistently documented and tracked by the OPDIVs and HHS.
8. **Remote Access Management** – Some OPDIVs had not developed formal and finalized remote access policies and procedures.
9. **Contingency Planning** – Some OPDIVs did not complete required contingency planning documentation, including Business Impact Analysis, Continuity of Operation Plans, and Information System Contingency Plans.
10. **Contractor Systems –** Some OPDIVs did not have an effective contractor oversight protocols.

Exploitation of these weaknesses could result in unauthorized access to, and disclosure of, sensitive information and disruption of critical operations for 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 IV to enhance information security controls to HHS and specific controls for the OPDIVs.

HHS Comments

In written comments to our draft report, HHS concurred or partially 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 C.

Table of Contents

INTRODUCTION 1
SECTION I – BACKGROUND 1
SECTION II – AUDIT SCOPE AND METHODOLOGY 2
SECTION III – CONCLUSIONS 3
SECTION IV – FINDINGS AND RECOMMENDATIONS 3
Finding #1 – Continuous Monitoring Management 4
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 Actions and Milestones (POA&M) 11
Finding #8 – Remote Access Management 13
Finding #9 – Contingency Planning 14
Finding #10 – Contractor Systems 15
APPENDIX A: OIG Response to DHS FISMA Reporting Metrics 9/30/2015 16
1: CONTINUOUS MONITORING 16
2. CONFIGURATION MANAGEMENT 17
3. IDENTITY and ACCESS MANAGEMENT 18
4. INCIDENT RESPONSE and REPORTING 19
5. RISK MANAGEMENT 20
6. SECURITY TRAINING 22
7. PLAN OF ACTION & MILESTONES (POA&M) 23
8. REMOTE ACCESS MANAGEMENT 24
9. CONTINGENCY PLANNING (CP) 25
10. CONTRACTOR SYSTEMS 26
APPENDIX B: FEDERAL REQUIREMENTS and GUIDANCE 27
APPENDIX C: HHS RESPONSE 28

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, 2015 based upon the questions outlined in the U.S. Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C) 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 DHS to administer the implementation of such policies and practices for information systems.

To comply with the FISMA, the DHS CS&C prescribed reporting requirements for agencies and Inspectors General. FISMA authorizes 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 representative 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 2015 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 (OCIO) Information Security and Privacy Program

HHS administers more than 300 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's 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 an incident response program that ensures proper and timely reporting to HHS. The OPDIV Chief Information Security Officers (CISOs) are responsible to implement Department and OPDIV policies and procedures that relate to IT security and privacy incident response.

SECTION II – AUDIT SCOPE AND METHODOLOGY

Scope

We reviewed HHS' compliance with FISMA as prescribed in the questions outlined in the FY 2015 DHS CS&C reporting metrics for the Inspectors General. The questions included in the DHS CS&C reporting metrics for the Inspectors General are listed in Appendix A. We did not review the overall internal control structure for HHS.

To respond to the questions outlined in the DHS CS&C reporting metrics for the Inspectors General, 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 artifacts.

We performed our fieldwork from April 2015 through September 2015 at HHS headquarters and selected OPDIVs as listed below.

- Administration for Children and Families (ACF)
- Centers for Medicare and Medicaid Services (CMS)
- Indian Health Service (IHS)
- National Institutes of Health (NIH)
- Office of the Secretary (OS)

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 accordance with generally accepted *Government Auditing Standards* (GAGAS). 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.

SECTION III – CONCLUSIONS

Our conclusions related to HHS' information security program are contained within the DHS FISMA reporting metrics in Appendix A.

SECTION IV – FINDINGS AND RECOMMENDATIONS

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

Overall, HHS continues to implement changes to strengthen its enterprise-wide information security program. However, opportunities were identified that will allow HHS to continue to enhance its enterprise-wide information security program. We identified several reportable exceptions in HHS' security program. The exceptions have been consolidated into ten findings for management consideration. Areas for improvement were identified in HHS' Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Action and Milestones (POA&M), Remote Access Management, 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 operation with changing threats, vulnerabilities, technologies, and missions and business processes. The implementation of a continuous monitoring program results in ongoing updates to the 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.

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

- Certain documentation of selected OPDIVs' ISCM programs were not continuously monitored, updated and finalized indicating how OPDIVs address, implement strategies and report on DHS metrics. This includes vulnerability management, software assurance, information management, patch management, license management, event management, malware detection, asset management, and network management.
- Instances of operational non-compliance with all OPDIVs ISCM program requirements were identified.

