United States Department of Agriculture
Office of Inspector General

U.S. Department of Agriculture

Office of the Chief Information Officer

Fiscal Year 2015

Federal Information Security Modernization Act

Audit Report 50501-0008-12
November 2015

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2015 Federal Information Security Modernization Act

Audit Report 50501-0008-12

What Were OIG's Objectives

Our objectives were to evaluate USDA's overall IT security program, compliance with FISMA, and the effectiveness of controls over configuration management, incident response, IT training, remote access management, identity and access management, continuous monitoring, contingency planning, and contractor systems.

What OIG Reviewed

The scope was Department-wide and included agency IT audit work completed during FY 2015, other OIG audits completed throughout the year, and the results of contract auditor reviews. This audit covered 8 agencies and staff offices, operating 178 of the Department's 286 general support and major application systems in the systems inventory.

What OIG Recommends

The Department should continue its progress by issuing critical policy and completing actions on the 26 outstanding recommendations from the FYs 2009 through 2014 FISMA audit reports and the 4 new recommendations included in this report.

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its IT security program and practices, as of FY 2015.

What OIG Found

The Office of Inspector General (OIG) found that, although the Department of Agriculture (USDA) continues to improve the security posture of its information technology (IT) infrastructure and associated data, many longstanding weaknesses remain. In fiscal years (FY) 2009-2014, OIG made 57 recommendations for improving the overall security of USDA's systems, but agreed upon corrective actions have been implemented for only 31. Security weaknesses still exist in 3 of the 31 closed recommendations.

We noted the Office of the Chief Information Officer (OCIO) is taking positive steps to improve its security posture. For example, OCIO has improved its incident response and Risk Management Framework. However, the agencies included in this review have not implemented all of the requirements for security training, remote access management, and contingency planning. It is now critical that agencies create and implement agency-specific procedures to ensure compliance with USDA policy and improve its security posture in the future.

Again this year, we continue to report weaknesses in USDA's IT security. The Department has not (1) performed an assessment of the skills, knowledge, and resources needed to effectively implement an Information Security Continuous Monitoring (ISCM) Strategic Plan; (2) defined or formally documented within the ISCM Strategic Plan the organization's process for collecting and considering lessons learned to improve ISCM processes; and (3) developed policies and procedures for remote access and teleworking that comply with National Institute of Standards and Technology (NIST) guidance.

The Department agreed with the recommendations.

United States Department of Agriculture
Office of Inspector General
Washington, D.C. 20250

November 10, 2015

The Honorable Shaun Donovan
Director
Office of Management and Budget
Eisenhower Executive Office Building
17th Street and Pennsylvania Avenue NW.
Washington, D.C. 20503

Dear Mr. Donovan:

Enclosed is a copy of our report, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2015 Federal Information Security Modernization Act* (Audit Report 50501-0008-12), presenting the results of our audit of the Department of Agriculture's (USDA) efforts to improve the management and security of its information technology (IT) resources. USDA and its agencies have taken actions to improve the security over their IT resources; however, additional actions are still needed to establish an effective security program.

If you have any questions, please contact me at (202) 720-8001, or have a member of your staff contact Mr. Gil H. Harden, Assistant Inspector General for Audit, at (202) 720-6945.

Sincerely,

Phyllis K. Fong
Inspector General

Enclosure

Table of Contents

Section 1: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2015 Federal Information Security Modernization Act ... 3

Findings and Recommendations ... 3

Scope and Methodology ... 9

Abbreviations ... 11

Exhibit A: Office of Management and Budget/Department of Homeland Security Reporting Requirements and U.S. Department of Agriculture Office of Inspector General Position ... 12

Exhibit B: Sampling Methodology and Projections ... 37

Background and Objectives

Background

Improving the overall management and security of Information Technology (IT) resources needs to be a top priority for the Department of Agriculture (USDA). Technology enhances users' ability to share information instantaneously among computers and networks, but it also makes organizations' networks and IT resources vulnerable to malicious activity and exploitation by internal and external sources. Insiders with malicious intent, recreational and institutional hackers, and attacks by foreign intelligence organizations are a few of the threats to the Department's critical systems and data.

On December 17, 2002, the President signed the e-Government Act (Public Law 107-347), which includes Title III, Federal Information Security Management Act (FISMA 2002). FISMA 2002 permanently reauthorized the framework established by the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. FISMA continued the annual review and reporting requirements introduced in GISRA, and also included new provisions that further strengthened the Federal Government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems.

On December 18, 2014, the President signed the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law 113–283) which amended FISMA 2002 to (1) reestablish the oversight authority of the Director of Office of Management and Budget (OMB) with respect to agency security policies and practices, and (2) set forth authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. FISMA requires the Secretary to develop and oversee implementation of operational directives requiring agencies to implement the Director's standards and guidelines for safeguarding federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. It authorizes the Director of OMB to revise or repeal operational directives that are not in accordance with the Director's policies. FISMA also directs the Secretary to consult with, and consider guidance developed by, the National Institute of Standards and Technology (NIST) to ensure that operational directives do not conflict with NIST information security standards.

FISMA changes the annual reporting requirements by requiring agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the Government Accountability Office (GAO). It requires such reports to include: (1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information. Further, it requires the OMB Director, in consultation with DHS, to report to Congress on the "effectiveness of information security policies and practices." NIST was tasked to work with agencies in developing standards as part of its statutory role in providing technical guidance to Federal agencies.

Instructions for Fiscal Year (FY) 2015 FISMA reporting are outlined in the OMB M-16-03 *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. DHS uses the CyberScope website for consolidated reporting.

FISMA requires that the head of each agency shall be responsible for:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- Complying with the requirements of NIST's related policies, procedures, and standards;
- Ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes; and
- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing risk, determining the levels of information security, implementing policies to cost-effectively reduce risks, and periodically testing and evaluating security controls.

In addition, FISMA requires each agency to have an annual independent evaluation of its information security program and practices and to determine the effectiveness of its program and practices. The evaluations are to be performed by the agency's Inspector General or an independent evaluator, and the results of these evaluations are to be reported to OMB.

Objectives

The objectives of this audit were to evaluate the status of USDA's overall IT security program by evaluating the:

- Effectiveness of the Department's oversight of agencies' IT security programs and compliance with FISMA;
- Agencies' systems of internal controls over IT assets;
- Department's progress in establishing a Departmentwide security program, which includes effective assessments and authorizations;
- Agencies' and the Department's plan of action and milestones (POA&M) consolidation and reporting process; and
- The effectiveness of controls over configuration management, incident response, IT training, remote access management, identity and access management, continuous monitoring, contingency planning, and contractor systems.

Section 1: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2015 Federal Information Security Modernization Act

Findings and Recommendations

This report constitutes the Office of Inspector General's (OIG) independent evaluation of USDA's IT security program and practices, as required by FISMA, and is based on the questions provided by OMB and DHS (OMB/DHS). These questions are designed to assess the status of the Department's security posture during FY 2015. The OMB/DHS framework requires OIG to audit processes, policies, and procedures that had been documented and implemented, and were being monitored during FY 2015.

The Office of the Chief Information Officer (OCIO) continues to take positive steps to improve the Department's security posture. OCIO released two critical Departmentwide policies which, once implemented, should improve IT security within USDA. However, USDA's FISMA score, as calculated by OMB, is expected to decline this year. Although OCIO has improved in incident response and the Risk Management Framework (RMF), the agencies included in this year's review have not implemented all of the requirements for security training, remote access management, and contingency planning. These weaknesses at the agency level have a negative effect on USDA's security posture as a whole and, consequently, the Department's FISMA results.

USDA needs to find a way to make sure each agency and staff office understands that how well it implements IT security directly impacts USDA's overall security posture and FISMA score. The decline in this year's FISMA score was caused by the deficiencies identified in the individual agencies reviewed. For USDA to attain a security posture that is secure and sustainable, all 35 of its agencies and offices must consistently implement Departmental policy based on a standard methodology. Once all of the Department's agencies and offices are compliant with NIST and USDA security policies, USDA's security posture will be consistent, efficient, and sustainable. The degree to which USDA, as a whole, complies with FISMA and other security guidance is directly correlated to the security posture of each agency and office. Once each and every agency and office is in compliance with USDA's policies, USDA as a whole will be FISMA compliant and, more importantly, will have a sustainable security posture.

USDA is working to improve its IT security posture, but many longstanding weaknesses remain. We continue to find that OCIO has not implemented corrective actions that the Department has committed to in response to prior OIG recommendations. In FYs 2009 through 2014, OIG made 57 recommendations for improving the overall security of USDA's systems, but only 31 of these have been closed (i.e., the agreed upon corrective action has been implemented). Our testing identified that security weaknesses still exist in 3 of the 31 closed recommendations. Due to these identified outstanding recommendations and weaknesses, we continue to report a material weakness in USDA's IT security that should be included in the Department's Federal Managers Financial Integrity Act report. Based on these outstanding recommendations, and the findings in

this report, OIG concludes that the Department lacks an effective information security program and practices.

