USDA

United States Department of Agriculture

Office of Inspector General

USDA Office of the Chief Information Officer, Fiscal Year 2013 Federal Information Security Management Act

50501-0004-12

November 2013

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2013 Federal Information Security Management Act

Audit Report 50501-0004-12

What Were OIG's Objectives

Evaluate USDA's overall IT security program, compliance with FISMA, and effectiveness of controls over continuous monitoring, configuration management, identity and access management, incident response, assessments and authorizations, IT training, Plan of Action and Milestones, remote access management, contingency planning, contractor systems, and capital planning.

What OIG Reviewed

The scope was Department-wide and included agency IT audit work completed during FY 2013, other OIG audits completed throughout the year, and the results of reviews performed by contract auditors. This audit covered 11 agencies and staff offices, operating 159 of the Department's 246 major systems.

What OIG Recommends

The Department should continue its progress by issuing critical policy and completing actions on the 30 outstanding recommendations from the FY 2009 through 2012 FISMA audit reports and the 6 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 2013.

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 through 2012, OIG made 49 recommendations for improving the overall security of USDA's systems, but only 19 of these have been closed. We noted that the Office of the Chief Information Officer (OCIO) is taking positive steps to improve its security posture in the future. For example, OCIO released three key Departmentwide policies in the latter part of FY 2013 and the beginning of FY 2014. However, it is now critical that agencies create and implement agency-specific procedures based on Departmental policy. OCIO then needs to review the agencies' implemented procedures to ensure compliance with USDA policy. Once this process is institutionalized throughout USDA, its security posture should improve and be sustainable in the future.

Again this year, we continue to report a material weakness in USDA's IT security. The Department has not (1) developed policies, procedures or strategies for continuous monitoring or risk management; (2) monitored agencies for compliance with baseline configurations and ensured known vulnerabilities were fixed; (3) deleted separated employees' access to computer systems; (4) developed and implemented a policy to detect and remove unauthorized network connections; or (5) finalized and issued policy for information security oversight of systems that contractors or other entities operate on USDA's behalf, including systems and services residing in the cloud.

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

November 26, 2013

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

Dear Ms. Burwell:

Enclosed is a copy of our report, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2013 Federal Information Security Management Act* (Audit Report 50501-0004-12), 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

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2013 Federal Information Security Management Act

Findings and Recommendations

This report constitutes the Office of Inspector General's (OIG) independent evaluation of the Department of Agriculture's (USDA) Information Technology (IT) security program and practices, as required by the Federal Information Security Management Act (FISMA) of 2002, and is based on the questions provided by the Office of Management and Budget (OMB)/Department of Homeland Security (DHS). These questions are designed to assess the status of the Department's security posture during fiscal year (FY) 2013. The OMB/DHS framework requires OIG to audit processes, policies, and procedures that had already been implemented and documented, and were being monitored during FY 2013.

We noted that the Office of the Chief Information Officer (OCIO) is taking positive steps to improve its security posture into the future. OCIO released three critical Departmentwide policies in the latter part of FY 2013 and the beginning of FY 2014. However, because they were not in effect for most of FY 2013, we could not evaluate the effects of these policies. This is a positive first step that will improve IT security within USDA. The second and most critical step requires organizations to create agency-specific procedures based on Departmental policy. The third and final step is for OCIO to review the agencies' compliance to ensure OCIO policy is implemented. Once this three-step process is institutionalized throughout USDA, its security posture should improve and be sustainable in the future. The degree to which USDA, as a whole, complies with FISMA and other security guidance is based on individual agency performance. If each agency is in compliance with the Department's policies, then USDA as a whole will be FISMA compliant, and more secure. Also, USDA's National Information Technology Center became compliant with the Federal Risk and Authentication Management Program (FedRAMP) in June 2013, one year earlier than the mandatory date for being compliant.[1]

USDA is working to improve its IT security posture, but many longstanding weaknesses remain. We continue to find that the OCIO has not implemented corrective actions that the Department has committed to as part of the management decision process. In FYs 2009 through 2012, OIG made 49 recommendations for improving the overall security of USDA's systems, but only 19 of these have been closed. Of those 19 closed recommendations, our testing found 4 where weaknesses continue to exist.

As with compliance, USDA's security is only as good as the security of its individual agencies and staff offices. As part of our FY 2013 FISMA audit testing, we performed a vulnerability

[1] The FedRAMP program supports the U.S. Government's objective to enable U.S. Federal agencies to use managed service providers that enable cloud computing capabilities. OMB Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments* (December 8, 2011), established the FedRAMP compliance date. FedRAMP is designed to comply with FISMA.

assessment on seven agencies that were included in our 2008 through 2012 FISMA reviews to determine if each agency was mitigating its vulnerabilities in a timely manner and thus improving its security posture.[2] We compared the average number of vulnerabilities per device identified in our 2013 scans to the average number of vulnerabilities found during the previous FISMA reviews. For all seven agencies, the average number of vulnerabilities per device increased—in most cases the number doubled; and for three agencies, the number increased by over eight times. As a result of this, and the other findings in this report, IT continues to be a material weakness for the Department.

In addition to the agencies not following policies and procedures, we continue to find instances when OCIO itself does not comply with regulations. For example, OMB defines a major IT investment as "a system or acquisition requiring special management attention because of its importance to the mission or function of the agency, a component of the agency, or another organization." However, in our review of a sample of major IT investments within USDA, we found that an IT investment, which would provide email access and support for over 121,000 USDA email users via a cloud provider, was not considered major by the Department upon its inception in April 2010. The investment is being reclassified as a major IT investment for FY 2015. However, we believe it should have been considered a major IT investment from the start, since it was important to the mission and function of the Department and required special management attention. We also found that the Department did not document its rationale for not including it as a major investment. By not classifying it as a major investment in 2010, the Department did not record and report the information security resources required for the investment during the annual budgeting process for FYs 2011, 2012 and 2013.

In addition, we recommended in the FY 2012 FISMA audit that USDA modify the service agreement between the Department and the email cloud service provider to incorporate appropriate detail, outlining the roles and responsibilities of each party pertaining to incident response and reporting and to gain visibility into USDA's email system (i.e., so that the Department can view/monitor network traffic in the cloud system). FedRAMP requires agencies and cloud service providers to stipulate any specific incident reporting requirements, including how to notify the agency and who to notify. USDA's current cloud service providers are required to become FedRAMP compliant by June 2014. However, when the cloud email services contract was renegotiated and signed on September 30, 2013, we determined OCIO did not take advantage of its contract renegotiation period. OCIO did not include incident response and reporting responsibilities detailed in FedRAMP guidance, incorporate our recommendation to add adequate detail to address incident reporting roles and responsibilities or monitoring requirements to help safeguard USDA systems.

USDA is a large, complex organization that includes 34 separate agencies and staff offices, most with their own IT infrastructure. OCIO and the 33 other agencies need to be held accountable for implementing the Department's policies and procedures. If compliance by all agencies is

[2] 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.

attained, then FISMA testing results will be similar, regardless of which agency was selected and tested, and the Department's overall security posture would improve.

The following summarizes 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 systems and agencies,[3] OIG independent contractor audits, annual agency self-assessments, and various OIG audits throughout the year.[4] 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 has not established a continuous monitoring program. Specifically, we found that the Department has not issued a policy, strategies, or plans for continuous monitoring. Additionally, we found 72 of 246 systems where ongoing assessments of selected security controls had not been performed in FY 2013. In our FY 2010 FISMA report, OIG recommended that the Department develop policies, procedures, strategies, and implementation plans for continuous monitoring. The Department concurred and stated it would have a policy, procedures, strategy, and plans in place by September 30, 2011; however, the recommendation remains open.

The Department has established, and is maintaining, a security configuration management program; however, there are opportunities for improvement. Specifically, we found that the Department has established adequate policy, and has made standard baseline configurations available for all operating systems in use; however, agencies have not followed the policy or baselines when configuring servers and workstations. Specifically, one agency that OCIO is responsible for was not scanning over 83 percent of its devices on a monthly basis, while another agency was not scanning over 29 percent of its devices. We also found that all seven agencies we reviewed did not have a process for timely remediation of scan result deviations. For example, OIG used a commercially available vulnerability scan tool to test 7,104 devices within seven agencies to verify that vulnerabilities were mitigated timely. We found 25,813 high and medium vulnerabilities were present and not corrected; 13,489 of these were over 7 months old. In the FY 2010 FISMA audit, OIG recommended the Department ensure scanning for compliance to the baseline configurations and for vulnerabilities be performed, as required by the National Institute of Standards and Technology (NIST). This recommendation remains open; OCIO has exceeded its estimated implementation date of August 30, 2011. OCIO is currently working on deploying a Departmentwide vulnerability scanner.

The Department has established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines to identify users and

[3] One agency selected for FISMA review actually supports IT services for 12 other USDA agencies and offices.
[4] Agency annual self-assessments derive 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.

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 access, in accordance with Government standards.[5] Additionally, agencies were able to identify devices, users, and non-users who access the organization's systems and networks. Also, the Department is moving towards a centralized enterprise solution for access management which should provide a standardized system that automates network 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 ensure that accounts were terminated or deactivated once access was no longer required. For example, we found 66 separated users in the two agencies that still had active accounts. Departmental policy requires that accounts be disabled within 48 hours of an employee's separation. Further testing identified three agencies that did not mandate multi-factor authentication, as required.[6] In addition, three agencies that had implemented multi-factor authentication were not using the organization's PIV card, as required.[7]

The Department has established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. 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. Our review of 92 incidents disclosed that 24 incidents were not handled in accordance with Departmental procedures.[8] Of the 24 incidents identified, USDA did not report 20 of the incidents to the United States-Computer Emergency Response Team (US-CERT) within the required timeframe. Of these incidents, 13 were the result of a lost or stolen device. These incidents were not promptly reported to OCIO's Incident Management Division (IMD).[9] Additional testing determined USDA has procured the tools to correlate incidents across the Department but has not deployed them effectively. As a result, USDA does not have the ability to correlate incidents across its entire network infrastructure. Based on tests of USDA's cloud provider's traffic, discussions with USDA IT personnel, and our review of the cloud provider's service agreement and incident plan, we also determined that the Department is not capable of

[5] 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 contract personnel and employees 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.