HHS is awaiting additional guidance from DHS on the ISCM elements and requirements before it finalizes and fully implements it continuous monitoring strategy Department-wide. In the interim, the HHS OPDIVs are currently developing their own ISCM policies, procedures and implementation strategy.

Without a Department-wide fully-implemented formal enterprise-level continuous monitoring strategy, HHS and its OPDIVs do not have a complete list of processes that need to be performed to assess and 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/resources.

Recommendation:

We recommend that the HHS OCIO continue to:

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

HHS OCIO Response:

HHS OCIO concurred with the finding and recommendation. As noted in the report, HHS is awaiting additional guidance from the Department of Homeland Security (DHS) on the ISCM elements and requirements before it finalizes and fully implements it continuous monitoring strategy Department-wide. HHS OCIO has already updated its ISCM Strategy and formed an OPDIV-wide ISCM working group. HHS' continuing initiatives will include updated enterprise ISCM policies, standards and procedures, based on the new software tools that will be implemented across the OPDIVs and the future dashboards designed by DHS.

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 five OPDIVs' configuration management policies and procedures were not updated timely, reviewed timely, or finalized.
- Instances of non-compliance with configuration management policies and procedures were noted at four of the five OPDIVs specific to patch management, software maintenance, baseline compliance assessments, and vulnerability scans performed through Security Content Automation Protocol tools.
- Waivers documenting the OPDIVs' acceptance of risks were not completed timely for one of the five OPDIVs.

OPDIVs have not fully developed, defined, and implemented specific configuration management policies and procedures.

Without a fully developed configuration management process, the OPDIVs' information systems may be exposed to vulnerabilities and exploitation.

Recommendation:

The findings identified are specific to the OPDIVs' information security environment. Detailed information and recommendations were provided to the officials responsible for the OPDIVs, so they could address these specific findings.

HHS OCIO Response:

HHS OCIO has received a copy of the OPDIV audit reports and is coordinating a review of the specific findings in order to evaluate the trends, identify common issues and support individual OPDIV remediation. OCIO will review all the information and determine if additional/ updated enterprise configuration management policies and/or procedures would assist the OPIVs, as well. These findings were discovered in only one of the OPDIVs reviewed during FY 15; therefore, OCIO does not believe that these are truly reflective of the overall Department's performance with respect to configuration management.

EY Response:

After reviewing the HHS OCIO's response, we maintain that our findings and recommendations are valid. HHS OCIO should continue to implement the actions noted in their response. With respect to the scope of the performance audit, EY did not review the overall control structure for HHS. Fieldwork was performed for a sample of five of the twelve HHS OPDIVs. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objectives.

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.

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

- Account management procedures were not followed by four of the five OPDIVs. This included maintaining documentation for new personnel and shared accounts, removing inactive accounts timely, and disabling or removing accounts of transferred and terminated personnel timely, and maintaining documentation to evidence the recertification of accounts.
- One OPDIV did not perform a recertification of its accounts timely.

Four of the five OPDIVs did not comply with their procedures for managing user access provisioning, user access de-provisioning, and general user account management.

Weaknesses in identity and access management controls may increase the risk of inappropriate access to the HHS network, information systems and data.

Recommendation:

The findings identified are specific to the OPDIVs' information security environment. Detailed information and recommendations were provided to the officials responsible for the OPDIVs to address these specific findings.

HHS OCIO Response:

HHS OCIO is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OPDIV remediation. HHS OCIO will review all the information and determine if additional/updated enterprise identity and access management policies and/or procedures would assist the OPDIVs.

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 are reported by affected persons to the appropriate personnel.

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

- The HHS CSIRC did not have an oversight process to confirm that the OPDIVs have reported their incidents in accordance with requirements defined by the HHS OCIO and other federal divisions, including the United States Computer Emergency Readiness Team (USCERT).
- Two of the five OPDIVs had not updated their incident response plan as required by the HHS OCIO.

The HHS OCIO has not enforced documentation review requirements of the OPDIVs' incident response plans as specified in applicable policies and procedures. Also, HHS is responsible for tracking report times, but has not performed additional procedures to confirm the OPDIVs are providing the required data timely.

Without an effective incident response plan, HHS may not resolve critical incidents timely, thereby increasing security risk to the HHS environment. Without updating tracking tools in a timely manner with accurate report times, there is a potential for HHS to be considered not in adherence to requirements from the Office of Management and Budget (OMB).