USDA is a large, complex organization that includes 35 separate agencies and staff offices, most with their own IT infrastructure. Each of USDA's 35 agencies and staff offices, including OCIO, needs to be held accountable for implementing the Department's policies and procedures. Once compliance by all agencies is attained, FISMA testing results should be similar, regardless of which agency is selected for testing. Also, the Department's overall security posture should improve.

The following paragraphs summarize the key matters discussed in Exhibit A of this report, which contains OIG's responses to the OMB/DHS questions. These questions were defined on the DHS CyberScope FISMA reporting website.

To address the FISMA metrics, OIG reviewed IT systems in individual agencies, OIG independent contractor audits, annual agency self-assessments, and various OIG audits throughout the year.[1] Since the scope of each review and audit differed, we could not use every review or audit to address each question.

During our review, we found that USDA had established a continuous monitoring program. Specifically, we found that the Department has issued a policy, as well as procedures, for continuous monitoring. The Department has also issued the *U.S. Department of Agriculture Strategic Plan for Information Security Continuous Monitoring* (ISCM) as its enterprise-wide ISCM Program.[2] However, we found issues with regard to the Department's implementation of its ISCM Program. Specifically, we found that USDA has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Also, the Department has not yet defined how it will use automation to produce an accurate inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. Overall we rate the level of the Department's ISCM at the ad hoc level, the first level in continuous monitoring maturity.[3]

The Department has established, and maintains, a security configuration management program. However, there are opportunities for improvement. Specifically, we found that the Department has established adequate policy and made standard baseline configurations available for all applicable operating systems; however, agencies have not followed the policy or baselines when configuring servers and workstations. At one agency, we found over 64 percent of NIST's baseline settings for Windows servers had deviations without the proper documentation. In the

---

[1] Agency annual self-assessments are derived from OMB Circular A-123, which defines *Management's Responsibilities for Internal Control in Federal Agencies* (December 21, 2004). The Circular requires agency management to annually provide assurances on internal control in Performance and Accountability Reports. During annual assessments, agencies take measures to develop, implement, assess, and report on internal controls, and take action on needed improvements.

[2] *U.S. Department of Agriculture Strategic Plan for Information Security Continuous Monitoring*, Version 1.2, (July 2015).

[3] Ad hoc is the first level of continuous monitoring and means that the ISCM program is not formalized and ISCM activities are performed in a reactive manner. An ad hoc program does not meet Level 2 requirements for a defined program consistent with Government standards.

FY 2010 FISMA audit, OIG recommended the Department ensure scanning be performed to assess compliance with the baseline configurations and to identify vulnerabilities, as required by NIST. This recommendation remains open; OCIO has exceeded its estimated implementation date of August 30, 2011.

The Department has established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines for identifying users and network devices. For example, the Department has developed an account and identity management policy that is compliant with NIST standards and has adequately planned for Personal Identification Verification (PIV) implementation for logical and physical access in accordance with Government standards.[4] The Department has also completed a centralized enterprise solution for access management, which provides a standardized system that automates identity management. However, our testing identified opportunities for improvement. We found that agencies did not ensure that users were granted access based on need, and agencies did not terminate or deactivate employee accounts when access was no longer required. Departmental policy requires that all user identifications and passwords, or other means of accessing files or using computer resources, shall be permanently disabled immediately upon notice of termination.[5]

The Department has established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. However, the newly issued incident policy did not include the required NIST element of performance measures.[6] Although USDA's incident handling has improved, we continue to find that the Department is not consistently following its own policy and procedures in regard to incident response and reporting. Based on our sample results, we estimate that 58 (about 8 percent) of 767 incidents were not handled in accordance with Departmental procedures.[7,8] Additionally, of the 58 incidents not handled in accordance with procedures, we estimate that USDA did not report 20 of 767 incidents (about 3 percent) to the United States-Computer Emergency Response Team (US-CERT) within the required timeframe. Of these incidents, three were the result of lost or stolen devices and were not reported to law enforcement as required.[9]

---

[4] The Executive Branch mandate entitled, *Homeland Security Presidential Directive 12* (HSPD-12), originally issued in August 2004, requires Federal agencies to develop and deploy, for all of their employees and contract personnel, a PIV credential which is used as a standardized, interoperable card capable of being used as employee identification and allows for both physical and IT system access.

[5] Departmental Regulation (DR) 3505-003, *Access Control Policy* (August 11, 2009).

[6] NIST Special Publication (SP) 800-61 Rev. 2, *Computer Security Incident Handling Guide* (August 2012).

[7] Agriculture Security Operations Center (ASOC) Computer Incident Response Team Standard Operating Procedure (SOP)-ASOC-001, *Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents* (June 9, 2009).

[8] We are 95 percent confident that between 16 (about 2 percent) and 101 (about 13 percent) incidents were not handled in accordance with Departmental procedures. Additional sample design information is presented in Exhibit B.

[9] The US-CERT is part of DHS' National Cybersecurity and Communications Integration Center and leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans.

We found that the Department has not developed an organization-wide risk management strategy that addresses risk from an organization perspective.[10] The Department has issued a guide[11] that addresses the six step RMF process.[12] Although improvements have been made, we continue to find authorization issues. For a system to become operational, NIST SP 800-37 requires USDA agencies to follow the RMF process to obtain an authorization to operate (ATO) and to effectively manage risk for their systems. In order for an ATO to be granted, systems must be categorized, controls identified and implemented, risks assessed, and the final concurrency review examined to proceed with accreditation. We found 17 operational systems with expired ATOs. The Department said these systems were necessary for USDA operations and therefore needed to operate without ATOs for business reasons. In the FY 2012 FISMA report, OIG recommended the Department verify that all systems have the proper ATO prior to implementation. USDA agreed and management decision has been reached, but OCIO has exceeded its estimated completion date of September 30, 2013 (i.e., the agreement between OIG and the agency on the corrective action plan to address the recommendation). As a result, these systems are operating without proper security certification, which leaves the Department vulnerable because the systems have not been through proper security testing.

The Department has established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The Department and one of two agencies we tested had policy and procedures[13] that met all NIST requirements for annual security awareness training and for specialized security awareness training.[14] However, we identified opportunities for improvement. Specifically, one of the two agencies we reviewed had not established procedures for annual security awareness training or specialized security awareness training. Additionally, in both reviewed agencies, more than 16 percent of the individuals reviewed had not completed the annual security awareness training and more than 51 percent had not completed specialized security training.[15]

The Department has established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, which tracks and monitors known information security weaknesses.[16] However, our testing identified some areas for improvement. For example, agencies were not creating POA&Ms for unresolved vulnerabilities existing for

---

[10] NIST SP 800-37 revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010), defines tier 1 of a risk management framework as addressing risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy.

[11] *USDA Six Step Risk Management Framework (RMF) Process Guide*, Revision 2.44 (May 2015).

[12] RMF is a NIST publication. The publication promulgates a common framework which is intended to improve information security, strengthen risk management, and encourage reciprocity between Federal agencies. NIST SP 800-37 revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010), was developed by the Joint Task Force Transformation Initiative Working Group. OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

[13] DR 3545-001, *Information Security Awareness and Training Policy* (October 22, 2013).

[14] Departmental SOP-CPPO-018, *Information Security Awareness Training* (April 21, 2011).

[15] NIST SP800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

[16] A POA&M is a tool that identifies tasks needing to be accomplished to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of efforts to correct security weaknesses found in programs and systems. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and scheduled completion dates for the milestones. The goal of a POA&M should be to reduce the risk of the weakness identified.

over 30 days, as required by Departmental policy.[17] In addition, our review of POA&Ms within Cyber Security Assessment and Management (CSAM) tool found that agencies were not adequately detailing plans for remediation and were not including proper supporting documentation for effective closure. We estimate that 123 of the 819 POA&Ms that were closed during FY 2015 had remediation actions that did not sufficiently address the identified weakness.[18] We also noted that priority levels are not being identified in CSAM for each POA&M and that milestone dates were not always adhered to.

The Department has established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. However, our testing identified that Departmental policies for remote access and teleworking did not meet NIST requirements.[19,20] There were three policy areas outlined by NIST that were not addressed in the Departmental policy. The three areas were the administration of remote access servers, documenting the telework security policy in the System Security Plan (SSP), and periodic reassessment of policies associated with telework devices. We also found one of the two agencies we reviewed did not have a remote access policy or procedures fully developed.