[6] Dual-factor (or multi-factor) authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. Departmental Regulation (DR) 3505-003, *Access Control Policy* (August 11, 2009), requires the use of dual or multi-factor authentication.

[7] Multi-factor authentication can also utilize a hardware token or virtual token or a smart card (PIV), ("something the user has"), or a thumbprint or iris scanner ("something the user is"). HSPD-12 requires the use of the PIV card.

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

[9] The US-CERT provides response support and defense against cyber-attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. NCSD was established by DHS to serve as the Federal Government's cornerstone for cyber security coordination and preparedness.

managing risks in this virtual/cloud environment. USDA lacks the ability to track cloud traffic, the cloud service does not have its own Data Loss Prevention (DLP) solution deployed, and the service agreement between USDA and its cloud service provider does not include the appropriate provisions outlining the incident reporting roles and responsibilities for each party.[10]

We found that OCIO is in the beginning phases of planning for risk management framework (RMF). Specifically, the Department does not have a RMF that incorporates all of the FISMA requirements, OMB policy, and applicable NIST guidelines.[11] According to the Department, this was due to lack of resources for OCIO's governance team. Agency officials are responsible for ensuring all systems meet Federal and Departmental requirements and documenting agency compliance in the Cyber Security Assessment and Management (CSAM) system.[12] OCIO is also responsible for ensuring that agencies are compliant with Federal and Departmental guidance and reporting aggregate results during the annual FISMA reporting cycle. NIST transformed the assessment and authorization (A&A) process into a six-step RMF process.[13]

The Department issued a guide that addresses parts of the six-step RMF process. The guide also clarifies the steps necessary to complete the A&A process. This process requires agencies to submit their systems' A&A packages and all supporting documents to the Department for an in-depth review (i.e., a concurrency review). During this review, USDA ensures that the documentation prepared to support system accreditation is complete, accurate, reliable, and meets NIST and other mandated standards. Although the process has changed, we continue to find:

- USDA completed its in-depth document reviews and appropriately returned A&A packages that did not meet NIST requirements to the agencies. However, we found that improvements are still needed. Specifically, we found the following deficiencies in the A&A packages reviewed by OCIO: (1) systems were not properly categorized; (2) system security plan (SSP) controls were not implemented properly and did not

[10] DLP is the ability "to detect inappropriate transport of sensitive information and halt the traffic prior to leaving the network. Examples of sensitive content are personal identifiers (e.g. credit card or Social Security numbers) or corporate intellectual property."

[11] The 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 Special Publication (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).

[12] CSAM is a comprehensive system developed by the Department of Justice, which can facilitate 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 pre-defined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. This includes agency-owned systems as well as those operated by contractors on the agency's behalf.

[13] A&A is the new terminology for the former C&A process mandated by OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (November 28, 2000). The process requires that IT system controls be documented and tested by technical personnel and that the system be granted a formal authority to operate (ATO) by an agency official.

sufficiently address each control; and (3) security assessment reports (SAR) did not include an authorized security assessment plan (SAP).[14] As a result, USDA cannot be assured that all system controls were documented and tested, and that systems were operating at an acceptable level of risk.

- In order for a system to become operational, NIST 800-37 requires USDA agencies to follow the RMF process to obtain an authority to operate (ATO) and to effectively manage risk for their systems. In order for an ATO to be granted, systems are categorized, controls are identified and implemented, risk are assessed, and the final concurrency review is examined to proceed with accreditation. We found an OCIO parent system in the development stage with four child systems that were operational with no ATO.[15] The Department said these systems were needed for USDA operations and therefore would operate without an ATO for business reasons. We found another five systems that were operational with no ATO. Furthermore, the Department has 27 systems with expired ATOs, including CSAM, the Department's system repository. 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.

The Department has established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The Department's policy met all NIST requirements for annual security awareness training.[16] However, we identified opportunities for improvement. Specifically, USDA does not have policy and procedures to govern specialized security (role-based) training for personnel with significant information security responsibilities. NIST states that before allowing individuals access to the application, all individuals should receive specialized training focused on their responsibilities. The Department's new policy, which includes guidance for Specialized Security Awareness Training, was officially published on October 22, 2013.[17]

The Department has established a plan of action and milestones (POA&M) program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks

[14] The SSP is a required A&A document that 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 the responsibilities and expected behavior of all individuals who access the system. NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* (February 2006). The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the SAR.

[15] A parent system owns, manages, and/or controls the child system. This example is a general security system. It has multiple children beneath it that do various specific security functions, such as vulnerability scanning and network monitoring.

[16] NIST SP800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009).

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

and monitors known information security weaknesses.[18] However, our testing identified some deficiencies. For example, four agencies did not create POA&Ms for vulnerabilities existing for over 30 days as required by Departmental policy.[19] This occurred because the Department's security manual did not include a policy for establishing a POA&M process until September 25, 2013. In addition, our review of POA&Ms within CSAM found that agencies were not adequately detailing plans for remediation and were not including proper supporting documentation for effective closure. We found that 128 of the 869 POA&Ms that were closed during FY 2013 had remediation actions that did not sufficiently address the identified weakness. 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 and OMB policy. In addition, the Department is implementing an enterprise solution for remote access which should provide centralized management once fully implemented. However, our testing identified that Departmental policies for remote access and teleworking did not meet NIST requirements. Specifically, we found both agencies reviewed did not have a fully developed remote access policy or procedures. This occurred because the agencies either had a policy or procedures, but not both. In our FY 2010 FISMA report, we recommended that the Department update its policy and procedures to be NIST-compliant. This recommendation is still open and OCIO has exceeded its estimated completion date of August 31, 2011. We also found that while the Department and agencies were monitoring, detecting, and reporting unauthorized (rogue) network connections, there are no documented policies that require it. This occurred because the Departmental policy was still in draft and has not been issued. USDA requires multi-factor authentication for all remote access (i.e., two means of identification).[20] However, one of two agencies reviewed did not have it properly implemented. This occurred because, although the enterprise solution for two-factor authentication (LincPass) is implemented and available, it is not required and therefore not being used Departmentwide. Also, the agencies' inability to distribute the PIV cards limits their participation. Two other agencies were found through contractor audits or agency self-reports as not having implemented multi-factor authentication.

The Department has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, our testing identified opportunities for improvement. Specifically, Departmentwide, we found that 89 of 243 systems were not testing

[18] 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 corrective efforts for 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.

[19] DM 3530-001 requires a POA&M to be developed in accordance with Federal Information Security Management Act (FISMA) reporting requirements for any unresolved critical vulnerabilities existing for more than 30 days from the date of the scan.

[20] Multi-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other is typically something memorized, such as a security code. In this context, the two factors involved are sometimes referred to as "'something you have' and 'something you know.'"

contingency/disaster plans annually, as required by NIST and the Department.[21] We found the template provided to agencies for contingency planning purposes was updated, available to the agencies, and contained all of the NIST-required elements. In addition, during our detailed testing at two agencies, we found that all 20 of those plans were developed with the appropriate information required by NIST.

The Department does not have a program in place, a documented policy, or fully developed procedures to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud. OCIO has had a policy in draft for 4 years that is not yet finalized. Due to the lack of policies and procedures in the Department, we found one system was not included in the inventory of contractor systems. In addition, FISMA requires USDA to maintain an inventory of its information systems that, among other information, identifies interfaces between other agency systems. We reviewed documentation for 15 contractor systems in CSAM and, as noted above, found 5 systems with expired ATOs, insufficient interconnection documentation for 3 systems, and missing authorizing signatures for 14 systems.

Our testing of USDA's capital planning process determined the Department has established and maintains a capital planning and investment program for information security. However, testing determined that USDA does not maintain sufficient documentation to support its annual IT investment budgetary requests. Therefore, agencies could not support the amounts requested during the annual budgeting process.

The following recommendations are new for FY 2013. Because 30 recommendations from FY 2009 through 2012 have not been closed, we have not made any repeat recommendations. If the plans initiated to close out the FY 2009 through 2012 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

Require agencies to perform annual assessments of system security controls in accordance with RMF procedures.

Recommendation 2

Monitor agencies' workstations for United States Government Configuration Baseline (USGCB) compliance, servers for NIST baseline compliance, and verify that deviations are documented, approved, and on file with the Department.

Recommendation 3

Validate the system inventory, annually.

[21] Systems Inventory as of October 28, 2013. *USDA Contingency Plan Exercise Handbook,* Rev 1.1 (February 2011).

Recommendation 4

Develop and implement a policy to detect and remove unauthorized (rogue) network connections.

Recommendation 5

Finalize and issue policy for information security oversight of all systems that contractors or other entities operate on the organization's behalf, including systems and services residing in the cloud.

Recommendation 6

Document decisions regarding classification of IT investments in order to meet OMB standards.

Background & Objectives

Background

Improving the overall management and security of IT resources needs to be a top priority for USDA. Technology enhances users' abilities 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 into law the e-Government Act (Public Law 107-347), which includes Title III, FISMA. FISMA 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. NIST was tasked to work with agencies in developing standards as part of its statutory role in providing technical guidance to Federal agencies.

FISMA also supplements the information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996. The Act is consistent with existing information security guidance issued by OMB and NIST. More importantly, however, FISMA consolidated these separate requirements and guidance into an overall framework for managing information security. It established new annual reviews, independent evaluations, and reporting requirements to ensure agency compliance. It also provided for both OMB and Congressional oversight.