Recommendations:

We recommend that the HHS OCIO continue to:

- Implement an oversight protocol to monitor the OPDIVs' timely reporting of incidents to the appropriate parties.
- Monitor that the policies and procedures for incident response developed at the OPDIVs' are reviewed and updated on an annual basis.

HHS OCIO Response:

The HHS OCIO partially concurred with the finding and recommendations. The HHS Computer Security Incident Response Center (CSIRC) adheres to all US-CERT reporting requirements and reviews OPDIV tickets for data quality and completion. Starting in 2016, CSIRC is scheduled to complete two incident response plan tabletop exercises per year with each OPDIV, where the OPDIV policies, procedures and plans are tested to ensure that they are up-to-date, effective and in compliance with US-CERT, HHS OCIO, and other Federal guidelines.

EY Response:

After reviewing the HHS OCIO's response, we maintain that our findings and recommendations are valid. HHS OCIO should continue to implement the actions noted in their response.

Finding #5 – Risk Management

The Risk Management Framework (RMF), as developed by the National Institute 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 with HHS' risk management program:

- The Department-level system inventory was not reconciled to the OPDIV-managed system inventory tools with those of three of the five OPDIVs to ensure that they are complete, accurate, and effectively managed.
- For the systems selected for four of the five OPDIVs, non-compliance with the risk management program was noted. This included security controls selected for testing that were not satisfied, partially implemented, not found or noted as inherited to an enterprise system control without sufficient evidence, and POA&Ms were not documented.

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.

Without establishing a consistent security authorization process that meets minimum IT security requirements, HHS management will not be able to evaluate 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.

Recommendations:

We recommend that the HHS OCIO continue to:

- Perform a detailed reconciliation with the HHS system inventory and each OPDIV system inventory on a monthly basis.
- Provide guidance to the OPDIVs specific to implementing a risk management program that is consistent with the HHS and NIST guidelines.

HHS OCIO Response:

The HHS OCIO partially concurred with the finding and recommendation. HHS OCIO will be implementing a new eGRC tool across the enterprise in conjunction with the DHS supplied Continuous Diagnostics Mitigation (CDM) tool 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. As these new tools are implemented, OCIO will be issuing new policies, standards, and/or guidance related to improved security implementation and tracking.

EY Response:

After reviewing the Agency's comments, we maintain that our findings and recommendations are valid. HHS OCIO should continue to implement the actions noted in their response.

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 information in today's highly networked systems environment without providing their people involved in using and managing IT training to: (a) understand their roles and responsibilities related to the organizational mission; (b) understand the organization's IT security policy, procedures, and practices; and; (c) have at least 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 with HHS' security training program:

- Appropriate role-based training was not taken by the some personnel at two of the five OPDIVs.
- One of the five OPDIVs was not able to identify their personnel that held significant security/responsibilities.

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:

The findings identified are specific to the OPDIVs' security training program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

HHS OCIO Response:

HHS OCIO is coordinating a review of specific findings in order to evaluate trends, identify common issues and support individual OPDIV remediation. HHS OCIO will review all the information and determine if additional/updated security training policies and/or procedures would assist the OPDIVs.

Finding #7 – Plan of Actions 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 with HHS' POA&M management program:

- Findings included in various security control assessments, external audit, internal audit, and performance audit reports were not recorded in three of the five OPDIVs' POA&M records.
- For four of the five OPDIV POA&M records, there were many POA&Ms in "ongoing" or "delayed" status that had estimated completion dates that had expired or contained blank fields for allocated personnel resources or points of contacts.
- Several POA&M records tracked and monitored by the OPDIV were not reconciled with POA&M records tracked by in the HHS OCIO.

Required POA&M information was not consistently recorded and reported to HHS and OPDIV stakeholders. A reconciliation process of the POA&Ms is not performed completely between the OPDIVs and HHS.

Without an effective POA&M process for managing security weaknesses, HHS management has minimal assurance that information system security weaknesses have been identified and adequately resolved. This could lead to inadequate resource allocation or corrective actions that do not adequately address the identified weaknesses and could compromise the overall information security at HHS.

Recommendation:

We recommend that the HHS OCIO continue to:

- Perform a formal reconciliation with HHS' POA&Ms and each OPDIV's POA&Ms on a monthly basis.