The Department has established and maintains an enterprise-wide business continuity/disaster recovery program. However, our testing identified opportunities for improvement. Specifically, Departmentwide, we found that 149 out of 275 systems did not have evidence of annual testing of contingency plans, as required by NIST and the Department. We sampled 61 systems from the Department and reviewed the last 3 years of contingency plan testing. If 1 of the 3 previous years did not have evidence of testing, we considered it as not meeting the requirement for ongoing testing of contingency plans. Based on our sample results, we estimate that 125 systems, about half the systems in the Department, did not have evidence of ongoing testing.[21] We found the template provided to the agencies by the Department for contingency planning purposes had been updated, was available to the agencies, and contained all of the NIST-required elements. In addition, during our detailed testing at two agencies, we found one agency had not updated its contingency plans in over 9 years.

We found the Department had a policy for information security oversight of systems operated on USDA's behalf by contractors or other entities, including systems and services residing in the public cloud. We found one of the two agencies reviewed did not have documented policies and procedures. FISMA requires USDA to maintain a complete inventory of systems operated on the organization's behalf by contractors or other entities, including cloud systems and services. We reviewed 24 operational contractor systems in CSAM and found 18 systems with unsigned SSPs, 8 systems with expired ATOs, and 9 systems with insufficient interconnection

---

[17] Departmental Manual (DM) 3530-001, *USDA Vulnerability Scan Procedures* (July 20, 2005), requires a POA&M to be developed in accordance with FISMA reporting requirements for any unresolved critical vulnerabilities existing for more than 30 days from the date of the scan.
[18] We are 95 percent confident that between 50 (6 percent) and 196 (25 percent) of closed POA&Ms in FY 2015 had remediation actions that did not sufficiently address the identified weaknesses in accordance with Government policies. Additional sample design information is presented in Exhibit B.
[19] USDA DR 3505-003, *Access Control for Information and Information Systems* (February 10, 2015).
[20] NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security*, Revision 1 (June 2009).
[21] We are 95 percent confident that between 97 (about 40 percent) and 153 (62 percent) systems did not have evidence of ongoing testing. Additional sample design information is presented in Exhibit B.

documentation.[22] In addition, we identified 35 cloud systems. We found 6 were not listed in USDA's inventory, and 1 system was marked as a child system.[23]

The following recommendations are new for FY 2015. Because 26 recommendations from FYs 2009 through 2014 have not been closed, we have not made any repeat recommendations. If the plans initiated to close out the FY 2009 through 2014 recommendations are no longer achievable, due to budget cuts or other reasons, then OCIO needs to update those closure plans and request a change in management decision, in accordance with Departmental guidance.

Recommendation 1

Perform an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program.

Recommendation 2

Define within the ISCM Strategic Plan (or other formal document) USDA's process for collecting and considering lessons learned to improve ISCM processes.

Recommendation 3

Define within the ISCM Strategy or Plan (or other formal document) how USDA will use automation to produce an accurate inventory of authorized and unauthorized devices.

Recommendation 4

Develop a remote access and telework policy and procedures that fully comply with NIST.

[22] NIST SP 800-53, control CA-3, states that interfaces or interconnections between systems are to be documented, including the interface characteristics, security requirements, and nature of the information communicated.
[23] *USDA's Risk Management Framework (RMF) Process Guide* states that contractor-provided services also include "Cloud"-like systems. Any system identified as a type of cloud system must be its own system in CSAM. It cannot be a child of, or a part of, another system.

Scope and Methodology

The scope of our review was Department-wide and included agency IT audit work completed during FY 2015. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Fieldwork for this audit was performed from March 2015 through October 2015. In addition, this report incorporates OIG audits completed during the year. Testing was conducted at offices in the Washington, D.C., and Kansas City, Missouri, areas. Additionally, we included the results of IT control testing and compliance with laws and regulations performed by contract auditors and agency self-assessments. In total, our FY 2015 FISMA audit work covered eight agencies and staff offices:

- Food and Nutrition Service
- Forest Service (FS)
- Farm Service Agency
- Natural Resources Conservation Service
- Office of the Chief Financial Officer
- OCIO
- Risk Management Agency (RMA)
- Rural Development (RD)

These agencies and staff offices operate 178 of the Department's 286 general support and major application systems.[24]

To accomplish our audit objectives, we performed the following procedures:

- Consolidated the results and issues from our prior IT security audit work and the work contractors performed on our behalf. Contractor audit work consisted primarily of audit procedures found in the GAO's *Financial Information System Control Audit Manual.*
- Performed detailed testing specific to FISMA requirements at selected agencies, as detailed in this report.
- Gathered the necessary information to address the specific reporting requirements outlined in OMB M-16-03 *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements.* DHS uses the website CyberScope to consolidate the reporting.
- Evaluated the Department's progress in implementing recommendations to correct material weaknesses identified in prior OIG and GAO audit reports.

[24] OMB Circular A-130, Appendix III, defines a major application as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A general support system is defined as an interconnected set of information resources under the same direct management control that share common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

- Performed statistical sampling for testing where appropriate. Additional sample analysis information is presented in Exhibit B.

We compared test results against NIST controls, OMB/DHS guidance, e-Government Act requirements, and Departmental policies and procedures to determine compliance.

Abbreviations

ASOC .....Agriculture Security Operations Center
ATO.....Authorization to Operate
BCP .....Business Continuity Plan
BIA.....Business Impact Analysis
CDM.....Continuous Diagnostics and Mitigation
CIO.....Chief Information Officer
CSAM.....Cyber Security Assessment and Management
CSP.....Cloud Service Provider
D/A.....Department/Agency
DHS.....Department of Homeland Security
DM .....Departmental Manual
DR .....Departmental Regulation
DRP .....Disaster Recovery Plan
FIPS.....Federal Information Processing Standard
FISMA 2002 .....Federal Information Security Management Act
FISMA.....Federal Information Security Modernization Act
FS .....Forest Service
FY.....Fiscal Year
GAO .....Government Accountability Office
GISRA.....Government Information Security Reform Act
HSPD-12.....Homeland Security Presidential Directive-12
ISA .....Interconnection Security Agreement
ISCM .....Information Security Continuous Monitoring
IT.....Information Technology
MOU .....Memorandum of Understanding
NIST.....National Institute of Standards and Technology
OCI.....Office of Compliance and Integrity
OCIO .....Office of the Chief Information Officer
OIG.....Office of Inspector General
OMB.....Office of Management and Budget
OS.....Operating System
PIV .....Personal Identification Verification
POA&M .....Plan of Action and Milestones
RD .....Rural Development
RMA.....Risk Management Agency
RMF .....Risk Management Framework
SAR.....Security Assessment Report
SLA .....Service Level Agreements
SOP .....Standard Operating Procedure
SP .....Special Publication
SSP.....System Security Plan
TT&E .....Test, Training, and Exercise
US-CERT .....US-Computer Emergency Response Team
USDA.....Department of Agriculture
USGCB.....United States Government Configuration Baseline

Exhibit A: Office of Management and Budget/Department of Homeland Security Reporting Requirements and U.S. Department of Agriculture Office of Inspector General Position

OMB/DHS' questions are set apart using boldface type in each section. We answered direct questions, in boldface, with either a Yes, a No, or the appropriate level in the Continuous Monitoring Management section.

The universe of systems and agencies reviewed varied during each audit or review included in this report. As part of FISMA, OIG reviewed: systems and agencies, audit work conducted for OIG by independent public accounting firm contractors, annual agency self-assessments, and various OIG audits conducted throughout the year.[25] Since the scope of each review and audit differed, we could not use every review or audit to answer each question.

The audit team reviewed all 10 FISMA areas and incorporated statistical sampling into three review areas. Each of the three areas was represented by the relevant universe associated with it. The specific sample designs are summarized in Exhibit B.

Section 1: Continuous Monitoring Management

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. – Level 1: Ad Hoc

1.1.1 Please provide the Department/Agency (D/A) ISCM maturity level for the People domain. – Level 1: Ad Hoc

OIG found that USDA has defined its ISCM stakeholders and their responsibilities; however, this information has not been fully communicated across the organization. Additionally, OIG found that USDA has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. USDA also has not fully defined how ISCM information will be shared with individuals with significant security responsibilities, or will be used to make risk-based decisions, and USDA is still tailoring the framework from OMB/DHS to fit USDA. OIG also found that USDA has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements; however, OCIO plans to leverage the newly established Continuous Diagnostics and Mitigation

[25] Agency annual self-assessments are required by OMB Circular A-123, *Management's Responsibility for Internal Control* (December 21, 2004), which defines management's responsibility for internal controls in Federal agencies. The Circular requires agencies' management to annually provide assurances on internal control in its Performance and Accountability Report. During the annual assessment, agencies take measures to develop, implement, assess, and report on internal control, and to take action on needed improvements.

(CDM)[26] tools to allow for more robust data to be fed into agency dashboards for real-time automated control testing.

1.1.2 Please provide the D/A ISCM maturity level for the Processes domain. – Level 1: Ad Hoc

Although USDA is inventorying its hardware and software assets, OIG found that ongoing assessments and monitoring of security controls are still being performed in a non-automated fashion. Additionally, USDA has not defined its processes for collecting and considering lessons learned to improve its ISCM processes and has not established automated processes for configuration setting management and common vulnerability management.