FISMA assigned specific responsibilities to OMB, agency heads, Chief Information Officers (CIO), and Inspectors General. OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. The responsibilities include the authority to approve agencies' information security programs. OMB also requires the submittal of an annual report to Congress summarizing the results of agencies' evaluations of their information security programs. Instructions for FY 2013 FISMA are outlined in the OMB M-14-04 *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* and DHS uses the website CyberScope to consolidate the reporting.

Each agency must establish a risk-based information security program that ensures information security is practiced throughout the lifecycle of each agency's system. Specifically, the agency's CIO must oversee this program, which, following OMB Memorandum 07-24, must include:

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems and data supporting critical operations and assets;

- development and implementation of risk-based, cost-effective policies and procedures to provide security protections for the agency's information;
- training that covers security responsibilities for information security personnel and security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of security policies, procedures, controls, and techniques;
- processes for identifying and remediating significant security deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- annual program reviews by agency officials.

In addition, FISMA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. 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 objective of this audit was 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 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, contractor systems and IT capital planning.

Scope and Methodology

The scope of our review was Departmentwide and included agency IT audit work completed during FY 2013. 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 remotely at USDA locations throughout the continental United States from December 2012 through November 2013. In addition, this report incorporates audits done throughout the year by OIG. 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 at eight additional USDA agencies. In total, our FY 2013 audit work covered 11 agencies and staff offices:

- Agricultural Research Service,
- Departmental Management,
- Foreign Agricultural Service,
- Food and Nutrition Service,
- Farm Service Agency,
- Food Safety and Inspection Service,
- National Agricultural Statistics Service,
- Natural Resources Conservation Service,
- Office of the Chief Financial Officer,
- OCIO, and
- Risk Management Agency.

These agencies and staff offices operate 159 of the Department's 246 general support and major application systems.

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 U.S. Government Accountability Office's (GAO) *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 the OMB Memorandum M-14_04 *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* and the DHS CyberScope FISMA Reporting Website.
- Evaluated the Department's progress in implementing recommendations to correct material weaknesses identified in prior OIG and GAO audit reports;

- Performed statistical sampling on 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 for compliance.

Abbreviations

A&A..... Assessment and Authorization
ARS..... Agricultural Research Service
ASOC..... Agriculture Security Operations Center
ATO ..... Authority to Operate
BIA..... Business Impact Analysis
C&A..... Certification and Accreditation
CIO..... Chief Information Officer
CIRT ..... Computer Incident Response Team
CISO ..... Chief Information Security Office
CPIC..... Capital Planning and Investment Control
CPD..... Capital Planning Division
CPO..... Cyber Policy Oversight
CSAM ..... Cyber Security Assessment and Management
DHS..... Department of Homeland Security
DLP ..... Data Loss Prevention
DM ..... Departmental Manual
DoD..... Department of Defense
DR..... Departmental Regulation
FCIC..... Federal Crop Insurance Corporation
FDCC ..... Federal Desktop Core Configurations
FedRAMP ..... Federal Risk and Authorization Management Program
FISMA ..... Federal Information Security Management Act
FS ..... Forest Service
FY ..... Fiscal Year
GAO..... Government Accountability Office
GISRA..... Government Information Security Reform Act
HSPD-12..... Homeland Security Presidential Directive-12
IMD..... Incident Management Division
IP ..... Internet Protocol
ISCM..... Information Security Continuous Monitoring
IT..... Information Technology
ITS..... International Technology Services
MOU ..... Memorandum of Understanding
NCSD..... National Cyber Security Division
NIST..... National Institute of Standards and Technology
NITC ..... National Information Technology Center
OCIO..... Office of the Chief Information Officer
OIG ..... Office of Inspector General
OMB ..... Office of Management and Budget
PIV ..... Personal Identification Verification
POA&M..... Plan of Action and Milestone
RMF ..... Risk Management Framework
SAP ..... Security Assessment Plan
SAR..... Security Assessment Report

SOP ..... Standard Operating Procedure
SP ..... Special Publication
SSP ..... System Security Plan
TT&E ..... Test, Training, and Exercise
USGCB ..... United States Government Configuration Baseline
US-CERT ..... US-Computer Emergency Response Team
USDA ..... Department of Agriculture

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. OIG checks items on OMB/DHS' list, boldfacing and underlining the relevant text. We answer direct questions with either Yes or No.

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.[22] 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 11 FISMA areas. We incorporated statistical sampling into four FISMA areas. Each of the four areas was represented by the relevant universe associated with it. The specific sample designs are summarized in Exhibit B.

S1: Continuous Monitoring Management

1.1 Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems 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?

1.1.1 Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7). - No

The Department has developed the risk management framework (RMF) guidance and is currently working on a Departmental Regulation (DR) policy entitled *Security Assessment and Authorization* in regards to continuous monitoring. However, this DR is still in draft and has not been implemented. Both the RMF and draft DR are pieces of the continuous monitoring strategy, but there is no over-arching continuous monitoring policy or procedures within the Department. We also identified one of two agencies reviewed that did not have an agency policy in place.[23]

[22] Agency annual self-assessments are a result of 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.

[23] NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009). CA-7 requires the organization to establish a continuous monitoring strategy and program.

1.1.2 Documented strategy and plans for continuous monitoring (NIST SP 800-37 Rev 1, Appendix G). - No

The Department provided a strategy for developing an enterprise-wide continuous monitoring plan. However, this strategy was in draft and has not been implemented. OCIO also provided OIG with the *USDA Information Security Continuous Monitoring Program Charter*. This document contains objectives and milestones that OCIO would like to achieve in order to improve continuous monitoring within agencies and the Department. Additionally, the Department has a variety of continuous monitoring tools that have helped benefit its security posture. For example, the Department has a network tool, and although not fully operational, it was actively monitoring for malicious activity within the USDA network.[24] One agency we reviewed met with the Agriculture Security Operations Center (ASOC) on a regular basis to discuss the security incidents found with this tool. Furthermore, USDA has been actively using another tool to help standardize and centralize the governance workstations and servers.

1.1.3 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, NIST 800-53A). - No

We identified 72 of 246 systems where ongoing assessments of selected security controls had not been performed in FY 2013.[25] The agencies that own these systems cannot ensure that controls remain effective over time, as changes occur in threats, missions, environments of operation, and technologies.

1.1.4 Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). - No

We found that one of two agencies was unable to verify that the required information was provided to the authorizing official or other key system officials.

In the FY 2010 FISMA report, we recommended that the Department ensure system authorizing officials and other key system officials are provided with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions. The recommendation remains open and exceeded the estimated completion date of September 30, 2011.

[24] When a sensor is not inline, traffic does not flow through the sensor. The sensor instead analyzes a copy of the monitored traffic. The advantage of operating this way is that the sensor does not affect network performance. The disadvantage of operating in this mode, however, is the sensor cannot actively stop malicious traffic from reaching its intended target. The response actions implemented by the sensor devices are post-event responses.
[25] The 246 major applications were reported in CSAM as of October 21, 2013.

1.2 Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.

No additional information to provide.

S2: 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

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. - Yes

No exception noted. NIST requires that the organization develop formal documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.[26] OIG found the configuration management program includes adequate documented policies and procedures at both the Department and agency level.

2.1.2 Defined standard baseline configurations. - Yes

No exception noted. The Department follows the NIST configuration baseline guides.[27]

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 that two of two agencies reviewed did not configure servers in accordance with the NIST requirements. Specifically, we found that over 89 percent of the settings on the Windows servers at both agencies were not compliant with the baseline guides provided by NIST. In addition, two other agencies 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 those settings not implemented. OCIO has exceeded its 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

[26] NIST SP 800-53 Rev. 3, control CM-1 requires that a formal documented configuration management policy and procedures be developed.
[27] NIST SP 800-70 Rev. 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers Recommendations* (February 2011).

should be documented and approved. OCIO has exceeded its estimated completion date of September 30, 2011.

2.1.4 Process for timely, as specified in organization policy or standards, remediation of scan result deviations. - No

We found that seven of seven agencies reviewed did not have a process for timely remediation of scan result deviations.[28] Specifically, OIG used a commercially available vulnerability scan tool to test 7,104 devices within seven agencies to verify that vulnerabilities were managed timely. We found 25,813 high and medium vulnerabilities were present and not corrected; 13,489 of these were over 7 months old. As a result, networks and devices within the Department are at increased risk of being compromised.

2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented. - No

NIST requires the organization to establish and document mandatory security configuration settings for information technology products employed within the information system. Two such requirements are the Federal Desktop Core Configurations (FDCC) secure configurations for user workstations and laptops[29] and the United States Government Configuration Baseline (USGCB) which evolved from the FDCC mandate to provide guidance to agencies on what should be done to improve and maintain effective configuration settings, focusing primarily on security. We found that two of two agencies reviewed did not fully implement FDCC/USGCB secure configuration settings and document all deviations from baseline settings. Specifically, in the agencies tested we found a total of 537,112 FDCC/USGCB settings that should have been implemented; however, 195,481 (36 percent) of the settings were not in compliance with those standards. These missing standards make the laptops and workstations less secure and users more susceptible to compromise.

In the FY 2009 FISMA report, OIG recommended the Department complete the FDCC deployment and ensure all FDCC deviations are documented by the agencies. Final action has been achieved; however, this problem continues.

2.1.6 Documented proposed or actual changes to hardware and software configurations. - No

NIST requires the organization to document approved configuration-controlled changes to the system. Our review did not identify any issues with documented proposed or actual changes to

[28] A vulnerability scan is the process of determining the presence of known vulnerabilities by evaluating the target system over the network. Departmental Manual (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.