In addition, findings were identified that are specific to the OPDIVs' POA&Ms' management program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

HHS OCIO Response:

The HHS OCIO concurred with the finding and recommendation. The HHS OCIO recently implemented a new reporting feature in the HHS Data Warehouse that outputs an online report of issues as an OPDIV uploads POA&M data. Another new feature is in development that will give both OCIO and the OPDIVs the ability to see historical information. This capability will allow management to see progress, issues and have additional oversight into the process. Also, the new enterprise governance, risk and compliance tool will standardize the collection and reporting mechanisms related to POA&Ms and improve OPDIVs and OCIO oversight of mitigation.

HHS OCIO is coordinating a review of specific findings in order to evaluate trends, identify common issues and support individual OPDIV remediation. HHS OCIO will review all the information and determine if additional/updated POA&Ms policies and/or procedures would assist the OPDIVs.

Finding #8 – Remote Access Management

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' remote access management program:

- Instances of remote access/teleworking policies and procedures that had not been updated or not developed.

OPDIVs did not update or finalize their remote access policies and procedures. 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 remote access, thereby leading to potentially unauthorized access to the network.

Recommendation:

The findings identified are specific to the OPDIVs' remote access program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

HHS OCIO Response:

HHS OCIO is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OPDIV remediation. HHS OCIO will review all the information and determine if additional/updated remote access management policies and/or procedures would assist the OPDIVs.

Finding #9 – 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 with HHS' contingency planning program:

- For four of the five OPDIVs, either the Continuity of Operations (COOP) or Business Impact Analysis (BIA) documentation did not meet all stated requirements.
- For selected systems, the Information System Contingency Plan had not been developed and finalized to include all HHS and NIST requirements, did not adequately document or obtain the alternative processing site, or subsequent tests and exercises of the contingency plan had not been performed on the annual basis required.
- For two of the five OPDIVs, instances were identified where a backup either failed or was missed, and subsequently failed follow-up attempts. Also, it was noted that evidence was not provided to support testing of backups.

OPDIVs have not documented and/or updated contingency plan and procedure documentation in accordance with HHS requirements. Four of the five OPDIVs did not have sufficient oversight over information systems they manage to ensure backups and subsequent restorations are consistently performed and that alternative processing and storage sites chosen meet HHS and NIST standards to support the adequate recoverability and security of data.

Without annual testing, reviews, and updates, the contingency plan might not provide adequate coverage of all system components, incorporate lessons learned from plan testing exercises, or address all potentially mission/business critical processes and their interdependencies.

Recommendation:

The findings identified are specific to the OPDIVs' contingency planning program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

HHS OCIO Response:

HHS OCIO is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OPDIV remediation. HHS OCIO will review all the information and determine if additional/updated enterprise contingency planning policies and/or procedures would assist the OPDIVs.

Finding #10 – 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 government agencies and employees.

The following findings were identified with HHS' contractor system program:

- Two of the five OPDIVs did not have an accurate system inventory of contractor and cloud systems.
- For certain contractor systems' security plans and other system authorization documentation, the required security controls were either not tested or testing results was not documented adequately. Testing results that yielded negative results were not incorporated in appropriate OPDIVs' POA&M records for tracking purposes.
- Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU) were not provided for selected systems and/or security authorization documentation for external systems and contractors that have network connections with the agency systems.

OPDIVs did not have sufficient oversight in the security authorization of contractor systems to verify that security controls directed to be tested from the Department are tested by system owners and points of contact. In addition, there is a lack of coordination and review to assess whether information listed in the security authorization documentation is reconciled with active ISA or MOU documentation.

Failure to exercise proper oversight over the security controls implemented and maintained by contractor systems could expose systems to unmitigated vulnerabilities and fosters a false sense of security that invites service interruptions, jeopardizes the availability and reliability of data, and could expose sensitive information. In addition, because there is a lack of documentation or coverage of agreement documents, the risk is increased that management is unaware of applicable components and contracts and that interconnections are not effectively monitored.

Recommendation:

The findings identified are specific to the OPDIVs' contractor systems. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

HHS OCIO Response:

HHS OCIO is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OPDIV remediation. HHS OCIO will review all the information and determine if additional/updated enterprise contractor system policies and/or procedures would assist the OPDIVs.

HHS Comments

In written comments to our draft report, HHS concurred or partially 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 C.