1.1.3 Please provide the D/A ISCM maturity level for the Technology domain. – Level 1: Ad Hoc

OIG found that OCIO has identified and defined an automated means of performing some ISCM functions. For example, USDA has an automated inventory of devices and software on most USDA networks. However, there is no automated way to determine whether the devices and software are authorized.

1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall. – Level 1: Ad Hoc

OIG found that USDA has defined the tools it will be using for its ISCM process within the Technology domain; however, both the Processes and People domains still have not been fully defined.

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.

No additional information was provided.

Section 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? – Yes

[26] The CDM program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. CDM offers commercial off-the-shelf tools, with robust terms for technical modernization as threats change. DHS, in partnership with GSA, established a Government-wide acquisition vehicle for CDM. The CDM blanket purchase agreement is available to Federal, State, local, and tribal government entities.

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

2.1.1 Documented policies and procedures for configuration management. – No

OIG compared the Department's Configuration Management policy with NIST's SP 800-53 requirements and found no issues.[27] However, we found one of the two agencies reviewed did not have policies, plans, and procedures developed, documented, and implemented. This occurred because the agency was in the process of updating its policy and procedures but had not yet published them.

2.1.2 Defined standard baseline configurations. – Yes

No exception noted. NIST requires the organization to develop, document, and maintain under configuration control, a current baseline configuration of the information system.[28] The Department has issued policy stating that NIST will be the official baseline configuration guide repository for all operating systems in use at USDA.[29] OIG found that the configuration management program includes defined standard baseline configurations and requires the agencies to use baselines on all systems.

2.1.3 Assessments of compliance with baseline configurations. – No

NIST requires the organization to develop, document, and maintain a current baseline configuration of the information system. We found over 64 percent (41,898 of 64,597) of the settings on the Windows servers at one agency were not compliant with the baseline guides nor were the deviations sufficiently documented. In addition, one other agency self-reported a deficiency with baseline configurations.

In the FY 2009 FISMA report, we recommended that the Department implement effective policies and procedures to ensure agencies use required NIST and Departmental configuration checklists and document the reasons for any settings not implemented. OCIO has exceeded its final action estimated completion date of July 30, 2011.

Also, in the FY 2010 FISMA report, we recommended that the Department ensure documented configuration management procedures are developed and consistently implemented across the Department, including baseline configurations for all approved software and hardware. Any changes to the baseline guides should be documented and approved. OCIO has exceeded its final action estimated completion date of September 30, 2011 for final action.

---

[27] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013). Control CM-1 requires that a formal documented configuration management policy and procedures be developed.
[28] NIST SP 800-70, revision 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers Recommendations* (February 2011).
[29] DR 3520-002, *Configuration Management* (August 12, 2014).

2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings. – No

We found that both agencies reviewed did not have a process for timely remediation of scan result deviations. Specifically, OIG reviewed scan results from the agencies and found one agency with over 9 percent (88,687 of 954,853) of its vulnerabilities not mitigated within 3 months.[30] Additionally, three agencies self-reported that they had an issue with the process for timely remediation of scan result deviations.

2.1.5 For Windows-based components, United States Government Configuration Baseline (USGCB) secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented. – Yes

No material exceptions noted. OMB requires the organization to establish and document mandatory security configuration settings for information technology products employed within the information system.[31] One such requirement is the USGCB secure configurations for user workstations and laptops. We found that the Department has achieved over 90 percent USGCB compliance and has implemented a deviation waiver program that appears to be in place and operational.[32]

In the FY 2013 FISMA report, OIG recommended the Department monitor agencies' workstations for USGCB compliance. The recommendation is still open, and OCIO has exceeded its final action estimated completion date of September 30, 2014.

2.1.6 Documented proposed or actual changes to hardware and software baseline configurations. – Yes

No exception noted. NIST requires the organization to document approved configuration-controlled changes to the system. OIG did not identify any problems with documented proposed or actual changes to hardware and software configurations for the agencies reviewed.

2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI-2). – No

The Department requires all agencies to establish and implement procedures for accomplishing vulnerability scanning of all networks, systems, servers, and desktops for which they have responsibility. This includes performing monthly scans and remediating vulnerabilities found as

---

[30] A vulnerability scan is the process of determining the presence of known vulnerabilities by evaluating the target system over the network. DM 3530-001, *USDA Vulnerability Scan Procedures* (July 20, 2005), requires that vulnerability scans are to be performed on a monthly basis for all existing and new networks, systems, servers, and desktops by duly authorized users in accordance with established procedures. DR 3565-003 *Plan of Action and Milestone Policy* (September 25, 2013), requires that a vulnerability be mitigated within 30 days, and if not, a POA&M needs to be created.

[31] OMB M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* (March 22, 2007), requires agencies to adopt the security configurations developed by NIST, the Department of Defense, and DHS.

[32] DR 3520-002, *Configuration Management* (August 12, 2014), requires agencies to submit a request for waiver annually for any deviation from the USGCB.

a result of the scans.[33] We found both agencies reviewed had not implemented software assessing (scanning) capability. We also found that agencies were not scanning all devices monthly as required by NIST. Specifically, we found that one agency was not scanning over 15 percent of its devices monthly as required by NIST. Additionally, three agencies self-reported that they had an issue with the process for timely remediation of scan result deviations.

In the FY 2010 FISMA report, OIG recommended that the Department develop automated procedures for the timely and secure installation of software patches. The recommendation is still open, and OCIO has exceeded its estimated final action completion date of June 15, 2011.

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

NIST requires Federal agencies to establish and document mandatory configuration settings for information technology products employed within the information system and to implement the recommended configuration settings. OIG found that both of the agencies reviewed did not remediate configuration vulnerabilities. Specifically, we found 7,528 configuration-related vulnerabilities on 16 websites maintained by the agencies.[34] Consequently, the websites are at risk for compromise.

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

NIST requires the organization to identify and correct system flaws and incorporate flaw remediation (known as vendor patches) into the organizational configuration management process. We found that both of the agencies reviewed had not implemented a process for timely and secure installation of software patches. Specifically, OIG found at one agency that over 9 percent (2,433 of 25,601) of the vulnerabilities were not corrected within 90 days with an available patch from the vendor. As a result, systems are at risk of compromise when they could have been secured, had the available patch been applied.

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.

OIG reviewed computers in use at USDA specifically looking for operating systems (OS) in use past their end-of-support.[35] We found 240 machines at USDA that were using an OS past its end-of-support. Devices using an expired OS are more vulnerable to malware, and agency data are at greater risk of unauthorized access.

---

[33] A patch is a small piece of software that is used to correct a problem with a software program or an operating system. Most major software companies will periodically release patches, usually downloadable from the internet, that correct very specific problems or security flaws in their software programs.

[34] We utilized a commercially available software package designed to thoroughly analyze web applications and web services (websites) for security vulnerabilities.

[35] End-of-support refers to the date when a vendor no longer provides automatic fixes, updates, or online technical support.

2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability? – No

The Department has issued policy to ensure there is an enterprise deviation handling process within the enterprise; however, it is not integrated with an automated solution.

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. – Yes

No exception noted. The Department has issued policies to ensure the risks introduced by identified deviations are mitigated.

Section 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? - Yes

Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

3.1.1 Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1). – Yes

No exception noted. We found that the Department's current policy was substantially compliant and procedures at the two agencies we reviewed were in compliance with NIST SP 800-53.

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD-12, NIST SP 800-53, AC-2). – No

OIG found that all agencies reviewed identified all users, including Federal employees, contractors, and others who access USDA's systems. However, a contractor review found that two of seven systems did not identify all users with access to USDA's systems. Additionally, one agency self-reported deficiencies in this area.

3.1.3 Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD-12, Federal Information Processing Standard (FIPS) 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). – Yes

No exception noted. We found that both of the agencies reviewed adequately planned for the implementation of PIV cards for logical access in accordance with government policies.[36]

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

No exception noted. We found that the two agencies reviewed adequately planned for the implementation of PIV cards for physical access in accordance with government policies.

3.1.5 Ensures that the users are granted access based on needs and separation-of-duties principles. – No

We found that one out of two agencies reviewed did not ensure that users were granted access based on need and "separation of duties" principles.[37] Additionally, a contractor review found that for three of seven systems reviewed, users were granted access based on needs. As a result, accounts have excessive privileges which may result in the unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

3.1.6 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. Internet Protocol phones, faxes, printers). – Yes

No exception noted. We found that all agencies reviewed identified hardware assets that have user accounts and non-user accounts.

3.1.7 Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy. – No

We found that both reviewed agencies were not ensuring that accounts were terminated or deactivated once access was no longer required. However, a contractor review found that for one of seven systems, accounts were terminated when access was no longer required. Additionally, four agencies self-reported deficiencies in this area. The agencies were not

---

[36] The Executive Branch mandate entitled HSPD-12, originally issued in August 2004, requires Federal agencies to develop and deploy for all of their employees and contract personnel a PIV credential which is used as a standardized, interoperable card capable of being used as employee identification and allows for both physical and information technology system access.