[29] OMB Memorandum 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.

hardware and software configurations. However, the A-123 self-inspection identified three of eight agencies self-reported deficiencies with configuration change control testing.

2.1.7 Process for timely and secure installation of software patches. - 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.[30] We found five of seven agencies reviewed did not have an implemented process for the timely and secure installation of software patches. Specifically, OIG found 293 high and medium vulnerabilities where the corrective action was to apply a vendor issued patch; in 271 of the 293 instances, patches were available for at least 7 months but the agency had not installed them.

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 completion date of June 15, 2011.

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). - No

DM 3530-001 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 a result of the scans. We found two of two agencies reviewed did not implement scanning capabilities, as required. Specifically, one agency was not scanning 1,275 of 1,530 devices monthly (83.33 percent).

In the FY 2009 FISMA report, OIG recommended that the Department develop and implement an effective monthly FISMA scorecard to be used for agency reporting and Departmental oversight. We also recommended that USDA ensure that the scorecard includes verifiable items such as vulnerability scanning, patching, anti-virus reports, and training. Final action has been achieved, but this problem continues. In the FY 2010 FISMA report, OIG recommended that the Department ensure scanning is performed as required by NIST for compliance with the baseline configurations and for vulnerabilities. This recommendation is open and has exceeded the estimated completion date of September 30, 2011. OCIO is currently working on deploying a Departmentwide vulnerability scanner.

In addition, OIG recommended in the FY 2011 FISMA report that the Department develop monitoring procedures to verify that monthly vulnerability scans are completed as required by Departmental guidance. Management decision has not been reached.

[30] 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.

2.1.9 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 two of two agencies reviewed did not remediate configuration vulnerabilities. Specifically, we found 733 configuration-related vulnerabilities on 646 network devices.[31] In addition, we found 6,089 configuration-related vulnerabilities on 6 websites maintained by the agencies.[32] Consequently, the devices and websites are at risk for compromise.

In the FY 2011 FISMA report, OIG recommended the Department develop monitoring procedures to verify that all Department and agency network devices are configured in accordance with NIST. Management decision has been reached with an estimated completion date of September 30, 2013.

2.1.10 Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2). - No

NIST requires Federal agencies to incorporate vendor software flaw remediation (patches) into the organizational configuration management process. We found that four of four agencies reviewed did not have a fully developed patch management process. Specifically, as noted in our response to question 2.1.7, we found 271 of 293 high and medium vulnerabilities were present on USDA devices where the patches were available for 7 months or more, but the agencies had not applied them. As a result, USDA devices are susceptible to compromise.

2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

No additional information to provide.

S3: 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?

[31] We utilized a commercially available software package designed to test security and configuration policies to analyze agency network devices for compliance with FISMA requirements.
[32] We utilized a commercially available software package designed to thoroughly analyze web applications and web services (websites) for security vulnerabilities.

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 is substantially compliant and procedures at the two agencies we reviewed met NIST SP 800-53.

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

We found that one of the two agencies reviewed did not identify all users, including Federal employees, contractors, and others who access USDA systems. Additionally, one agency self-reported deficiencies in this area. For example, one agency does not segregate Federal employees, contractors, and others who access the organization systems in its user access management database. However, the agency stated this was a priority to address in FY 2014, as they move to the Department's new enterprise user access management database system. The other agency reported that a system it owned did not distinguish between guest and temporary accounts and they could not be properly identified with the incomplete user account attribute data available.

3.1.3 Identifies when special access requirements (e.g., multifactor authentication) are necessary. - No

Currently, the Department requires agencies to implement multi-factor authentication for all forms of remote access to agency information systems.[33] However, we found one of two agencies reviewed by OIG did not have multi-factor authentication properly implemented. Additionally, two agencies self-reported deficiencies in this area. One agency reviewed was using the Departmental LincPass system for remote access; however, users were still able to use their username and password to perform authentication remotely.

3.1.4 If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800- 53, IA-2). - No

We found that one of two agencies reviewed by OIG did not use multi-factor authentication linked to the Department's Personal Identification Verification (PIV) credentials program.[34] In addition, two agencies self-reported deficiencies in this area. One agency was using the PIV cards for remote access; however, users were still able to use their username and password to perform authentication remotely. Inadequate security controls over special access requirements could result in the unauthorized access, use, disclosure, modification, or destruction of information.

---

[33] Departmental Regulation (DR) 3505-003, *Access Control Policy* (August 11, 2009). Multi-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as "something you have" and "something you know."

[34] 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 contract personnel and employees 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.

3.1.5 Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). - No

We found that one of two agencies reviewed did not use PIV cards for logical access in accordance with Government policies. This occurred because the agency was not able to provide evidence that supported that it had a plan for PIV card implementation.

3.1.6 Organization has adequately 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). - No

OIG found that one of two agencies was unable to provide evidence of adequate planning.

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

OIG testing found no exceptions in granting access based on needs and separation-of-duties in the agencies we reviewed. However, three agencies were reported in contractor reviews and two agencies self-reported deficiencies in this area. As a result, accounts have excessive privileges which may result in the unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

3.1.8 Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts). - Yes

No exception noted. OIG found that all agencies reviewed were able to provide evidence that their Identity and Access Management program identified devices with Internet Protocol (IP) addresses that are attached to the network.

3.1.9 Identifies all user and non-user accounts (Refers to user accounts that are on a system). Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.) - Yes

No exception noted. OIG found that all agencies reviewed were able to identify user and non-user accounts.

3.1.10 Ensures that accounts are terminated or deactivated once access is no longer required. - No

OIG found that two of the two agencies reviewed did not ensure that accounts were terminated or deactivated once access was no longer required. In addition, three of seven agencies were also reported in contractor reviews as not terminating or deactivating accounts once access was no

longer required. Additionally, three of eight agencies self-reported deficiencies in this area. For example, we found 66 separated users in the two agencies that still had active accounts. This occurred because the agencies reviewed used a manual process to determine which accounts to terminate, leaving the process prone to errors. This process is also not considered a timely way of tracking and reporting separated employees. Departmental policy states that accounts should be disabled within 48 hours of an employee's separation. The agencies are not properly terminating users when access is no longer required, which may result in the unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

3.1.11 Identifies and controls use of shared accounts. - Yes

No exception noted. OIG determined that all agencies reviewed, identified, and controlled 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 to provide.

S4: 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 Departmental policy and procedures met all of the NIST requirements.[35] However, our review of two agencies found that one agency had not developed procedures and the other agency had procedures, but they were not current.

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

Our review found that 24 of 92 incidents were not handled in accordance with Departmental procedures.[36] Based on our overall sample results we estimate that 530 incidents (26 percent of

[35] NIST SP 800-61, *Computer Security Incident Handling Guide* (March 2008).

[36] We based our sample size on a 40 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 92 incidents for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

the universe) were not handled in accordance with Departmental procedures.[37] For example, agencies are required to submit documentation to the Department, detailing the steps taken to close out the incident. Specific documents and completed forms are required to be returned to the Department; however, we found that 5 of the 24 incidents had either incomplete incident documentation or did not include the required documentation outlined in the procedures. For example, four incidents did not complete the required incident identification form.

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). - No

The US-Computer Emergency Response Team (US-CERT) requires USDA to notify it of incidents within specified timeframes, based on the category of the incident.[38] We reviewed a statistical sample of incidents that disclosed USDA had not reported 20 of 92 incidents to US-CERT within the required timeframe, 13 of which were the result of a lost or stolen device that were not promptly reported to OCIO's Incident Management Division (IMD).[39] Based on our overall sample results, we estimate that 460 incidents (22.4 percent of the universe), were not reported to US-CERT as required.[40] For example, US-CERT requires actual or potential PII incidents to be reported within one hour, which includes lost or stolen equipment; however, we found that an agency did not report a lost equipment incident to IMD (to forward to US-CERT) for 26 days.[41] Additionally, we found one lost equipment incident that was not reported to US-CERT at all. ASOC was unable to verify if US-CERT was notified of this incident.

4.1.4 When applicable, reports to law enforcement within established timeframes (NIST SP 800-61). - No

We found 1 of 4 (25 percent) of tested incidents were not reported to law enforcement 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, and OMB M-07-16, M-06-19). - Yes

No exception noted.

---

[37] We are 95 percent confident that between 344 (17 percent of the universe) and 716 (35 percent of the universe) FY incidents were not handled in accordance with Departmental procedures. Additional sample design information is presented in Exhibit B.

[38] US-CERT provides response support and defense against cyber-attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners. US-CERT is the operational arm of NCSD at DHS. NCSD was established by DHS to serve as the Federal Government's cornerstone for cyber security coordination and preparedness.

[39] We based our sample size on a 40 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 92 incidents for review and selected them by choosing a stratified sample. Additional sample design information is presented in Exhibit B.

[40] We are 95 percent confident that between 283 (13.8 percent of the universe) and 637 (31 percent of the universe) incidents in FY were not reported to US-CERT as required. Additional sample design information is presented in Exhibit B.

[41] Lost equipment is defined as a lost or stolen laptop, smartphone, or other electronic device that is issued to USDA employees for performance of the employees' day-to-day responsibilities.

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. - No

We conducted testing to determine if USDA is capable of tracking and managing risks in a virtual/cloud environment. Based on the test traffic we sent to and received from the cloud provider, discussions with USDA IT personnel, and our review of the cloud provider's agreements and incident plan, we determined that USDA is not capable of managing risks in a virtual/cloud environment.[42] USDA lacks the ability to track cloud traffic, the cloud email solution does not have a deployed Data Loss Prevention (DLP) solution, and the service agreement between USDA and its cloud service provider does not include the appropriate detail outlining the roles and responsibilities for each party.[43]

In the FY 2012 FISMA audit, we recommended that USDA modify the service agreement between the Department and the email cloud service provider to incorporate appropriate detail, outlining the roles and responsibilities of each party pertaining to incident response and reporting. Additionally, the Department should work with the cloud provider to gain visibility into USDA's email system (i.e., so that the Department can view/monitor network traffic in the cloud system). Also, a Federal initiative, the Federal Risk and Authorization Management Program (FedRAMP), effective June 2014, requires agencies and cloud service providers to stipulate any specific incident reporting requirements, including who to notify and how to notify the agency.[44] USDA's current cloud service providers are required to become compliant by June 2014.