APPENDIX A: OIG Response to DHS FISMA Reporting Metrics 9/30/2015

1: CONTINUOUS MONITORING		
	1.1 Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.	
	1.1.1 Please provide the D/A ISCM maturity level for the People domain.	**Defined (Level 2)**
	1.1.2 Please provide the D/A ISCM maturity level for the Processes domain.	**Defined (Level 2)**
	1.1.3 Please provide the D/A ISCM maturity level for the Technology domain.	**Defined (Level 2)**
	1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall.	**Defined (Level 2)**
	1.2 Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above. Comment: **HHS has formalized its ISCM program through development of ISCM policies, procedures, and strategies.**	

2. CONFIGURATION MANAGEMENT		
	2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **Four of five OPDIVs reviewed have not adequately established a configuration management program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "No" for this section. We noted that the Department and its OPDIVs need to make improvements as noted with "No" below.**	**No**
	2.1.1 Documented policies and procedures for configuration management.	**Yes**
	2.1.2 Defined standard baseline configurations.	**Yes**
	2.1.3 Assessments of compliance with baseline configurations.	**Yes**
	2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings. Comment: **Four of five OPDIVs reviewed need improvement to ensure that scan result deviations are remediated timely.**	**No**
	2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.	**No**
	2.1.6 Documented proposed or actual changes to hardware and software configurations.	**No**
	2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).	**Yes**
	2.1.8 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53: CM-4, CM- 6, RA-5, SI-2).	**No**
	2.1.9 Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).	**No**
	2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above. No additional comments	
	2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability.	**No**
	2.3.1 Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.	**No**

3. IDENTITY and ACCESS MANAGEMENT		
	3.1. Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes? Comment: **Four of five OPDIVs reviewed have established an identity and access management program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "Yes" for this section.**	**Yes**
	3.1.1. Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).	**Yes**
	3.1.2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2).	**Yes**
	3.1.3. Organization has planned for implementation of PIV for logical 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).	**Yes**
	3.1.4. Organization has planned for implementation of 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).	**Yes**
	3.1.5. Ensures that the users are granted access based on needs and separation-of-duties principles.	**No**
	3.1.6. Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers)	**Yes**
	3.1.7. Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.	**No**
	3.1.8. Identifies and controls use of shared accounts.	**No**
	3.2. Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above. No additional comments	

4. INCIDENT RESPONSE and REPORTING		
	4.1. Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **Four of five OPDIVs reviewed have adequately established an incident response and reporting program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "Yes" for this section.**	**Yes**
	4.1.1. Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).)	**Yes**
	4.1.2. Comprehensive analysis, validation, and documentation of incidents.	**Yes**
	4.1.3. When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).	**Yes**
	4.1.4. When applicable, reports to law enforcement and the agency Inspector General within established timeframes.	**Yes**
	4.1.5. Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).	**No**
	4.1.6. Is capable of correlating incidents.	**Yes**
	4.1.7. Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).	**Yes**
	4.2. Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above. No additional comments	

5. RISK MANAGEMENT		
	5.1. Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **Four of five OPDIVs reviewed have adequately established a risk management program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "Yes" for this section.**	**Yes**
	5.1.1. Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.	**Yes**
	5.1.2. Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.	**Yes**
	5.1.3. Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.	**Yes**
	5.1.4. Has an up-to-date system inventory. Comment: **All OPDIVs reviewed need to improve processes to ensure that hardware and software system inventories are up-to-date.**	**No**
	5.1.5. Categorizes information systems in accordance with government policies.	**Yes**
	5.1.6. Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.	**No**
	5.1.7. Implements the approved set of tailored baseline security controls specified in metric 5.1.6.	**No**
	5.1.8. Assesses the security 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.	**Yes**
	5.1.9. Authorizes information system operation 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.	**Yes**
	5.1.10. Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.	**Yes**
	5.1.11. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).	**Yes**

5. RISK MANAGEMENT		
	5.1.12. 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.	**Yes**
	5.1.13. Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).	**Yes**
	5.1.14. The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.	**Yes**
	5.1.15. For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.	**Yes**
	5.2. Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above. Comment: **3 of 5 OPDIVs reviewed had systems that had expired authorizations.**	

6. SECURITY TRAINING		
	6.1. Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **Two of five OPDIVs reviewed have not adequately established a security training program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "No" for this section. We noted that the Department and its OPDIV's need to make improvements as noted with "No" below.**	**No**
	6.1.1. Documented policies and procedures for security awareness training (NIST SP 800-53: AT- 1).	**Yes**
	6.1.2. Documented policies and procedures for specialized training for users with significant information security responsibilities.	**Yes**
	6.1.3. Security training content based on the organization and roles, as specified in organization policy or standards.	**Yes**
	6.1.4. Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.	**No**
	6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.	**No**
	6.1.6. Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).	**Yes**
	6.2. Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above. No additional comments	