[37] Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment. In effect, checks and balances need to be designed into both the process as well as the specific, individual duties of personnel who will implement the process. Ensuring that such duties are well defined is the responsibility of management.

properly terminating users when access was no longer required, which could result in the unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

3.1.8 Identifies and controls use of shared accounts. – Yes

No exception noted. OIG found that all agencies reviewed do not use shared accounts.

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 information was provided.

Section 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? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1). – No

We found that the Department had developed policy and procedures for incident handling. However, we found that Departmental policy[38] did not include all NIST required elements and the procedures were not consistent with USDA's current practices.[39] Our review of two agencies found that both agencies had developed procedures, but these procedures were not in accordance with USDA's current incident processes.

In the FY 2011 FISMA report, OIG recommended that the Department update its incident handling procedures to reflect current practices. This recommendation has reached management decision but has exceeded OCIO's estimated final action completion date of September 30, 2012.

4.1.2 Comprehensive analysis, validation, and documentation of incidents. – No

Our review found that 11 of 101 incidents were not handled in accordance with Departmental procedures.[40] Based on our overall sample results, we estimate that 58 incidents (8 percent of the universe) were not handled in accordance with Departmental procedures.[41]

---

[38] DM 3505-005, *Cyber Security Incident Management Policy* (October 31, 2013).
[39] NIST SP 800-61, revision 2, *Computer Security Incident Handling Guide* (August 2012).
[40] We based our sample size on a 25 percent error rate and a desired absolute precision of +/-10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 101 incidents for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.
[41] We are 95 percent confident that between 16 (2 percent of the universe) and 101 (13 percent of the universe) FY 2015 incidents were not handled in accordance with Departmental procedures. Additional sample design information is presented in Exhibit B.

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

No material exceptions noted. Based on our testing and our overall sample results, we estimate that less than 3 percent were not reported to US-CERT as required; and therefore, the Department has materially complied.[42]

4.1.4 When applicable, reports to law enforcement and the agency Inspector General within established timeframes. – No

USDA's Incident Response Policy (DM 3505-001), states that OCIO Cyber Security is responsible for incident reporting to OIG, US-CERT, and law enforcement entities when there is a potential violation of the law. Our review of 101 incidents identified 10 which were law enforcement reportable. We found that 3 of the 10 incidents were not reported to law enforcement entities as required.

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). – Yes

No material exceptions noted. Departmental procedures require that, if an incident is not closed after 30 days, the agency is required to open a POA&M. We found that all incidents reviewed were resolved in a timely manner. Additionally, we reviewed incidents to determine if appropriate actions were taken for the resolution of the incident, and identified 1 of 101 incidents which had inadequate remediation actions for closure.

4.1.6 Is capable of correlating incidents. – Yes

No exception noted. The Department has deployed new tools to correlate incidents.

In our FY 2011 and 2012 FISMA reports, OIG recommended the Department deploy adequate resources to monitor and configure new security tools, then adequately report and close the related incidents. Management decision has been reached on both recommendations. Final action has not been achieved for either recommendation and both have exceeded OCIO's estimated completion date of September 30, 2013.

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

No exception noted. We found that the Department has continually improved its overall incident management processes.

[42] We are 95 percent confident that between 9 (about 1 percent) and 32 (about 4 percent) incidents were not reported to US-CERT within the required timeframes.

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 information to provide.

Section 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? – No

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

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. – No

The Department has developed a risk management guide for USDA, but it has not developed a risk management strategy that addresses risk from an organizational perspective.[43] This occurred due to a lack of resources for the team which is responsible for the development and implementation of the governance strategy. As a result, the Department cannot ensure that managing information system-related security risks is consistent with the organization's mission/business objectives and overall risk strategy.

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. – No

As noted in question 5.1.1, the Department does not have a governance structure and an organizational risk management strategy. Therefore, it has not defined the risks from a mission and business process perspective in order to address them from an organizational perspective.

5.1.3 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1. – No

As noted in question 5.1.1, the Department does not have a governance structure and an organizational risk management strategy. Therefore, officials have not defined the information system risks necessary to address them from a mission and business perspective.

[43] *USDA Six Step Risk Management Framework Process Guide* (May 2015).

5.1.4 Has an up-to-date system inventory. – No

The Department does not have an up-to-date inventory. We found six contractor systems not recorded in CSAM.[44] As a result, the organization's systems' confidentiality, integrity, and availability could be exposed to compromise without discovery.

5.1.5 Categorizes information systems in accordance with government policies. – Yes

No exception noted. We generated a report from CSAM which identified the impact level for each of the Department's systems. The report included the impact levels for confidentiality, integrity, and availability, which were categorized as high, moderate, or low.[45] We compared the generated report to NIST's guidance and found no exceptions.[46]

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. – Yes

No exception noted. During our review we did not find an issue with how the Department's risk management program selects the set of baseline security controls. The correct categorization noted in 5.1.5 led to adequate baseline controls being implemented. The Department's RMF Process Guide states that once the security categorization of the information system is documented in CSAM, the corresponding set of controls (high, moderate, or low) will automatically be selected for the information system within CSAM.

5.1.7 Implements the approved set of tailored baseline security controls specified in metric 5.1.6. – Yes

No exception noted. NIST SP 800-53 recommends a set of minimum baseline security controls based on the system's overall categorization. The lower the category, the fewer controls required. The correct categorization noted in 5.1.5 led to adequate controls being implemented.

---

[44] CSAM is a comprehensive system developed by the Department of Justice, which can help in achieving FISMA compliance. CSAM provides a vehicle for the Department, agencies, system owners, and security staffs to (1) manage their system inventory, interfaces, and related system security threats and risks; (2) enter system security data into a single repository to ensure all system security factors are adequately addressed; (3) prepare annual system security documents, such as security plans, risk analyses, and internal security control assessments; and (4) generate custom and predefined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. This includes agency-owned systems or those operated by contractors on the agency's behalf.

[45] FISMA (44 U.S.C. Section 3542) defines integrity as guarding against improper information modification or destruction, and includes ensuring information on repudiation and authenticity. Confidentiality is defined as preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Availability is defined as ensuring timely and reliable access to and use of information.

[46] NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Vol. 1 (August 2008).

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

No exception noted. The Department 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.

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. – No

The Department does not authorize information system operation based on a determination of the risk to organizational operations and assets. We found 17 operational systems with expired ATOs.[47] As a result, these systems are operational, but without proper security certification, which leaves the agencies and the Department vulnerable because the systems have not been through proper security testing.

In the FY 2012 FISMA report, OIG recommended the Department should verify that all systems have the proper ATO prior to implementation. Management decision has been reached, but OCIO has exceeded the estimated completion date of September 30, 2013.

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

No exception noted. The Department does communicate information system-specific, mission/business-specific, and organizational level risks to appropriate levels of the organization.

5.1.11 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., Chief Information Security Officer). – Yes

No exception noted. The Department briefs appropriate personnel through weekly and daily activity reports.

[47] Total number of systems without ATOs generated out of CSAM as of September 9, 2015.

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

No exception noted. The Department's Risk Management program prescribes the active involvement of information system owners and common control providers, CIOs, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

5.1.13 Security authorization package contains system security plan, security assessment report (SAR), POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37). – Yes

No exception noted. The security authorization package contains SSP, SAR, POA&Ms, and accreditation boundaries that are in accordance with government policies.[48]

5.1.14 The organization has an accurate and complete inventory of their cloud systems, including identification of Federal Risk and Authorization Management Program approval status. – No

We reviewed 35 USDA cloud systems and found 6 were not listed in the inventory.

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. – No

The Department was unable to identify the security controls, procedures, policies, contracts, and SLAs in place to track the performance of the CSP and manage the risks of Federal program and personal data stored in cloud systems. This led to the incorrect cloud inventory noted in 5.1.14.

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.

No additional information to provide.

[48] NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* (February 2006), requires the SSP as part of the Assessment and Authorization documentation. It provides an overview of the security requirements of the system and describes the controls in place (or planned) for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system.

Section 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? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1). – No

Exception noted. We determined the Department and both of the reviewed agencies' security awareness policies[49] met the requirements outlined in NIST SP 800-53. In addition, the Department's security awareness training procedures met NIST SP 800-53 requirements.[50] However, one of two agencies we reviewed during this audit did not have adequate procedures in place to ensure employees and contractors received adequate security awareness training.

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities. – No

Exception noted. The Department and both agencies' policies for specialized security training were effective and fully developed in accordance with NIST SP 800-53 for FY 2015.[51] However, we found one of two agencies did not have documented procedures in place to meet NIST requirements.

6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards. – No

Exception noted. NIST SP 800-53 requires agencies to provide role-based training. OIG reviewed the training content for individuals of the two sampled agencies with significant information security responsibilities. We found 316 of 617 users (51 percent) had not completed role-based training.