Although our review was conducted prior to the June 2014 deadline, the cloud email services contract was renegotiated and signed on September 30, 2013. We determined USDA did not take advantage of its contract renegotiation period to include adequate detail within the contract to address incident reporting roles and responsibilities, nor did it include monitoring requirements to help safeguard USDA systems.

4.1.7 Is capable of correlating incidents. - No

Based on our testing, we determined that, although the Department has the capability to monitor and correlate incidents for the incident response and reporting within USDA, the current security tools do not see nor capture all network traffic.

---

[42] The test traffic generated was an email message that was sent from a USDA cloud-based email account to a test Google email account (Gmail). The e-mail message contained an unencrypted spreadsheet that included 50 fictitious names, fictitious social security numbers, and fictitious credit card numbers. When the e-mail was sent, it was sent to the Cloud Service Provider through the USDA network and subsequently received by the Gmail account from the Cloud Service Provider.

[43] DLP is the ability "to detect inappropriate transport of sensitive information. Examples of sensitive content are personal identifiers (e.g. credit card or social security numbers) or corporate intellectual property."

[44] The FedRAMP program supports the U.S. Government's objective to enable U.S. Federal agencies to use managed service providers that enable cloud computing capabilities. The program is designed to comply with FISMA.

In the FISMA 2011 and 2012 reports, OIG recommended the Department deploy adequate resources to monitor and configure new security tools and then adequately report and close the related incidents. Management decision has not been reached on the FY 2011 recommendation, but has been reached on the FY 2012 recommendation, with an estimated completion date of September 30, 2013.

4.1.8 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. Our review of the Department's incident monitoring and detection coverage determined that it has sufficient incident detection and monitoring coverage.

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.

S5: 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 Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. - No

The Department does not have a finalized risk management policy. The Department does have procedures, but it lacks some required elements. For example, the procedures are missing guidance for an authorization termination date. This date is established by the authorizing official to indicate when the security authorization expires.[45] The Department is in the process of making revisions and addressing missing requirements and enhancements to the procedures. Without a policy, the Department does not have a consistent and effective approach to risk management that is applied to all risk management processes and procedures.

In the FISMA 2011 report, OIG recommended the Department develop a risk management policy and associated procedures that fully comply with NIST. Management decision has been reached with an estimated completion date of September 30, 2013.

[45] USDA *Six Step Risk Management Framework Process Guide* (July 2011). NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010), states that organizational officials must identify the resources necessary to complete the risk management tasks described in this publication and ensure that those resources are made available to appropriate personnel.

5.1.2 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 not developed an organization-wide risk management strategy that addresses risk from an organizational perspective. According to OCIO officials, funding was reduced for the team responsible for the development and implementation of the governance project, which included the RMF strategy.

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

As noted in questions 5.1.1 and 5.1.2, the Department does not have a policy, adequate procedures, a governance structure, or 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.

5.1.4 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 questions 5.1.1 and 5.1.2, the Department does not have policies, adequate procedures, 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.

5.1.5 Has an up-to-date system inventory. - No

The Department does not have an up-to-date system inventory. We found a contractor system not recorded in the Cyber Security Assessment and Management (CSAM) system.[46] In addition, the required system inventory reconciliation was not completed this year because the system that was used in previous reconciliations was retired.[47] Currently, there is not a way for USDA to ensure that all systems are recorded in CSAM and that USDA has an accurate inventory.

[46] 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.

[47] FISMA requires an inventory to be kept and maintained at least annually.

5.1.6 Categorizes information systems in accordance with government policies. - No

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, and low.[48] If any one of the impact levels are high, for instance, then the system must be categorized as a high system. We compared the generated report to the recommended categorization levels in NIST and found 18 of 233 systems were not properly categorized.[49] These systems had a lower categorization rating than was recommended, without adequate justification.[50] NIST requires that any adjustments to the recommended impact levels be documented and include justification for the adjustment.

5.1.7 Selects an appropriately tailored set of baseline security controls. - No

NIST SP 800-53 recommends a set of minimum baseline security controls to be implemented based on a system's overall categorization. The lower the category, the fewer required controls. Therefore, the incorrect categorization noted in 5.1.6 led to inadequate controls being implemented for those 18 systems. NIST SP 800-60 states that an incorrect information system impact analysis can result in the agency either overprotecting the information system (thereby wasting valuable security resources), or under-protecting the information system and placing important operations and assets at risk.

5.1.8 Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. - No

As noted in 5.1.6, the incorrect categorization noted in 5.1.7 led to inadequate controls being implemented for those 18 systems.

5.1.9 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. - No

We found that security controls were not implemented correctly. Specifically, systems' security controls did not include sufficient support for implementation. For example, for 15 of 15 systems reviewed, the controls involving security awareness training, incident response, or program management were described as inherited. However, these controls could not be inherited. The Department requires the agencies to develop specific procedures on how the organization will implement these types of controls.

---

[48] 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.
[49] Systems inventory as of September 3, 2013.
[50] NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories, Vol. 1* (August 2008).

5.1.10 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 5 systems operational with no authority to operate (ATO), and 27 systems with expired ATOs that were operational. We also found a parent system identified as being in development, but the system had four child systems that were operational without ATO's.[51] This occurred because the Department felt that the systems needed to be operational for business needs.

In the FY 2009 FISMA report, OIG recommended that the Department develop and implement an effective certification & accreditation (C&A) process based on NIST guidance and ensure that all systems have the proper ATO.[52] This recommendation reached final action; however, we found that the same issue still exists.

5.1.11 Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. - No

NIST SP 800-53 states that the organization will assess the security controls in an information system as part of the testing/evaluation process. However, as noted in 1.1.3, we identified 72 of 246 systems where ongoing assessments of selected security controls had not been performed in FY 2013.[53]

5.1.12 Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization. - No

As noted in 5.1.1-5.1.4, the Department does not have policies, adequate procedures, a governance structure, or an organizational risk management strategy with defined risks in place. Therefore, we were unable to determine if the information-system-specific risks were communicated to appropriate levels of the organization.

[51] Total number of systems generated out of CSAM as of September 3, 2013.
[52] The assessment & authorization (A&A) is the new terminology for the former certification and accreditation process mandated by OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (November 28, 2000). The process requires that IT system controls be documented and tested by technical personnel and that the system be given formal ATO by an agency official.
[53] Systems Inventory as of October 21, 2013.

5.1.13 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). - Yes

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

5.1.14 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 RMF guide prescribes the active involvement of appropriate personnel.

5.1.15 Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (NIST SP 800-18, 800-37). - No

The system security plans (SSP) we reviewed were inadequate and not in accordance with Government policies.[54] We found 15 of 15 SSPs did not meet the minimum security requirements required by NIST SP 800-53. Specifically, these systems' security controls did not include sufficient support for implementation. For instance, we found controls that had not been assessed and the agencies did not have evidence to support why the controls were not assessed.

We also reviewed 15 of the Department's security assessment reports (SARs) and found that all did not meet the minimum security required by NIST SP 800-37.[55] Specifically, NIST SP 800-37 requires a security assessment plan (SAP) to be included with the SAR, which provides the objectives for the security control assessment, a detailed roadmap of how to conduct the assessment. We found during our review three of the three SAPs that had fully completed the assessment & authorization (A&A) process had not been approved or authorized. As a result, USDA cannot be assured that all system controls had been documented and tested, and that systems were operating at an acceptable level of risk.

As noted in 7.1.6 USDA, POA&Ms did not meet Federal guidelines.

5.1.16 Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems. - No

During our review of SSP's we verified that system accreditation boundaries were accurately defined in accordance with Government policies. We found 4 of 15 systems did not adequately

[54] NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* (February 2006), requires the SSP as part of the A&A 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.

[55] The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the SAR.

define and/or explain the system boundaries. Unclear boundaries can lead to confusion over responsibility for system components.

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.

S6: 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). - Yes

We determined the Department and two of the two reviewed agencies' security awareness policies and procedures met all the requirements outlined in NIST SP 800-53 for FY 2013. [56]

In the FY 2011 FISMA report, OIG recommended that the Department develop monitoring procedures to appropriately report the status of USDA employees being trained to meet their information security awareness needs. This recommendation reached management decision, but has exceeded the estimated completion date of September 30, 2013.

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

The Department's policy for specialized security training was not fully developed. In addition, the Department's specialized security training procedures and the procedures for two of two agencies reviewed were not effective, fully developed, or sufficiently detailed.[57] Specifically, we found the Department's policy for specialized training did not include a definition of significant information security responsibilities.

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

[57] 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.

In the FY 2009 FISMA report, OIG recommended that the Department develop training policies and procedures for personnel with significant security responsibilities, to include a Departmental definition of what constitutes significant security responsibilities. The recommendation reached management decision but the policy and procedures exceeded the estimated published date of September 30, 2011. The Department's new policy, which includes guidance for specialized security awareness training, was officially published on October 22, 2013.[58]

6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards. - Yes

No exception noted. OIG reviewed the training content for individuals of the two sampled agencies with significant information security responsibilities. All 58 reviewed employees had training that was documented and was appropriate for role-based training.

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. - Yes

No substantial 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 3 of 9755 users (less than 1 percent) with login privileges without evidence that the users had completed the annual security awareness training. We consider the Department to have substantially met the requirements.