7. PLAN OF ACTION & MILESTONES (POA&M)		
	7.1. Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **Four of five OPDIVs reviewed have adequately established a Plan of Action & Milestones program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "Yes" for this section.**	**Yes**
	7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.	**Yes**
	7.1.2. Tracks, prioritizes, and remediates weaknesses.	**No**
	7.1.3. Ensures remediation plans are effective for correcting weaknesses.	**Yes**
	7.1.4. Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates Comments: **All 5 OPDIVs reviewed need to improve its processes to ensure adherence to milestone remediation dates.**	**No**
	7.1.5. Ensures resources and ownership are provided for correcting weaknesses.	**Yes**
	7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).	**Yes**
	7.1.7. Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25).	**No**
	7.1.8. Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53:CA-5; OMB M-04- 25).	**Yes**
	7.2. Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above. No additional comments	

8. REMOTE ACCESS MANAGEMENT		
	8.1. Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **All 5 OPDIV reviewed have adequately established a remote access management program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "Yes" for this section.**	**Yes**
	8.1.1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).	**Yes**
	8.1.2. Protects against unauthorized connections or subversion of authorized connections.	**Yes**
	8.1.3. Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, and Section 5.1).	**No**
	8.1.4. Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).	**Yes**
	8.1.5. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.	**No**
	8.1.6. Defines and implements encryption requirements for information transmitted across public networks.	**Yes**
	8.1.7. Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.	**Yes**
	8.1.8. Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).	**Yes**
	8.1.9. Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).	**Yes**
	8.1.10. Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).	**Yes**
	8.2. Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above. No additional comments	
	8.3. Does the organization have a policy to detect and remove unauthorized (rogue) connections?	**Yes**

9. CONTINGENCY PLANNING (CP)		
	9.1. Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **Four of five OPDIVs reviewed have not adequately established a contingency planning program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; therefore the Department receives a "No" for this section. We noted that the Department and its OPDIVs need to make improvements as noted with "No" below.**	**No**
	9.1.1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).	**No**
	9.1.2. The organization has incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. (NIST SP 800-34)	**No**
	9.1.3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34).	**No**
	9.1.4. Testing of system-specific contingency plans.	**No**
	9.1.5. The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).	**No**
	9.1.6. Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, and NIST SP 800-53).	**Yes**
	9.1.7. Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.	**Yes**
	9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).	**Yes**
	9.1.9. Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).	**No**
	9.1.10. Backups of information that are performed in a timely manner (FCD1, NIST SP800-34, NIST SP 800-53).	**No**
	9.1.11. Contingency planning that considers supply chain threats.	**N/A**
	9.2. Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above. No additional comments	

10. CONTRACTOR SYSTEMS		
	10.1. Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? Comment: **Four of five OPDIVs reviewed have established a program to oversee systems operated on its behalf by contractors or other entities; therefore the Department receives a "Yes" for this section.**	**Yes**
	10.1.1. Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud	**Yes**
	10.1.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).	**No**
	10.1.3. A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private cloud.	**No**
	10.1.4. The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).	**No**
	10.1.5. The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.	**No**
	10.1.6. The inventory of contractor systems is updated at least annually.	**Yes**
	10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above. No additional comments	

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-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices* (October 3, 2014);
- OS *Program Guide for Security Training and Awareness*

APPENDIX C: 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: Thomas M. Salmon
Assistant Inspector General for Audit Services
Department of Health and Human Services

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

DATE: January 9, 2016

SUBJECT: Response to the Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015 (A-18-15-30300)

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) 2015. 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 collaborative efforts to enhance information technology security and further implement safeguards and practices that protect HHS data and the health information of the American public.

If you have any questions or need additional information, please reach out to the HHS Chief Information Security Officer, Sara Hall at sara.hall@hhs.gov or 202-260-6058.

Regards,

Beth Killoran
HHS Chief Information Officer (Acting)

Attachment

CC:
Sara Hall, HHS Chief Information Security Officer
Leo Scanlon, HHS Deputy Chief Information Security Officer
Jeff Arman, OIG Information technology Audit Manager

Response from the HHS Office of the Chief Information Officer (OCIO) regarding the ***Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015 (A-18-15-30300) dated December 10, 2015.***

General Comment:

HHS OCIO appreciates the work and coordination that the Office of the Inspector General (OIG) and Ernest & Young (E&Y) extended to our Operating Divisions (OpDivs) during the 2015 FISMA Audit. As noted in the report, only five (5) of the twelve (12) Operating Divisions are audited each year. HHS recognizes that this is a point in time review of a subset of our security across the enterprise and may not reflect the actual security posture. HHS will use these findings as a tool to further research and analyze the security programs across the other OpDivs in HHS.