---

[49] DR 3545-001, *Information Security Awareness and Training Policy* (October 22, 2013).
[50] Departmental SOP-CPPO-018, *Information Security Awareness Training* (April 21, 2011).
[51] NIST SP 800-53 requires the organization to provide basic security awareness training to all users. Additionally, it requires the organization to identify and provide information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software with role-based specialized security training related to their specific roles and responsibilities. The organization is to determine the appropriate content of security training and the specific requirements of the organization and the information systems to which personnel have authorized access.

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

Exception noted. NIST SP 800-53 requires agencies to document and monitor individual information system security training activities and to retain individual training records. During our review of two agencies, we found 7,176 out of 42,788 (over 16 percent) users with login privileges had not completed the annual security awareness training.

In the FY 2010 FISMA report, OIG recommended that the Department ensure its training repository is completely populated and all required personnel receive the training. USDA reported that this recommendation has reached final action; however, we take exception to the recommendation being closed.

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

Exception noted. NIST SP 800-53 requires agencies to provide role-based training. Agencies are required to document and monitor individual information system security training activities and to retain individual training records. OIG reviewed the training content for individuals with significant information security responsibilities in the two sampled agencies. Our testing of 617 employees with significant security responsibilities found 316 employees (51 percent), from the two sampled agencies, had not completed adequate role based training to meet NIST requirements.

6.1.6 Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53). – Yes

No exception noted. We found that the material for the security awareness training contained the appropriate content to meet NIST SP 800-53 and NIST SP 800-50 requirements.[52]

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 information to provide.

[52] NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003).

Section 7: Plan of Action and 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? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

7.1.1 Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation. – Yes

No material exceptions noted. The Department's security manual included a policy establishing a POA&M process for reporting IT security deficiencies and for tracking the status of remediation efforts. We reviewed this document and found it included all required elements. The Department has also established procedures. Our review of the POA&M SOP[53] determined it was updated to include OMB-outlined criteria.[54] Additionally, testing at two agencies found that both had established POA&M procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation. However, both agencies' procedures were lacking elements required by OMB M-04-25.

7.1.2 Tracks, prioritizes and remediates weaknesses. – No

We found the Department's POA&M program tracks weaknesses. However, we identified 200 of 1,069 open and approved POA&Ms as of September 4, 2015, that did not have an identified priority level. The Department uses CSAM as the central repository for POA&Ms, which includes tracking weaknesses, identifying priority levels, and housing all supporting documentation of remediation. In addition, the Department holds bi-weekly meetings with each agency to discuss POA&M status and any outstanding POA&M issues in order to continually monitor agency progress.

7.1.3 Ensures remediation plans are effective for correcting weaknesses. – No

OMB M-04-25 specifies that effective remediation of IT security weaknesses is essential to achieve a mature and sound IT security program and to secure information and systems. It further states that a milestone should identify specific requirements to correct an identified weakness. To test the Department's remediation effectiveness, we reviewed a statistical sample of 60 POA&Ms that were closed during FY 2015 and found 9 were closed without documented

[53] Departmental Oversight and Compliance Division SOP-003, *Plan of Action and Milestones Management* (July 2013).
[54] OMB M-04-25, FY 2004, *Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

remediation plans.[55] Based on our sample results, we estimate 123 POA&Ms (15 percent) were closed in FY 2015 with remediation actions that did not sufficiently address the identified weaknesses.[56] The Department also reviewed 66 POA&Ms and found that 16 were not acceptable due to insufficient documentation to support remediation, or failure to follow proper closure procedures.

In the FY 2009 FISMA report we recommended that the Department develop and implement an effective process to ensure POA&Ms are entered, tracked, and closed properly. Although this recommendation has reached final action and is closed, we take exception to the recommendation being closed.

7.1.4 Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates. – No

We found that 709 of the 2,855 (25 percent) milestones completed in FY 2015 were not completed by the planned milestone finish date. We found that milestone dates are being established, but the remediation dates are not always adhered to.

7.1.5 Ensures resources and ownership are provided for correcting weaknesses. – No

We found that weaknesses were not being remediated. We identified 495 delayed POA&Ms as of September 4, 2015. We determined 231 of the 495 POA&Ms were delayed due to inadequate resources. Additionally, 73 POA&Ms were delayed without providing an explanation.

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). – No

OMB requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been identified. The Department's SOP requires an agency to create a POA&M when an identified weakness cannot be remediated within 30 days. However, we found POA&Ms had not been created for four FY 2013 FISMA Departmental audit recommendations and one FY 2014 FISMA Departmental audit recommendation. Also, we found that two agencies were not creating POA&Ms for vulnerabilities that were outstanding for over 30 days.

7.1.7 Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25). – Yes

No material exception noted.

---

[55] We based our sample size on a 19 percent error rate and desired absolute precision of +/-10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 60 POA&Ms for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

[56] We are 95 percent confident that between 50 (6 percent) and 196 (24 percent) of closed POA&Ms in FY 2015 had remediation actions that did not sufficiently address the identified weaknesses in accordance with Government policies. Additional sample design information is presented in Exhibit B.

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

No exception noted. OIG determined that the Department's POA&M program has established a process for program officials and contractors to report on remediation progress to the CIO on a regular basis, and that OCIO tracks and reviews POA&Ms at least quarterly. We found that the CIO receives monthly and weekly status reports for POA&Ms; additionally, the POA&M lead for the Department meets with agencies on a bi-weekly basis to discuss and address any issues identified during this review of their POA&Ms in progress.

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 information to provide.

Section 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? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

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). – No

Although the Department has a remote access policy,[57] our testing found it did not meet all NIST requirements.[58] There were three policy areas not addressed in the Departmental policy as outlined by NIST. The three areas were the administration of remote access servers, the documentation of the telework security policy in the SSP, and the periodic reassessment of the policies associated with telework devices. Specifically, we found one of two agencies reviewed did not have a remote access policy or procedures fully developed. This occurred because the agency policy provided was too broad and only contained a small section on remote access. As a result, inadequate security over remote access could result in the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

In the FY 2010 FISMA report, we recommended that the Department develop a remote access and telework policy and procedures that fully comply with NIST requirements, and the recommendation has been closed. However, based upon our findings in 8.1.1 above, where three policy areas were not addressed in the Departmental policy, we take exception to the recommendation being closed.

---

[57] USDA DR 3505-003, *Access Control for Information and Information Systems* (February 10, 2015).
[58] NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security*, revision 1 (June 2009).

8.1.2 Protects against unauthorized connections or subversion of authorized connections. – Yes

No exception noted. We found both agencies reviewed were capturing and monitoring (or reviewing) logs for remote access and therefore had programs protecting against unauthorized connections or subversion of authorized connections.

8.1.3 Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1). – Yes

No exception noted. Two of two agencies we reviewed were using the Departmental solutions for multi-factor authentication and for management of mobile device security. We found no issues with the Department's management of mobile device security and multifactor authentication.

8.1.4 Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). – No

As reported in 8.1.1, the Department has a remote access (and telework) policy, but our testing found it did not meet all NIST requirements. Specifically we found one of two agencies reviewed did not have a fully developed telecommuting policy. This occurred because the agency policy and procedures provided no detailed instructions for IT security.

8.1.5 Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. – Yes

No exception noted. We found that both agencies reviewed were requiring PIV (LincPass) cards for logical access and have multi-factor authentication[59] properly implemented. Also, we found that multi-factor authentication for remote access is required by Departmental policy, and the Department's two-factor authentication solution (Enterprise Virtual Private Network) meets NIST requirements for remote electronic authentication.

In the FY 2010 FISMA report, we recommended that the Department complete the Departmental projects that will enforce multi-factor authentication and external media encryption. The recommendation has reached management decision but has exceeded the estimated completion date of September 30, 2011.

8.1.6 Defines and implements encryption requirements for information transmitted across public networks. – Yes

No exception noted. We found two of two agencies reviewed had defined and implemented encryption requirements for information transmitted across public networks.

[59] USDA DR 3505-003, *Access Control for Information and Information Systems* (February 10, 2015).

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

No exception noted. We reviewed two agencies' remote access session time-out settings and found they were compliant with OMB M-07-16 and timed-out after less than 30 minutes of inactivity, after which re-authentication was required.[60]

8.1.8 Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines). – No

Our review of 36 incidents involving lost or stolen remote access devices found 4 were not reported timely, 1 was not handled correctly, and 3 were not reported to law enforcement entities.

8.1.9 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). – No

We found one of two agencies reviewed did not have signed rules of behavior agreements that were adequate in accordance with government policies.

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). – No

We reviewed rules of behavior/user access agreements in 8.1.9 and found one of two agencies reviewed did not have signed rules of behavior agreements that were adequate in accordance with government policies.

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 information to provide.

8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections? – Yes

No exception noted. The Department and both agencies reviewed had policies to detect and remove unauthorized (rogue) connections.