Although these two agencies have substantially met the requirements, there is still an open recommendation. 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. This recommendation is still open and has exceeded the estimated completion date of August 30, 2011.

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. - Yes

No substantial 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 of the two sampled agencies. Our testing of 58 employees with significant security responsibilities found all 58 employees from the two sampled agencies had adequate role-based training to meet NIST requirements and had documented evidence of specialized training attendance. The contractor review identified one of eight agencies that had an issue with the identification and tracking of the status of specialized training for all personnel with significant information security responsibilities that

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

required specialized training. We consider the Department to have substantially met the 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 does contain the appropriate content to meet NIST SP 800-53.

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.

S7: Plan Of Action & Milestones (POA&M)

7.1 Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? - 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. - No

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; however, this document was not finalized until September 25, 2013, and was not in effect as guidance for the agencies to follow during FY 2013. We reviewed this document and found it to include all required elements.

Additionally, the Department has established procedures. Our review of the POA&M SOP determined it was updated to include OMB-outlined criteria,[59] and that it reflected the current POA&M process.[60] However, we found one of two agencies reviewed did not have established POA&M procedures for managing IT security weaknesses discovered during security control assessments that required remediation.

7.1.2 Tracks, prioritizes and remediates weaknesses. - No

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

We found the Department's POA&M program tracks weaknesses. However, we identified 42 of 677 open and approved POA&Ms as of September 25, 2013, that did not have an identified priority level. Additional testing by contractors identified one of six agencies did not have a POA&M program that tracks, prioritizes, and remediates weaknesses. 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 04-25 specifies that effective remediation of IT security weaknesses is essential to achieve a mature and sound IT security program, and for securing 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 68 POA&Ms that were closed during FY 2013, and found 10 were closed without documented remediation plans.[61] Based on our sample results, we estimate 128 POA&Ms (15 percent of the universe) were closed in FY 2013 with remediation actions that did not sufficiently address the identified weaknesses in accordance with Government policies.[62] Additionally, of the POA&M closures reviewed by the Department, 12 of 163 closures were not acceptable, due to insufficient documentation to support remediation, or closure procedures were not followed.

7.1.4 Establishes and adheres to milestone remediation dates. - No

We found that 597 of the 2,806 (21 percent) milestones completed in FY 2013 were not completed by the planned milestone finish date. This is down from 28 percent in FY 2012. We found that milestone dates are being established, but the remediation dates are not always adhered to. Additional testing by contractors identified one of six agencies did not have a POA&M program, which establishes and adheres to milestone remediation dates.

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

We found weaknesses that were not being remediated due to inadequate resources. We identified 261 delayed POA&Ms as of August 28, 2013. We determined 132 of the 261 POA&Ms were delayed due to inadequate resources. Additionally, 32 POA&Ms were delayed without providing an explanation. We also found that ownership was not assigned for 44 of 763 open POA&Ms as of August 1, 2013. Additional work by contractors identified one of three agencies did not have a POA&M program that ensures resources and ownership are provided for correcting weaknesses.

[61] We based our sample size on a 25 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 68 POA&Ms for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

[62] We are 95 percent confident that between 56 (6.4 percent) and 200 (23 percent) of closed POA&Ms in the FY 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.

7.1.6 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 found. 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 four agencies that were not creating POA&Ms for vulnerabilities that were outstanding for over 30 days.

7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25). - Yes

No exception noted. OMB requires that POA&Ms include the estimated funding resources required to resolve the weakness. We found 42 of 763 (5.5 percent) POA&Ms that did not have associated costs. The Department has made significant progress since FY 2011 when we found that 38 percent of the POA&Ms did not have associated costs. Therefore we consider the error rate in FY 2013 to be insignificant.

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, Rev. 3, Control CA-5; OMB M-04-25). - Yes

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 for OCIO to track and review POA&Ms at least quarterly. However, there is still room for improvement in the tracking and reviewing of audit POA&Ms. The Department's SOP requires that all closed POA&Ms resulting from a GAO or OIG audit are subject to the Department's closure review process. We identified 11 closed audit POA&Ms that had not been reviewed by OCIO.

In the FY 2011 FISMA report, OIG recommended that the Department actively manage the POA&M process, which includes tracking and reviewing POA&Ms in accordance with its recently issued SOP. The recommendation is open with management decision.

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.

S8: 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, our testing found it did not meet all NIST requirements. [63] There were two policy areas that were not addressed in the Departmental policy as outlined by NIST. One area was the administration of remote access servers and the other was the periodic reassessment of the telework device policies. Additionally, we found two of two agencies reviewed did not have a remote access policy or procedures fully developed. This occurred because the agencies either had a policy, or procedures, but not both. As a result, inadequate security of remote access could result in the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

In the FY 2010 FISMA report, we recommended the Department develop remote access and telework policy and procedures that fully comply with NIST. The recommendation is still open; OCIO has exceeded the estimated completion date of August 31, 2011.

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

No exception noted. We found two of two agencies reviewed 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). - No

We found one of two agencies reviewed was not using multi-factor authentication (which uniquely identifies and authenticates remote users) for remote access as required. This occurred because while the enterprise solution for two-factor authentication (LincPass) is implemented and available, it is not required and therefore not being used Departmentwide (see 8.1.5 below). We also found the telework policy was insufficient (see 8.1.6 below). In addition, one contract audit found and one agency self-reported not having two-factor authentication for remote access properly implemented.

[63] NIST SP 800-46 Rev. 1, *Guide to Enterprise Telework and Remote Access Security* (June 2009).

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

As reported in item 8.1.1 above, the Department has a remote access (and telework) policy but our testing found it did not meet all NIST requirements. It establishes the telework program for the agency and outlines parts of the program like the types of telework agreements, eligibility, exclusions, etc. However, the information security section does not provide detailed policy guidance for securing the equipment, work products, and software while teleworking. Specifically we found two of two agencies reviewed did not have a fully developed telecommuting policy. This occurred because the agency depended on the Departmental policy, which had deficiencies.

In the FY 2010 FISMA report, we recommended that the Department develop a remote access and telecommuting policy and procedures that fully comply with NIST. The recommendation is still open and OCIO has exceeded its estimated completion date of August 31, 2011.

8.1.5 If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3). - No

While multi-factor authentication for remote access is required by Departmental policy, we found one of two agencies we reviewed did not have it properly implemented. This occurred because while the enterprise solution for two-factor authentication (LincPass) is implemented and available, it is not required and therefore not being used Departmentwide. Also, the agencies' inability to distribute its PIV cards limited staff participation. In addition, one contract audit found, and another agency self-reported, not having two-factor authentication for remote access properly implemented.

In the FY 2010 FISMA report, we recommended the Department complete the Departmental projects that will enforce multi-factor authentication and external media encryption. The recommendation is still open; OCIO has exceeded its estimated completion date of September 30, 2011.

8.1.6 Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms. - No

If the Department would require the use of PIV cards for remote access authentication, it would satisfy all the NIST requirements, including strength mechanisms.[64] As reported in item 8.1.5 above, we found that while multi-factor authentication for remote access was required by Departmental policy, one of two agencies we reviewed did not properly implement it.

8.1.7 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.

[64] NIST SP 800-63, *Electronic Authentication Guideline* (April 2006).

8.1.8 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 requirements and timed-out after 30 minutes of inactivity and re-authentication was required.[65]

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

Even though lost and stolen equipment was consistently being processed (wiped and/or disabled), we found 13 of 13 incidents of lost or stolen remote access devices were not appropriately reported within the required timeframe.

8.1.10 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). - Yes

No exception noted. We reviewed two agencies' rules of behavior agreements, and found they were in accordance with Government policies.

8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1, NIST SP 800-53, PS-6). - Yes

No exception noted. We reviewed two agencies' user access agreements, and found they were 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? - No

While the Department and agencies were monitoring, detecting, and reporting unauthorized (rogue) connections, we found no documented policies requiring it. This occurred because the Departmental *Logical and Physical Access Control Policy* was still in draft and had not been issued.

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

S9: 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 develops, disseminates, and reviews/updates a formal, documented contingency planning policy. We found that the Department's contingency planning policy met these requirements.

In the FY 2011 FISMA report, OIG recommended that the Department update the contingency plan template to adequately address all NIST SP 800-53 requirements.[66] The recommendation has reached final action and the Department issued an updated contingency planning template that meets NIST requirements.[67]

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

NIST SP 800-34 states that conducting the BIA is a key element in a comprehensive information system contingency planning process.[68] The Department's guide on developing contingency plans requires that a BIA be completed, during the concurrency review, for each system.[69] We found two of two agencies reviewed by OIG did not have a BIA for any of their systems.

9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34). - Yes

No exception noted. We found that all contingency plans (20 of 20) had addressed the key information required by NIST 800-34. Both tested agencies used the same outline for all contingency plans.

[66] USDA *Contingency Plan Template* (March 2011).
[67] USDA *Contingency Plan Template* (December 2012).
[68] NIST SP 800-34, *Contingency Planning Guide For Federal Information Systems* (May 2010).
[69] Department Manual 3570-001, *Disaster Recovery and Business Resumption Plans* (February 17, 2005).

9.1.4 Testing of system specific contingency plans. - No

NIST SP 800-53 requires Federal agencies to test and exercise contingency plans for information systems, using organization-defined tests or exercises. This is done to determine the plans' effectiveness and the organization's readiness to execute the plans and initiate corrective actions. We identified 89 of 243 systems for which USDA system contingency plans had not been tested or documentation had not been updated during FY 2013 as required.[70]

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 formal, documented procedures to facilitate the implementation of its contingency planning policy and associated controls. We found that the documented business continuity and disaster recovery plans were not in place and cannot be implemented when necessary. For example, 13 of 51 statistically sampled system contingency plans did not have evidence of ongoing testing of the plan.[71] Based on our sample results, we estimate that 58 systems in our universe (about 26 percent of the universe) did not have evidence of ongoing testing.[72]

9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). - Yes

No exception noted. NIST SP 800-53 requires Federal agencies to test and exercise contingency plans for information systems, using organization-defined tests or exercises. We found that all 64 of the systems we reviewed had documented training, testing, and exercise programs incorporated in their contingency plans.