Finding #1 - Continuous Monitoring Management

OIG Recommendation:

We recommend that the HHS OCIO continue to:

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

OCIO Response: Concur

As noted in the report, HHS is still awaiting additional guidance from the Department of Homeland Security (DHS) on the ISCM elements and requirements before it finalizes and fully implements it continuous monitoring strategy Department-wide. Since the FY15 audit was performed, OCIO has already updated its ISCM Strategy and formed an OpDiv-wide ISCM working group. HHS also understands that effective continuous monitoring management is rooted in both a strong governance structure and the implementation of tools and technology to provide near real-time insight into the threats and vulnerabilities the Department faces. In September 2015, DHS – under the Continuous Diagnostics and Mitigation (CDM) program – awarded an implementation support contract to assist HHS in implementing hardware, software, configuration and vulnerability management tools received in 2014. Since the time of award, OCIO has coordinated meetings between the vendor provided by DHS and the OpDivs to discuss their current architecture and plans going forward. HHS's continuing initiatives will include updated enterprise ISCM policies, standards and procedures, based on the new software tools that will be implemented across the OpDivs and the future dashboards designed by DHS.

Finding #2 – Configuration Management

OIG Recommendation:

The findings identified are specific to the OPDIVs' information security environment. Detailed information and recommendations were provided to the officials responsible for the OPDIVs, so they could address these specific findings.

OCIO Response:

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OpDiv remediation. OCIO will review all the information and determine if additional/updated enterprise configuration management policies and/or procedures would assist the OpDivs, as well. While OCIO understands the importance of both up-to-date configuration management policies and procedures and timely acceptance of risk, these findings were discovered in only one of the OpDivs reviewed during FY15; therefore OCIO does not believe that these are truly reflective of the overall Department's performance with respect to configuration management.

Finding #3 – Identity and Access Management

OIG Recommendation:

The findings identified are specific to the OPDIVs' information security environment. Detailed information and recommendations were provided to the officials responsible for the OPDIVs to address these specific findings.

OCIO Response:

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OpDiv remediation. OCIO will review all the information and determine if additional/updated enterprise identity and access management policies and/or procedures would assist the OpDivs, as well.

Finding #4 – Incident Response and Reporting

OIG Recommendations:

We recommend that the HHS OCIO continue to:

• Implement an oversight protocol to monitor the OPDIVs' timely reporting of incidents to the appropriate parties.

• Monitor that the policies and procedures for incident response developed at the OPDIVs' are reviewed and updated on an annual basis.

OCIO Response: Partially Concur

The HHS Computer Security Incident Response Center (CSIRC) adheres to all 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.

HHS has a Department-wide incident response community lead by the HHS CSIRC, where subject matter experts share knowledge, challenges and best practices. The CSIRC team works with the OpDivs on a continuing basis regarding new requirements (ex. revised categories), current initiatives, and overall threats and incidents.

Starting in 2016, CSIRC is scheduled to complete two incident response plan tabletop exercises per year with each OpDiv, where the OpDiv policies, procedures and plans are tested to ensure that they are up-to-date, effective, and in compliance with US-CERT, HHS OCIO, and other federal guidelines (including the timeliness and completeness of reported data).

Finding #5 – Risk Management

OIG Recommendations: Partial Concur

We recommend that the HHS OCIO continue to:

• Perform a detailed reconciliation with the HHS system inventory and each OPDIV system inventory on a monthly basis.

• Provide guidance to the OPDIVs specific to implementing a risk management program that is consistent with the HHS and NIST guidelines.

OCIO Response: Partially Concur

The data in the HHS Data Warehouse (HSDW) is a compilation of data uploaded by the OpDivs on a monthly basis. The OpDivs run reports from their individual tools based on a standardized format so that OCIO collects the same data elements in the same format from every OpDiv. OCIO does not change the system and POA&M information supplied by the OpDivs. OCIO does not have access to the tools used at the OpDivs, so any reconciliation must be done by the OpDivs based on the dashboards that OCIO sends out following the monthly data uploads.