[60] OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

Section 9: Contingency Planning

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? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

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). – Yes

No exception noted. NIST SP 800-53 states that the organization must develop, disseminate, and review/update documented contingency planning policy. We found that the Department's contingency planning policy met these requirements.

9.1.2 The organization has incorporated the results of its system's Business Impact Analysis (BIA) and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (NIST SP 800-34). – No

NIST states that conducting the BIA is a key element in a comprehensive information system contingency planning process.[61] The Department's guide on developing contingency plans requires that a BIA be completed during the concurrency review for each system.[62] We found one of two agencies reviewed by OIG had not incorporated the BIA into their contingency plans and in one agency the BIA had not been updated in 10 years.

9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34). – No

One of the agencies reviewed by OIG did not use the current template provided by the Department because it had not updated its contingency plans in over 9 years.

9.1.4 Testing of system-specific contingency plans. – No

NIST SP 800-53 requires Federal agencies to test contingency plans for information systems, using organization-defined tests. This is done to determine the plans' effectiveness and the organization's readiness to execute the plans. We identified 149 of 275 systems[63] for which USDA system contingency plans had not been tested or documentation had not been updated during FY 2015 as required.[64]

---

[61] NIST SP 800-34, *Contingency Planning Guide For Federal Information Systems* (May 2010).
[62] DM 3570-001, *Disaster Recovery and Business Resumption Plans* (February 17, 2005).
[63] System inventory as of October 1, 2015.
[64] *USDA Contingency Plan Exercise Handbook*, Rev 2.0 (October 2014).

9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). – No

NIST SP 800-53 requires the agency to have procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. We found that the documented business continuity and disaster recovery plans were not in place and cannot be implemented when necessary. For example, we sampled 61 systems from the Department and reviewed the last 3 years of contingency plan testing. If one of the three previous years did not have evidence of testing, we considered the system as not meeting the requirement for ongoing testing of contingency plans. We found that 31 of 61 statistically sampled systems did not have evidence of testing in CSAM.[65] Based on our sample results, we estimate that 125 systems (about 51 percent) did not have evidence of ongoing testing.[66]

9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). – No

NIST SP 800-53 requires Federal agencies to test the contingency plan to determine the effectiveness of the plan and their readiness to execute the plan. We found that all 61 of the systems we reviewed in our sample had documented TT&E programs incorporated in their contingency plans. However, one of two agencies we reviewed did not have a TT&E program and had not tested its system specific contingency plans as noted in 9.1.4.

9.1.7 Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. – No

NIST SP 800-53 requires Federal agencies to test contingency plans for information systems, review the contingency plan test results, and initiate corrective actions, if needed. We sampled 61 systems from the Department and reviewed the last 3 years of contingency plan testing. If one of the three previous years did not have evidence of testing then we considered the system as not meeting the requirement for ongoing testing and maintenance of contingency plans. We found that there were 31 of 61 system contingency plans that did not have evidence of ongoing testing. We also identified 149 of 275 agency systems within the Department that did not have a testing date recorded in CSAM during FY 2015.

9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). – No

NIST SP 800-34 states that all recovery and reconstitution events should be well documented, including actions taken and problems encountered during recovery and reconstitution efforts. An after-action report, with lessons learned, should be documented and updated. Our review of 61 sampled systems from agencies in the Department found that 29 did not have after-action reports

---

[65] We based our sample size on a 30 percent error rate and desired absolute precision of +/- 10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 61 contingency plans for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

[66] We are 95 percent confident that between 97 (about 40 percent) and 153 (62 percent) systems did not have evidence of ongoing testing. Additional sample design information is presented in Exhibit B.

for the current year. As noted in 9.1.4, we found one of two agencies we reviewed did not test system-specific contingency plans and therefore did not have after-action reports.

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

NIST SP 800-53 requires alternate processing sites be established for information systems in case of a disaster. We statistically sampled 61 systems and found 60 of those systems met the requirement to provide an alternate processing site. One system in our sample did not have an alternate processing site that was not subject to the same risks. We also found one of two agencies OIG reviewed did not have an alternate processing site established for any of its IT infrastructure.

9.1.10 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). – Yes

NIST SP 800-53 states that the organization should conduct user-level, system-level, and information system documentation backups. We found both agencies reviewed by OIG were performing backups in a timely manner.

9.1.11 Contingency planning that considers supply chain threats. – Yes

No material exception noted. We found 1 of 61 contingency plans in our statistical sample of Department systems that did not document, or consider, supply chain threats within the contingency plan. This occurred because the disaster recovery plan had not been completed. Based on our sample results, we estimate that less than 7 percent of the systems may not have complied with the requirement to consider supply chain or vendor threats.[67] As noted in 9.1.3, one of two agencies we reviewed did not have current contingency plans and therefore we could not review supply chain threats.

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 information to provide.

[67] We are 95 percent confident that less than 7 percent of the agency systems selected may not have complied with the requirement to consider supply chain threats.

Section 10: Contractor Systems

10.1 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in a cloud external to the organization? – No

The Department has a published policy for overseeing systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization; however, our testing of the inventory identified deficiencies significant enough to indicate that the agencies are not following the guidance, and therefore it is not effectively implemented.

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

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. – No

We found that the Department had documented policies for information security oversight of systems operated on its behalf by contractors or other entities, including USDA systems and services residing in the public cloud. However, we found two of three agencies reviewed during FY 2015 FISMA and other OIG audits, did not have documented policy or procedures. This occurred because one agency's policy and procedures were in draft and another agency was unable to provide the interface procedures.

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

As noted in 10.1.3, we found 18 systems with unsigned SSPs, 8 systems with expired ATOs, 9 systems with insufficient interconnection documentation, and 6 cloud systems not in the inventory. Based upon these results, we determined that the Department's contractor systems program was not ensuring that security controls of contractor systems and services were effectively implemented and in compliance with organization guidelines. Although the Department has sufficient published policies, agencies were responsible for all control procedures and were not sufficiently following Departmental guidance.

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

USDA's contractor systems program does not include a complete inventory of systems operated on its behalf by contractors or other entities (including other government agencies), including organization systems and services residing in public, hybrid, or private clouds. We reviewed 24 operational contractor systems in CSAM and found 18 systems with unsigned SSPs,

8 systems with expired ATOs, and 9 systems with insufficient interconnection documentation. In addition, we identified 35 USDA cloud systems and found 6 were not listed in the inventory and 1 was marked as a child system.

10.1.4 The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5). – No

We reviewed interconnection documentation for 24 operational contractor systems in CSAM and found that 9 had not adequately identified or documented their interfaces in CSAM. This occurred because although the Department had sufficient published policies, the agencies were responsible for all control procedures and were not sufficiently following Departmental guidance.

10.1.5 The organization requires appropriate agreements (e.g., Memorandum Of Understanding, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. – No

The Department's contractor systems program was not requiring appropriate agreements (e.g., Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA), contracts, etc.) for interfaces between these systems and those that it owns and operates. In 10.1.4, we found nine contractor systems that had not adequately identified or documented their interfaces in CSAM, which shows that the program was not sufficiently requiring the appropriate agreements.

In the FY 2012 FISMA report, we recommended the Department develop and implement an effective process for making sure interface connections are documented and that ISAs accurately reflect all connections to the systems. The Department needs to review interfaces during the annual testing processes. Although management decision has been reached, the recommendation was still open and had exceeded USDA's estimated final action completion date of September 30, 2013.

10.1.6 The inventory of contractor systems is updated at least annually. – Yes

No exception noted. We found that the inventory of contractor systems had been updated within the last year.

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 information to provide.

Exhibit B: Sampling Methodology and Projections

Objective:

This sample was designed to support OIG's FY 2015 FISMA audit. The objective of this audit was to evaluate the status of USDA's overall IT security program based on the following overarching criteria:

- Effectiveness of the Department's oversight of agencies' IT security programs, and compliance with FISMA;
- Agencies' systems of internal controls over IT assets;
- Department's progress in establishing a Departmentwide security program, which includes effective assessments and authorizations;
- Agencies' and the Department's POA&M consolidation and reporting process; and
- The effectiveness of controls over configuration management, incident response, IT training, remote access management, identity and access management, continuous monitoring, contingency planning, and contractor systems.

FISMA Audit Universes and Sample Designs:

FISMA contains multiple areas pertaining to various areas of IT security. We incorporated statistical sampling in three FISMA areas. Each of those areas was represented by a different universe. The specific designs are summarized below.

1. Incident Response and Reporting

Universe:
The audit universe consisted of 767 incidents reported during FY 2015, as of March 25, 2015.[68] Each incident had a unique identifier and was categorized based on incident type into one of seven categories (coded as 0 to 6).

Sample Design:
Each incident category has specific procedures and timelines that must be met by OCIO and the agency. While standards differ among the categories, the standards fall into four common groups: checklist requirements, reporting requirements, timely resolution, and damage containment. Thus, each incident response can be assessed as "pass" or "fail" when compared to the criteria that specifically apply to that incident type. This allowed us to combine incident response performance results (pass or fail) for the mix of incident types.

Our audit team began data gathering by reviewing three USDA agencies – FS, RD, and RMA. At least one incident per category had to be selected for review. Category 5 included only two

[68]Originally the universe data consisted of 770 incidents which included OIG's IT security operations. OIG's operations, however, are reviewed by the Office of Compliance and Integrity (OCI). OCI performs independent quality assurance and internal control reviews of OIG operations. Therefore, we excluded the 3 OIG incidents from the 770 universe total. Hence, the projectable universe totals 767 incidents.

incidents; we purposefully selected both for review. We placed the remaining incidents in a stratum of their own and selected a simple random sample of those incidents for review. Once incidents data from the entire Department was available, we selected samples from those for review. Table 1, below, presents a summary of the sample design and incident counts per stratum.

Table 1: Sample design summary for Incident Response and Reporting

	Agency	*Stratum*	*Description*	*Universe*	*Sample*
Initial data review	RMA, RD, FS	I	A purposeful census stratum of 1 incident from RMA.	1	1
		II	SRS of incidents from all remaining agencies.	143	49
Final data review	Remaining Department agencies (OIG excluded)	III	A purposeful census stratum of 2 incidents from category 5.	2	2
		IV	SRS of incidents from all remaining categories.	621	49

Sample sizes for the random samples were based on:

- 95 percent confidence level,
- +/-10 percent precision in an attribute testing scenario,
- A universe size of 746 units in random strata, and
- An average expected error rate of 25 percent, based on historical information.

Results:

Results are projected to the audit universe of 767 incidents. Achieved precision, relative to the universe, is reflected by the confidence interval for a 95 percent confidence level. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.[69]

The audit team tested a variety of criteria: whether or not the incidents were reported to US-CERT within the required timeframe; whether or not the proper checklist was completed, and if not, was still accepted by the ASOC; whether or not the completed Incident Identification Form was completed in its entirety; whether or not the required incident category checklist was completed; if incidents were open for over 30 days without a POA&M being created; and if the incidents were resolved to minimize further damage.

We developed a projection based on the number of incidents found in our sample with at least one exception. We are reporting actual findings for the rest of the criteria tested.

[69] Scheaffer, Mendenhall, Ott, *Elementary Survey Sampling*, Seventh Edition, Duxbury Press, c1990.

Projections are shown in Table 2. The narrative interpretation of the results is presented below the table.

Table 2: Incident Response and Reporting Projections[70]

Criteria Tested	Estimate	Standard Error	95 Percent Confidence Interval		Coefficient of Variation	Achieved Precision[71]
			Lower	Upper		
Estimated number of incidents not reported to US-CERT within the required timeframe	20	5.856	9	32	0.287	2%
as a % of universe	3%	1%	1%	4%		
Estimated total number of incidents with at least one exception	58	21.439	16	101	0.367	6%
as a % of universe	8%	3%	2%	13%		

Based on our sample results, we estimate that:

- 20 incidents (about 3 percent of the universe) were not reported to US-CERT within the required timeframe. We are 95 percent confident that between 9 (about 1 percent) and 32 (about 4 percent) incidents have an exception in this criterion.
- 58 incidents (about 8 percent of the universe) were not handled in accordance with Departmental procedures. We are 95 percent confident that between 16 (2 percent) and 101 (13 percent) incidents had exceptions in one or more criteria tested.

2. Closed POA&Ms

Universe:
The audit universe consisted of 819 POA&Ms.

Sample Design:
We selected a simple random sample of 60 closed POA&Ms for review. We based our sample size on the following factors:

- 95 percent confidence level,
- +/- 10 percent precision in an attribute testing scenario,
- universe size of 819 units, and
- average expected error rate of 19 percent based on historical information.

[70] All percentages used in this table and tables below are rounded to the nearest whole number.
[71] Achieved precision is the difference between the estimate and the bounds divided by the size of the universe. For example: (32-20)/767 = 2 percent (rounded to the nearest whole number).

Results:
Results for all criteria are projected to the audit universe of 819 closed POA&Ms. Achieved precision relative to the audit universe is reported for each criterion. The corresponding lower and upper bounds of the 95 percent confidence interval are also included. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.[72]

Projections are shown in Table 3 below. The narrative interpretation of the results can be found below the table.

Table 3: POA&M (closed) Projections

Criteria Tested	Estimate	Standard Error	95 Percent Confidence Interval		Coefficient of Variation	Achieved Precision
			Lower	Upper		
Estimated number of POA&Ms that did not have effective remediation plans for correcting identified weakness	123	36.652	50	196	.298	9%
as a % of universe	15%	4%	6%	24%		

Based on our sample results, we estimate that 123 POA&Ms in our universe (about 15 percent of the universe) did not have effective remediation plans detailed in CSAM to correct identified weakness. We are 95 percent confident that between 50 (6 percent) and 196 (24 percent) POA&Ms in the audit universe are non-compliant with this criterion.

[72] Op. cit., Scheaffer et al.

3. System / Contingency Planning

Universe:
We worked with three separate universes of systems. One universe consisted of 246 FISMA reportable systems from a variety of agencies that were documented in CSAM as of August 6, 2015. The other two universes consisted of reportable systems in two agencies we reviewed – FS – 13 systems and RMA – 4 systems.

Each system is to have a contingency plan that contains very specific recovery information in the event of a disaster.

Sample Designs:
From the three universes mentioned above, we selected:

- A simple random sample of 61 from the 246 systems used by various USDA agencies
- A full review, i.e. a census of all 13 FS systems
- A full review, i.e. a census of all four RMA systems

The sample size for our simple random sample was based on:

- 95 percent confidence level,
- +/-10 percent precision in an attribute testing scenario,
- universe size of 246 units, and
- an expected error rate of 30 percent, based on historical information.

Results:
We are using projections derived only from the sample representing the combined agencies universe of 246 department systems. The rest of our report presents actual findings and contains no estimates. Based on our review of all systems from FS and RMA, we are reporting actual findings, not statistical projections for those agencies as well.

Results are projected to the audit universe of 246 systems. Achieved precision relative to the universe is reported for each criterion. The corresponding lower and upper bounds of the 95 percent confidence interval are also included. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.[73]

Projections are shown in Table 4. A narrative interpretation of the results is presented below the table.

[73] Ibid.

Table 4: System / Contingency Planning Projections

Criteria Tested	Estimate	Standard Error	95 Percent Confidence Interval		Coefficient of Variation	Achieved Precision
			Lower	Upper		
Estimate of the number of systems with no evidence of ongoing testing	125	13.769	97	153	.110	11%
as a % of universe	51%	6%	40%	62%		
Estimate of the number of systems with no evidence of after action	117	13.754	89	144	.118	11%
as a % of universe	48%	6%	36%	59%		

Based on our sample results, we estimate that:

- 125 systems (about 51 percent of the universe) did not have ongoing testing or did not provide documentation of testing. We are 95 percent confident that between 97 (40 percent) and 153 systems (62 percent) are noncompliant with this criterion.
- 117 systems (about 48 percent of the universe) did not have evidence of after action. We are 95 percent confident that between 89 (36 percent) and 144 systems (59 percent) are noncompliant with this criterion.

In addition, we found:

- No exceptions (0 errors) in our sample when we checked if systems had test, training and exercise programs in their contingency planning programs. Based on this finding, we are 95 percent confident that more than 95 percent of the systems in our universe are compliant in this criterion.
- One exception (1 error) where a system did not have an alternate site in a geographically different area and thus posed a risk to the agency. Based on this finding, we are 95 percent confident that more than 93 percent of all systems in the universe have an alternate site in a geographically different area.
- One exception (1 error) where contingency plans did not consider their vendors and supply chain. Based on this finding, we are 95 percent confident that more than 93 percent of all systems in the universe considered their vendors and supply chain in their contingency plan.

To learn more about OIG, visit our website at
www.usda.gov/oig/index.htm

How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse

File complaint online: http://www.usda.gov/oig/hotline.htm
Click on Submit a Complaint

Telephone: 800-424-9121
Fax: 202-690-2474

Bribes or Gratuities
202-720-7257 (24 hours a day)

The U.S. Department of Agriculture (USDA) prohibits discrimination in all of its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex (including gender identity and expression), marital status, familial status, parental status, religion, sexual orientation, political beliefs, genetic information, reprisal, or because all or part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD).

To file a complaint of discrimination, write to USDA, Assistant Secretary for Civil Rights, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue, SW., Stop 9410, Washington, D.C. 20250-9410, or call toll-free at (866) 632-9992 (English) or (800) 877-8339 (TDD) or (866) 377-8642 (English Federal-relay) or (800) 845-6136 (Spanish Federal-relay). USDA is an equal opportunity provider and employer.