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 and exercise contingency plans for information systems, review the contingency plan test/exercise results, and initiate corrective actions. As noted in 9.1.5, we found that there were 13 of 51 systems within our sample of Departmental systems that did not perform testing or provide evidence to show ongoing testing of plans. We also identified 89 of 243 Departmental systems without a testing date during FY 2013 recorded in CSAM.

---

[70] Systems Inventory as of October 28 2013. *USDA Contingency Plan Exercise Handbook,* Rev 1.1 (February 2011).

[71] We selected a simple random sample of 51 contingency plans for review. For a 95 percent confidence level, this sample size was adequate for a range of potential outcomes: from a 0 percent exception rate with a 5 percent upper limit to a 20 percent error rate with +/-10 percent precision. Additional sample design information is presented in Exhibit B.

[72] We are 95 percent confident that between 33 (15 percent) and 82 systems (37 percent) are non-compliant with this criterion. Additional sample design information is presented in Exhibit B.

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. As stated in 9.1.7, our review of 51 sampled systems from the Department found that 13 did not have a record of testing and therefore, no after action report.

9.1.9 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). - Yes

No exception noted. NIST SP 800-53 requires alternate processing sites to be established for information systems in case of a disaster. We statistically sampled 51 systems and found all of those systems met the requirement to provide an alternate processing site.

9.1.10 Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800- 53). - Yes

No exception noted. We found that 51 of 51 systems from our statistical sample had alternate processing sites that were not subject to the same risks as the primary site**.**

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

No exception noted. NIST SP 800-53 states that the organization should conduct user-level, system-level, and information system documentation backups. We found two of two agencies reviewed by OIG were performing backups in a timely manner.

9.1.12 Contingency planning that considers supply chain threats. - No

We found 4 of 51 contingency plans in our statistical sample of Department systems did not document or consider supply chain threats within the contingency plan.[73] This occurred because the disaster recovery plans had not been completed. Based on our sample results, we estimate that 18 systems in our universe (about 8 percent of the universe) did not have evidence that they considered their supply chains or vendors.[74]

[73] We selected a simple random sample of 51 contingency plans for review. For a 95 percent confidence level, this sample size was adequate for a range of potential outcomes: from a 0 percent exception rate with a 5 percent upper limit to a 20 percent error rate with +/-10 percent precision. Additional sample design information is presented in Exhibit B.

[74] We are 95 percent confident that between 4 (actual number found, 2 percent) and 33 systems (15 percent) are non-compliant with this criterion.

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.

S10: Contractor Systems

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

Besides the improvement opportunities that may have been identified by the OIG, does the program includes 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 organization systems and services residing in a public cloud. - No

We found that the Department has not established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in a cloud environment external to the organization. We found that the Department does not have documented policies relating to this topic.

In the FY 2010 FISMA report, we recommended that the Department develop policy and procedures for information security oversight of systems operated on the agency's behalf. The policy and procedures should ensure that an accurate inventory of contractor systems and memoranda of understanding/interconnection service agreements are completed periodically. The recommendation is still open and has exceeded the estimated completion date of September 15, 2011. OCIO has had a policy in draft for 4 years and has not yet finalized it.

10.1.2 The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2). - No

As noted in 10.1.3 below, we found operational contractor systems in CSAM that did not have a current ATO, interconnections were not sufficiently documented, or did not have a signed SSP. Based on these findings, we determined that the Department's contractor systems program was not ensuring that security controls of contractor systems and services were effectively implemented and complied with organizational guidelines.

10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud. - No

USDA's contractor systems program does not include a complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a cloud. We found 1 contractor system was not in the Department's inventory, 1 cloud system was incorrectly identified as a non-contractor system, 3 contractor systems had insufficient interconnection documentation, 5 systems had expired ATOs, and 14 systems had missing authorizing signatures. We also reviewed a random sample of 40 non-contractor systems and found that 4 had insufficient interconnection documentation. Based on our sample results, we estimate 20 non-contractor systems (10 percent of the universe) had insufficient interconnection documentation.[75]

In the FY 2010 FISMA report, we recommended that OCIO ensure contractor and non-contractor systems inventory and interfaces are accurate and updates are completed at least annually. The recommendation is still open; OCIO has exceeded its estimated completion date of September 15, 2011.

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 15 operational and reportable contractor systems in CSAM and found that 3 did not have adequately identified or documented interfaces in CSAM.

In the FY 2012 FISMA report, we recommended that OCIO develop and implement an effective process for making sure interface connections are documented, and that Interconnections Security Agreements accurately reflect all connections to the systems. The Department needs to review interfaces during its annual testing processes. The recommendation is still open; OCIO has exceeded its estimated completion date of September 30, 2013.

As noted in 10.1.3 above, in the FY 2010 FISMA report, we recommended that the Department ensure contractor and non-contractor systems inventory and interfaces are accurate and updates are completed at least annually. The recommendation is still open; OCIO has exceeded its estimated completion date of September 15, 2011.

Also, in the FY 2009 FISMA report, we recommended the Department develop and implement an effective process to ensure system interfaces are accounted for in CSAM. The Department reached final decision by issuing a CSAM Users Guide and POA&M SOP (CPO-SOP-002). Because these are not policy guidance, we take exception to final action being reached on this recommendation.

[75] We are 95 percent confident that between 3 (1 percent) and 38 (19 percent) non-contractor systems may have insufficient interconnection documentation in CSAM. Additional sample design information is presented in Exhibit B.

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

The Department's contractor systems program was not requiring appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. As noted in 10.1.4 above, we found three contractor systems that did not have adequately identified or documented interfaces in CSAM.

10.1.6 The inventory of contractor systems is updated at least annually. - No

We found that inventory reconciliation had not been performed for over 4 years and the Department did not have documented policies and procedures for oversight of contractor systems.

As noted in 10.1.3 above, in the FY 2010 FISMA report, we recommended that OCIO ensure contractor and non-contractor systems' inventory and interfaces are accurate and updates are completed at least annually. The recommendation is still open; OCIO has exceeded its estimated completion date of September 15, 2011.

10.1.7 Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. - No

We found 5 contractor systems with expired ATOs, 3 contractor systems with missing interconnection agreements, and 14 contractor systems with missing SSP signatures. We also found a cloud system that was not included in the Department's inventory and another that was not identified as a contractor system.

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.

S11: Security Capital Planning

11.1 Has the organization established a security capital planning and investment program for information security? - Yes

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

11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process. - Yes

No exception noted. In response to our FY 2011 audit recommendation, OCIO issued a new policy on May 29, 2013 updating the definition of a major IT investment.

11.1.2 Includes information security requirements as part of the capital planning and investment process. - No

We reviewed the Exhibit 53B documentation submitted by USDA and four selected agencies as part of the annual budgeting process. Our testing determined USDA's security capital planning and investment program includes information security requirements as part of the capital planning and investment process; however, detailed testing determined all four of the reviewed agencies could not provide adequate supporting documentation for the amounts submitted on its annual Exhibit 53B. This occurred because the agencies were unaware of the need to retain adequate supporting documentation used during the budgeting process. As a result, USDA lacks justification for the IT security costs portion in its budgetary request.[76]

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2). - No

We reviewed the Exhibit 53B documentation submitted by USDA and four selected agencies as part of the annual budgeting process. However, as noted in 11.1.2, detailed testing determined four of the four agencies selected could not provide adequate supporting documentation for the amounts submitted on their annual Exhibit 53B, therefore a discrete line item for information and security in organizational programming and documentation could not be supported.

11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3). - No

We reviewed a sample of Exhibit 300 documents submitted by agencies within USDA to verify that the Exhibit 300 included OMB required supporting documentation.[77] Our testing determined that USDA does not consistently employ business cases across Exhibit 300s based on the absence of required documentation for 4 of the 11 Exhibit 300s reviewed. As a result, the Major IT investments within USDA lack the required supporting documentation that outlines the investment's planning, funding, and implementation progress through the project life cycle. This occurred because OCIO's Capital Planning Division (CPD) did not require all supporting documentation to be submitted.

In addition, our testing identified an IT investment that was not considered major by the Department upon its inception on April 30, 2010. Based on the definition of a major investment

[76] Agencies must provide IT Investment information using the Agency IT Investment Portfolio (Exhibits 53A&B), *Guidance on Exhibit 53 – Information Technology and E-Government*, OMB (2011).
[77] Exhibit 300 establishes policy for planning, budgeting, acquisition, and management of major IT capital investments. OMB, *Guidance on Exhibit 300 – Planning, Budgeting, Acquisition, and Management of IT Capital Assets* (2011).

by OMB as "*a system or acquisition requiring special management attention because of its importance to the mission or function of the agency, a component of the agency, or another organization;"* we believe the investment should have been considered a major IT investment in 2010. This is based upon the investment's function, which provides cloud-based email support to USDA, and is a critical function within the Department. The Department categorized the investment as major in FY 2013 for the FY 2015 budget cycle; however, by not classifying it as a major investment in 2010, the Department did not record and report the information security resources required for the investment during the annual budgeting process for the previous three years.

11.1.5 Ensures that information security resources are available for expenditure as planned. - No

We reviewed the Exhibit 53B documentation submitted by USDA and the four selected agencies as part of the annual budgeting process. Our testing determined that the Exhibit 53B was prepared and submitted; however, as noted in 11.1.2, the agencies could not provide documentation that supported the amounts included on the Exhibit 53B. We determined the agencies did not adequately plan when expending IT resources based on the Exhibit 53B because supporting documentation for the amounts was not maintained. This occurred because CPD did not require the submission of all supporting documentation. As a result, USDA lacks justification for the IT security costs portion of its budgetary request.

11.2 Please provide any additional information on the effectiveness of the organization's Security Capital Planning 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 audit number 50501-0004-12. 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' CIOs, and compliance with FISMA;
- Agencies' system of internal controls over IT assets;
- Department's progress in establishing a Departmentwide security program, which includes effective assessments and authorizations;
- Agencies' and Department's POA&M consolidation and reporting process; and
- Effectiveness of controls over configuration management, incident response, IT training, remote access management, identity and access management, continuous monitoring, contingency planning, contractor systems, and capital planning.

FISMA Audit Universes and Sample Designs:
FISMA contains multiple areas pertaining to various areas of IT security. We incorporated statistical sampling in four FISMA areas. Each of those areas was represented by a different universe. The specific design is summarized below for each of the four audit areas.

1. Incident Response and Reporting

Universe:
The audit universe consisted of 2,050 incidents reported for FY 2013, as of July 15, 2013. Each incident had a unique identifier (incident number) and was categorized based on incident type into one of nine categories. We wanted to ensure that at least one incident of each type was selected in our sample for review. One of the incident categories—CAT2—contained only three incidents. To make sure that that incident type would get selected for review, we separated it into a census stratum of its own. We called that our stratum 1. Stratum 2 consisted of all other types of incidents—a total of 2,047.

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 apply specifically to that incident type. This allowed us to combine incident response performance results (pass or fail) for the mix of incident types.

Stratum 1 was a census stratum consisting of the 3 CAT2 incidents.

From stratum 2, which consisted of 2,047 incidents, we selected a simple random sample of 89 incidents for review. The sample size was calculated based on the following factors:

- A desired 95 percent confidence level;
- A desired +/-10 percent precision in an attribute testing scenario;
- A universe size of 2,047 units;
- An expected error rate of 40 percent, based on historical information.

A listing and counts of incidents within the different categories in our universe and sample are presented in Table 1.

Table 1: Sample design summary for Incident Response and Reporting

	Incident type	*Number of incidents in the universe*	*Number of incidents in the sample*
Stratum 1	CAT2 incidents - census	3	3
	Total for this stratum	3	3
Stratum 2	USCERT CAT0 - Exercise/Network Defense Testing Count	150	7
	USCERT CAT1 - Unauthorized Access Count	32	1
	USCERT CAT3 - Malicious Code Count	798	29
	USCERT CAT4 - Improper Usage Count	83	6
	USCERT CAT5 - Scans/Probes/Attempted Access Count	19	1
	USCERT CAT6 - Investigation Count	455	17
	USDA CAT8 (USCERT CAT1) - Loss, Theft, Missing Count	242	13
	USDA CAT9 - Block List Count	268	15
	Total for this stratum	2047	89
	Grand Total	2050	92

Results:
Results are projected to the audit universe of 2,050 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 stratified sample.[78]

The audit team tested a variety of criteria: whether or not the required personally identifiable information checklist was completed; 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 IMD; whether or not the completed incident identification form was completed in its entirety; whether or not the required incident category checklist was completed; and if incidents were open for over 30 days without a POA&M being created.[79]

[78] Scheaffer, Mendenhall, Ott, Elementary Survey Sampling, Fourth Edition (Chapter 5), Duxbury Press, c1990.
[79] Personally identifiable information is defined as any information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to the individual.

We developed a projection for whether or not incidents were reported to US-CERT within the requested timeframe, and an overall projection, which is 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.

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

Table 2: Incident Response and Reporting Projections

Estimate description for tested criteria	Estimate	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved Precision[80]
			Lower	Upper		
Estimated number of incidents not reported to US-CERT within the required timeframe	460	89.079	283	637	.194	9%
as a % of universe	22%	4%	14%	31%		
Estimated total number of incidents with at least one exception	530	93.426	344	716	.176	9%
as a % of universe	26%	5%	17%	35%		

Based on our sample results:

- We estimate that 460 incidents (about 22 percent of the audit universe) were not reported to US-CERT within the required timeframe. We are 95 percent confident that between 283 (14 percent) and 637 (31 percent) incidents in the audit universe are non-compliant with this criterion.
- We estimate that 530 incidents (about 26 percent of the audit universe) had at least one exception in the tested criteria. We are 95 percent confident that between 344 (17 percent) and 716 (35 percent) incidents in the audit universe were not handled in accordance with departmental procedures.

2. POA&Ms

POA&Ms (closed)

Universe:
The universe consisted of 869 POA&Ms.

Sample Design:
We selected a simple random sample of 68 closed POA&Ms for review. We based our sample size on the following factors:

- A desired 95 percent confidence level;
- A desired +/-10 percent precision in an attribute testing scenario;

[80] Achieved precision is the difference between the estimate and the bounds divided by the size of the universe. For example: (637- 460)/2050 = 9 percent (rounded to the nearest whole number).

- A universe size of 869 units;
- An expected error rate of 25 percent, based on historical information.

Results:
Results for all criteria are projected to the audit universe of 869 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.[81]

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

Estimate description for tested criteria	Estimate	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved Precision
			Lower	Upper		
Estimated number of closed POA&Ms reviewed that did not have effective remediation plans detailed in CSAM to correct the identified weakness.	128	36.099	56	200	.282	8%
as a % of the universe	15%	4%	6%	23%		

Based on our sample results, we estimate that 128 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 56 (6 percent) and 200 (23 percent) POA&Ms in the audit universe are non-compliant with this criterion.

3. System / Contingency Planning

Universe:
Our universe consisted of 220 FISMA reportable systems for a variety of agencies reviewed as of July 17, 2013. Each system is to have a contingency plan that contains very specific recovery information in the event of a disaster.

Sample Design:
We wanted to ensure that at least one contingency plan per agency chosen for FISMA review was selected in our sample for review. All agencies, except one, contained at least 19 incidents in our universe. It contained only two incidents. Hence, we separated one agency into a census stratum of its own, which we call stratum 1. Stratum 2 contained all other incidents – a total of 218. In stratum 2, we selected a simple random sample of 49 contingency plans for review. Our sample size was based on the following factors:
- A desired 95 percent confidence level;
- A desired +/-10 percent precision in an attribute testing scenario;

[81] Op. cit., Scheaffer et al. Chapter 4.

- A universe size of 218 units;
- An expected error rate of 20 percent, based on historical information.

Results:
The audit team reviewed the 51 system contingency plans selected in the sample. Results are projected to the audit universe of 220 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. For one criterion, the lower bound was lower than the number of exceptions observed in the sample. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.[82]

Projections are shown in Table 4. The narrative interpretation of the results can be found below the table.

Table 4: System / Contingency Planning Projections

Description of estimate for tested criteria	Estimate	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved Precision
			Lower	Upper		
Number of systems that did not have ongoing testing or did not provide documentation of testing	58	12.231	33	82	.211	11%
as a % of universe	26%	6%	15%	37%		
Number of contingency plans that did not have evidence that they considered their supply chains or vendors	18	7.586	4*	33	.426	7%
as a % of universe	8%	3%	2%	15%		

* Actual number found. Statistical lower bound = 3.

Based on our sample results:

- We estimate that 58 systems in our universe (about 26 percent of the universe) did not have ongoing testing or did not provide documentation of testing. We are 95 percent confident that between 33 (15 percent) and 82 systems (37 percent) are non-compliant with this criterion.
- We estimate that 18 systems in our universe (about 8 percent of the universe) did not have evidence that they considered their supply chains or vendors. We are 95 percent confident that between 4 (actual number found, 2 percent) and 33 systems (15 percent) are non-compliant with this criterion.

In addition to the criteria above, the audit team tested and found the following:

- 51 of 51 agency contingency plans incorporated test, training, and exercise programs into their plans. All the systems in our sample were compliant with the requirement. Based on this sample result, we are 95percent confident that non-compliance in this criterion does not exceed 5 percent.

[82] Ibid.

- We found 51 of 51 agency contingency plans included an alternate processing site. All were compliant. Based on this sample result, we are 95 percent confident that non-compliance in this criterion does not exceed 5 percent.
- We found 51 of 51 alternate processing sites were not subject to the same risks as the primary site. All were compliant. Based on this sample result, we are 95 percent confident that non-compliance in this criterion does not exceed 5 percent.

4. CSAM for non-contractor systems

Universe:
Our universe consisted of 201 operational, FISMA-reportable, non-contractor systems. We excluded OIG and the two sample agencies from our universe and sample because they were chosen as sample agencies for our FY 2013 FISMA review, so their systems were already under review.

Sample Design:
We selected a simple random sample of 40 systems for review. The audit team expected to find very few errors. We based the sample size on an expected error rate of 15 percent and a desired precision of +/-10 percent at the 95 percent confidence level.

Results:
Our audit team reviewed all 40 systems selected in the sample and found none that were misidentified. Based on this result, we are 95 percent confident that the percentage of systems that are misidentified does not exceed 6.5 percent of all the systems in our audit universe.

Auditors reviewed documentation and found 4 non-contractor systems with insufficient interconnection documentation. Based on this sample result, we project that 20 systems in the universe of 201 have this issue. We are 95 percent confident that between 3 and 38 CSAM systems may have insufficient documentation. Table 5 shows the parameters for this projection.

Table 5: CSAM for non-contractor systems projections

Description of estimate for tested criteria	Estimate	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved Precision
			Lower	Upper		
Estimated number of systems with insufficient interconnection documentation	20	8.642	3	38	.430	9%
as a % of universe	10%	4%	1%	19%		

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
e-mail: USDA.HOTLINE@oig.usda.gov
phone: 800-424-9121
fax: 202-690-2474

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