OCIO has recently implemented a new reporting feature in HSDW that outputs an online report of issues as an OpDiv uploads system inventory data. If major problems exist on the report, it is rejected and the OpDiv must resubmit the data once it is corrected. In addition, this report

identifies other problems with the data such as expired dates and blank data fields. OpDivs can easily download the report so they can update the data in their reporting tool accordingly, and then resubmit their report. This new feature was put into production for the January 2016 reporting period. In addition, OCIO will be generating additional reports on a monthly basis that will identify missing information and potential risks.

When OCIO was asked to compare the OpDiv reports with the HSDW reports during the audit period, we found cases where the OpDivs did not use the same parameters for the system reports resulting in a difference in the data (i.e. retired or non-operational systems may have been in the OpDiv report), or POA&Ms were closed but this information was not uploaded by the OpDiv to HSDW. HSDW is a data warehouse based on OpDiv submissions.

OpDivs should be following their security authorization process based on NIST and HHS policy. Per these policies, it is the responsibility of the system owners and the OpDiv Chief Information Security Officer's teams to ensure security controls are implemented and documented at the system level and to report this status to OCIO via the HSDW tool.

OCIO will be implementing a new eGRC tool across the enterprise in conjunction with the DHS supplied Continuous Diagnostics Mitigation (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. The OpDivs will still need to ensure that the data they enter into the tool is accurate and that they have done their due diligence in reviewing and documenting the data and supplying supporting evidence. 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 issuing new policies, standards and/or guidance related to improved security implementation and tracking.

Finding #6 – Security Training

OIG Recommendation:

The findings identified are specific to the OPDIVs' security training program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

OCIO Response:

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OpDiv remediation. OCIO will review all the information and determine if additional/updated security training policies and/or procedures would assist the OpDivs, as well.

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

OIG Recommendation:

We recommend that the HHS OCIO continue to:

• Perform a formal reconciliation with HHS' POA&Ms and each OPDIV's POA&Ms on a monthly basis.

In addition, findings were identified that are specific to the OPDIVs' POA&Ms' management program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

OCIO Response: Concur

During 2015 OCIO realized that the OpDivs' overall tracking of POA&M items was not always up to date. OCIO understands that this can be an overwhelming, resource intensive task. Based on our observations of the data being supplied, in order to facilitate better tracking and more frequent updates, OCIO recently implemented a new reporting feature in HSDW that outputs an online report of issues as an OpDiv uploads POA&M data. If major problems exist on the report, it is rejected and the OpDiv must resubmit the report once the data is corrected. In addition, this report identifies other problems with the data such as expired dates and blank data fields. OpDivs can easily download the report so they can update the data in their reporting tool, accordingly, and then resubmit their report. This new feature was put into production for the January 2016 reporting period. Another new feature is in development that will give both OCIO and the OpDivs the ability to see historical information. This capability will allow management to see progress, issues and have additional oversight into the process.

In addition to facilitating system inventory data collection and a risk management program, the new eGRC tool discussed in the *Risk Management* finding will standardize the collection and reporting mechanisms related to POA&Ms and also improve OpDiv and OCIO oversight of mitigation. The OpDivs will still need to ensure that the data they enter into the tool is accurate and that they have done their due diligence in reviewing and documenting the data and supporting evidence, but it will also give OCIO more visibility into the data.

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the additional specific findings in order to evaluate trends, identify common issues and support individual OpDiv remediation. OCIO will review all the information and determine if additional/updated enterprise POA&M policies and/or procedures would assist the OpDivs, as well.

Finding #8 – Remote Access Management

OIG Recommendation:

The findings identified are specific to the OPDIVs' remote access program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

OCIO Response:

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OpDiv remediation. OCIO will review all the information and determine if additional/updated remote access management policies and/or procedures would assist the OpDivs, as well.

Finding #9 – Contingency Planning

OIG Recommendation:

The findings identified are specific to the OPDIVs' contingency planning program. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

OCIO Response:

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OpDiv remediation. OCIO will review all the information and determine if additional/updated enterprise contingency planning policies and/or procedures would assist the OpDivs, as well.

Finding #10 – Contractor Systems

OIG Recommendation:

The findings identified are specific to the OPDIVs' contractor systems. Detailed information and recommendations were provided to the officials responsible for the OPDIVs so that they could address these specific findings.

OCIO Response:

OCIO has received a copy of the OpDiv audit reports and is coordinating a review of the specific findings in order to evaluate trends, identify common issues and support individual OpDiv remediation. OCIO will review all the information and determine if additional/updated enterprise contractor system policies and/or procedures would assist the OpDivs, as well.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu