United States Department of Agriculture
Office of Inspector General

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2012 Federal Information Security Management Act

Audit Report 50501-0003-12

November 2012

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2012
Federal Information Security Management Act

Audit Report 50501-0003-12

What Were OIG's Objectives

Our objective was to evaluate USDA's overall IT security program, including the effectiveness of the Department's oversight, compliance with FISMA, 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.

What OIG Reviewed

The scope of this audit was Departmentwide and included agency IT audit work completed during FY 2012, other OIG audits completed throughout the year, and the results of reviews performed by contract auditors. In total, our FY 2012 audit work covered 10 agencies and staff offices, operating about 124 of the Department's 251 major systems.

What OIG Recommends

The Department should complete actions on the 29 outstanding recommendations from the FY 2009-2011 FISMA audit reports and the 6 new recommendations included in this report.

As required by the Federal Information Security Management Act (FISMA), OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices, as of FY 2012.

What OIG Found

The Office of Inspector General (OIG) found that, although the Department of Agriculture (USDA) has made improvements in its information technology (IT) security over the last decade, many longstanding weaknesses remain. In fiscal years (FY) 2009, 2010, and 2011, OIG made 43 recommendations for improving the overall security of USDA's systems, but only 14 of these have been closed. OIG has reported many of these remaining recommendations since 2001, when we first detailed a material weakness in the design and effectiveness of USDA's overall IT security program.

In order to mitigate the continuing material weakness, we have recommended that USDA and its agencies work together to define and accomplish a manageable number of critical objectives before proceeding to the next set of priorities. Instead, when the Department received $66 million in increased funding in FY 2010 and 2011, the Office of the Chief Information Officer (OCIO) used the money to fund 16 separate projects, some of which did not address the Department's most critical IT security concerns.

Again this year, we continue to report a material weakness in USDA's IT security. The Department has not (1) established a continuous program for monitoring IT security or contractor systems; (2) ensured that agencies securely configure their computers, as required; (3) mandated user multi-factor authentication; (4) consistently reported security incidents; (5) implemented a risk-based framework for handling security issues; (6) adequately remediated weaknesses; (7) implemented adequate contingency policies and procedures; and (8) adequately planned for security costs.

USDA

U.S. Department of Agriculture
Office of Inspector General
Washington, D.C. 20250

OFFICE OF INSPECTOR GENERAL OIG USDA

DATE: NOV 15 2012

Jeffrey D. Zients
Deputy Director for Management
The Office of Management and Budget
725 17th Street, NW
Washington, D.C. 20503

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2012 Federal Information Security Management Act Report (Audit Report 50501-0003-12)

This report presents the results of our audits 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.

Sincerely,

Phyllis K. Fong
Inspector General

Table of Contents

Findings and Recommendations..1

Recommendations..8

Background 10

Objectives 11

Scope and Methodology...12

Abbreviations 14

Exhibit A: Office of Management and Budget (OMB)/Department of Homeland Security (DHS) Reporting Requirements and U. S. Department of Agriculture (USDA) Office of Inspector General (OIG) Position.....................16

Exhibit B: Sampling Methodology and Projections 49

U. S. Department of Agriculture, Office of the Chief Information Officer (OCIO), Fiscal Year 2012 Federal Information Security Management Act (FISMA) (Audit Report 50501-0003-12)

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) 2012. 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 2012. While USDA's planned activities might improve its security posture in the future, we could not evaluate these initiatives as part of our FY 2012 FISMA review because they were not fully operational during the year. However, we did note that during FY 2012, the Office of the Chief Information Officer (OCIO) began a reorganization, appointed its first Chief Information Security Officer, and elevated the responsibility for policies to the executive level.

USDA has made improvements in its IT security over the last decade, but many longstanding weaknesses remain. In our FISMA audits for FYs 2009, 2010, and 2011, OIG made 43 recommendations for improving the overall security of USDA's systems. By the end of FY 2012, the Department had remediated and closed only 14 recommendations, leaving 29 to be addressed. OIG has reported on many of these remaining recommendations since 2001, when we first detailed material weaknesses in the design and effectiveness of USDA's overall IT security program. The findings in this report continue to be a material IT weakness for the Department.

USDA is a large, complex organization that includes 34 separate agencies and staff offices, most with their own IT infrastructure. Since 2009, in order to mitigate continuing material weaknesses, we have reported that the Department should concentrate its efforts on a limited number of priorities, instead of attempting to achieve numerous goals simultaneously in short timeframes. We recommended that USDA and its agencies work together to define and accomplish a limited number of critical objectives before proceeding to the next set of priorities.

When the Department received $66 million in increased funding in FYs 2010 and 2011, OCIO used the money to fund 16 separate projects rather than funding a manageable number of prioritized projects.[1] When OCIO initially requested the increase in funding from Congress, OCIO proposed that these funds be used to bolster three IT security areas: Network Security Assessments, Security Tools, and the creation of an Agriculture Security Operations

[1] Audit 88401-0001-12, *Audit of the Office of the Chief Information Officer's FYs 2010 and 2011 Funding Received for Security Enhancements* (August 2012).

Center (ASOC). However, we found that when OCIO received its funding increase for the proposed projects, it did not use the money exclusively for the purposes outlined in its Congressional request or for projects addressing the Department's most critical IT security concerns. Network Security Assessments were not completed for all agencies, security tools were not fully implemented and those implemented were not capable of capturing all USDA network traffic, and the ASOC is not a 24x7x365 operation.[2] Rather, OCIO expended over $6.7 million of these funds for an IT intern program, a re-engineered Certification and Accreditation (C&A) project, and a governance and risk compliance team. While these three programs may be beneficial in the long run, they did little to further the more pressing objective of improving USDA's IT security. Focusing resources on these three projects may have detracted from other more pressing projects—such as conducting network security assessments—that more directly addressed Congress' and the Department's IT security priorities. In addition, in April 2011, Congress reduced OCIO's appropriation as part of the continuing resolution. This caused many of the 16 projects to be severely scaled back and project timelines to be extended further into the future.

We continue to recommend that USDA undertake a manageable number of its highest priority projects and show measureable progress towards the milestones for each active project. USDA's inability to complete projects in a timely manner continues to hinder its progress towards improving its security posture.

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 in OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (October 2, 2012) and DHS Federal Information Security Memorandum 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (February 15, 2012).

To address the FISMA metrics, OIG reviewed systems and agencies, OIG independent contractor audits, annual agency self-assessments, and various OIG audits throughout the year.[3] 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 established a policy, strategies, or plans for continuous monitoring. Additionally, we found 25 of 254 systems where ongoing assessments

[2] In FY 2010, OCIO informed Congress that it would utilize $12.3 million to establish ASOC, which was to "coordinate continuous 24x7x365 security operations to defend USDA information, assets, network and systems." The term "24x7x365" is defined as 24 hours a day, 7 days a week, and 365 days a year.

[3] 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's 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.

of selected security controls had not been performed in FY 2012.[4] As a result, agencies that own these systems cannot ensure that controls remain effective over time, as changes occur in threats, missions, environments of operation, and technologies. 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. OCIO stated that it does not have the resources currently to support this function and is waiting for more definite Federal guidance from the National Institute of Standards and Technology (NIST) and other working groups.

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 their servers and workstations. Specifically, one agency that OCIO is responsible for was not scanning its devices, while another agency was only scanning 11 percent of its devices. We also found that five of five agencies reviewed did not have a process for timely remediation of scan result deviations.[5] For example, OIG ran a commercially available vulnerability scan tool on 4,372 devices within the Department to verify that vulnerabilities were mitigated timely. We found 6,109 high and medium vulnerabilities were present and not corrected; 3,111 of these were over 6 months old. In the FY 2010 FISMA audit, OIG recommended the Department ensure scanning for compliance to the baseline configurations and for vulnerabilities is performed, as required by 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 and identifies users and network devices. 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.[6] Additionally, agencies were able to identify devices, users, and non-users who access their organization's systems and networks. However, our testing identified opportunities for improvement. We found that the Department and two agencies reviewed do not mandate

[4] The 254 major applications were reported in the Cyber Security Assessment and Management (CSAM) system as of October 2, 2012 at 8:49 a.m.

[5] 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.

[6] 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.

multi-factor authentication, as required.[7] In addition, agencies that had implemented multi-factor authentication were using an alternate method, instead of the organization's PIV card.[8] Agencies were reluctant to use the PIV card due to the length of time involved in receiving new or replacement cards. We also found that agencies did not ensure that users are granted access based on need and agencies did not ensure that accounts were terminated or deactivated once access was no longer required. We found 363 separated users in the two agencies that still had active accounts. One agency stated that its goal was to keep the separated employees with active accounts to less than 3 percent. Department policy states that accounts should be disabled within 48 hours of an employee's separation.

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. OCIO has implemented new procedures that it actually uses daily, but it has not updated its official documented procedures. Our review of 75 incidents disclosed that 32 incidents were not handled in accordance with Departmental procedures.[9] Of the 32 incidents identified, USDA did not report 31 of the incidents to United States-Computer Emergency Response Team (US-CERT) within the required timeframe—18 of these incidents were the result of a lost or stolen device. These incidents were not promptly reported to the Incident Handling Division (IHD).[10] Additional testing determined the Department has implemented technical capabilities to allow it to correlate incidents across the Department; however, based on the status of the tools deployed, as well as the methodologies utilized for deployment, it does not have the ability to correlate incidents throughout the entire USDA network infrastructure. Based on testing of USDA's cloud provider's traffic, discussions with USDA IT personnel, and our review of the cloud provider Service Agreement and Incident Plan, we also determined that the Department is not capable of managing risks in a 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 roles and responsibilities for each party.[11]

[7] 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.

[8] 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.

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

[10] 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 the DHS. NCSD was established by DHS to serve as the Federal Government's cornerstone for cyber security coordination and preparedness.

[11] 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."

The Department does not have a Risk Management Framework (RMF) that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.[12] We continue to find that the RMF required by NIST has not been planned and implemented. According to the Department, this occurred 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 CSAM system.[13] OCIO is also responsible for ensuring that agencies are compliant with Federal and Departmental guidance and are reporting aggregate results during the annual FISMA reporting cycle. NIST transforms the traditional Assessment and Authorization (A&A) process into a six-step RMF process.[14]

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 to agencies that did not meet NIST requirements. However, we found that improvements are still needed. Specifically, the following A&A documentation did not meet NIST requirements: (1) systems were not properly categorized; (2) system security plan (SSP) controls were not implemented properly and did not sufficiently address each control; and (3) security assessment reports did not include an authorized security

[12] 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).

[13] 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.

[14] 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 is granted a formal Authority to Operate (ATO) by an agency official.

assessment plan.[15] 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.

- Additionally, we found an OCIO parent system in the development stage with three child systems that were operational with no Authority to Operate (ATO), and another six systems that are operational with no ATO.[16] Furthermore, the Department has 22 systems with expired ATOs, one system being 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. Department policy met all NIST requirements for annual security awareness training.[17] However, we identified opportunities for improvement. Specifically, USDA lacks 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 and the application rules.

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 and monitors known information security weaknesses.[18] However, our testing identified some deficiencies. For example, the Department did not have effective policies and procedures for reporting IT security deficiencies in CSAM. We found the POA&Ms did not always include all known security weaknesses. For example, the Department failed to create POA&Ms for the 10 OIG recommendations, based on IT security deficiencies, in the FY 2011 FISMA audit report. These missing POA&Ms occurred because the Department security manual did not include a policy for establishing a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts. In addition, our review of POA&Ms within CSAM found that agencies were not adequately detailing their plans for remediation and were not including proper supporting documentation for effective closure. We found 176 of 1,106 FY 2012 closed POA&Ms had remediation actions that did not sufficiently address the identified

[15] 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 security assessment report (SAR).

[16] A parent system owns, manages, and/or controls the child system.

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

[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.

weakness. We also noted that the Department is not tracking and reviewing POA&Ms, as required by the Department's SOP.[19] Finally, we found that the Department was not completing quarterly reviews of closed POA&Ms and was not reviewing all closed audit POA&Ms, as required.

The Department has established a remote access program that is consistent with FISMA requirements and OMB policy. However, our testing identified that Departmental policies for remote access and teleworking did not meet NIST requirements and the two agencies we reviewed stated that they depended on the Departmental policies. 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; OCIO has exceeded its estimated completion date of August 31, 2011. We also found, or the agencies self-reported, that three out of three agencies' remote access programs did not protect against unauthorized connections or subversion of authorized connections. The agencies were not reviewing access logs to determine if unauthorized remote access had occurred. The agencies stated that they were reviewing the logs, but were unable to provide any documentation that the review had occurred. USDA requires multi-factor authentication for all remote access (i.e., two means of identification).[20] However, we found, or the agencies self-reported, that four of four agencies did not have multi-factor authentication properly implemented. As noted above, agencies are reluctant to use the PIV card, due to the length of time involved for receiving new or replacement cards. Inadequate security controls over remote access and teleworking could result in the unauthorized access, use, disclosure, modification, or destruction of information.

The Department has established an enterprisewide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. However, our testing identified opportunities for improvement. Specifically, the Department's contingency policies and procedures did not meet NIST SP 800-53 requirements. We found the Departmental template provided to the agencies for contingency planning purposes did not contain all of NIST's required elements. In the FY 2010 FISMA report we recommended that OCIO update the contingency plan template to meet NIST requirements. This recommendation is still open; OCIO has exceeded the estimated completion date of September 30, 2011. The Department has stated that it has updated the template and it is currently in the approval process. We also found 42 of 247 systems in CSAM that had not completed contingency plan testing or updated documentation in CSAM for FY 2012.[21] Agencies stated that this occurred because of a lack of proper documentation or inadequate resources.

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

[19] Departmental SOP, *Plan of Action and Milestones Management* (June 29, 2011).

[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.'"

[21] The 247 major applications were reported in CSAM as of October 2, 2012.

2 years and has not yet finalized it. 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. Specifically, we found eight contractor systems with expired ATOs, four contractor systems with missing interconnection agreements, and five contractor systems with missing authorizing signatures. Additionally, OIG found one vendor-controlled (cloud) system that was in production for 15 months before NIST-required documentation was in CSAM.

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. The agencies stated that they were unaware of the need to retain adequate supporting documentation used for the budgeting process.

The below recommendations are new for FY 2012. Because 29 recommendations from FY 2009, FY 2010, and FY 2011 remain without final closure, we have not made any repeat recommendations. If the plans initiated to close out the FY 2009, 2010, and 2011 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.

Recommendations

1. Modify the service agreement between the Department and the e-mail 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 e-mail system (i.e., so that the Department can view/monitor network traffic in the cloud system).

2. The Department should deploy adequate/appropriate technology on the necessary routers to capture all network traffic.

3. The Department should finalize the deployment of its security tools in order to correlate incidents across the network.

4. The Department should verify that all systems have the proper authority to operate prior to implementation.

5. Develop and implement an effective process for making sure interface connections are documented, and that Interconnections Agreements accurately reflect all connections to the systems. The Department needs to review interfaces during the annual testing processes.

6. Incorporate a review of line items in the annual Capital Planning cycle to verify that information security resources requested by the agencies are accompanied by required supporting documentation.

Background & Objectives

Background

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

On December 17, 2002, the President signed 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 security of Federal Government data and information systems, such as requiring the development of minimum control standards for agencies' systems. NIST was tasked to work with agencies in developing those standards as part of its statutory role in providing technical guidance to Federal agencies.

FISMA 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*. 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 agencies implemented FISMA. It also established how OMB and Congress would oversee IT security.

FISMA assigned specific responsibilities to OMB, agency heads, Chief Information Officers (CIO), and Inspectors General (IG). In OMB Memorandum M-10-28, OMB transferred portions of its responsibilities to DHS. The memorandum clarified that OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. It further stated that DHS exercises primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA. DHS was given broad implementation responsibilities to include overseeing agencies' compliance with FISMA and developing analyses for OMB to assist in the development of its annual FISMA report.

Each agency must establish a risk-based information security program that ensures information security is practiced throughout the lifecycle of each agency's systems. Specifically, the agency's CIO is required to oversee the program, which 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 to the responsibilities listed above, FISMA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and a compliance assessment. The evaluations are to be performed by the agency's IG 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 assessment and authorizations;
- Agencies' and the 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.

Scope and Methodology

The scope of our review was Departmentwide and included agency IT audit work completed during FY 2012. 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 May 2012 through October 2012. 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 seven additional USDA agencies. In total, our FY 2012 audit work covered 10 agencies and staff offices:

- Agricultural Research Service (ARS),
- Foreign Agricultural Service (FAS),
- Federal Crop Insurance Corporation (FCIC),
- Forest Service (FS),
- Farm Service Agency (FSA),
- International Technology Services (ITS),
- National Information Technology Center (NITC),
- Natural Resources Conservation Service (NRCS),
- Office of the Chief Financial Officer (OCFO), and
- Office of the Chief Information Officer (OCIO).

These agencies and staff offices operate approximately 124 of the Department's 251 general support and major application systems.[22]

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*;
- Evaluated the Department's progress in implementing recommendations to correct material weaknesses identified in prior OIG and GAO audit reports;
- Gathered the necessary information to address the specific reporting requirements outlined in OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the*

[22] The 251 major applications were reported in CSAM as of October 2, 2012 at 6:26 a.m. The total number of systems can vary based upon the date/time the report is run. New systems can be added and old systems retired. The total universe of systems in this report varies because tests were done at different times throughout FY 2012.

Federal Information Security Management Act and Agency Privacy Management (October 2, 2012);

- Performed detailed testing specific to FISMA requirements at selected agencies, as detailed in this report; and
- Performed statistical sampling on testing, where appropriate. Additional sample analysis information is presented in Exhibit B.

Testing results were compared 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
ASCO	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
FAS	Foreign Agricultural Service
FCIC	Federal Crop Insurance Corporation
FDCC	Federal Desktop Core Configurations
FISMA	Federal Information Security Management Act
FS	Forest Service
FSA	Farm Service Agency
FY	Fiscal Year
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
HSPD-12	Homeland Security Presidential Directive-12
IG	Inspector General
IHD	Incident Handling Division
IP	Internet Protocol

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
NRCS	National Resources Conservation Service
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
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
US-CERT	US-Computer Emergency Response Team
USDA	Department of Agriculture

Exhibit A: Office of Management and Budget (OMB)/Department of Homeland Security (DHS) Reporting Requirements and U. S. Department of Agriculture (USDA) Office of Inspector General (OIG) 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 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.[23] 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 for 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 800-53: CA-7)? - No

The Department's continuous monitoring policies and procedures were still in draft as of September 30, 2012. In the FY 2009 and 2010 FISMA report, OIG recommended that the Department develop policies, procedures, strategies, and implementation plans for continuous monitoring. The recommendation is still open and has exceeded the estimated completion date of September 30, 2011. OCIO stated that they do not have the resources currently to support this function and are waiting for more finite Federal guidance from NIST and other working groups.

[23] 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.

In addition, we identified that two out of two agencies reviewed did not have an agency policy in place or the policy was missing NIST-required criteria.[24]

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

The Department did not provide a strategy or plan for developing an entity-wide continuous monitoring plan. OIG was provided a draft Continuous Monitoring Concept PowerPoint presentation which has yet to be implemented. As noted above, the Department is over 1 year past the date these plans and strategies were due to be implemented. Without an entity-wide continuous monitoring program, the Department cannot effectively detect compliance and determine if the complete set of planned, required, and deployed security controls for an information system continue to be effective over time, in light of changes that occur on an ongoing basis.

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 800-53, NIST 800-53A)? - No

We identified 24 of 254 systems where ongoing assessments of selected security controls had not been performed in FY 2012.[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.

In the FY 2010 FISMA report, we recommended that the Department develop ongoing assessments of selected security controls that agencies have performed, based on the approved continuous monitoring plans. OCIO has exceeded its estimated completion date of September 30, 2011.

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 POA&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 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 Plan of Action and Milestones (POA&M) additions. OCIO has exceeded its estimated completion date of September 30, 2011.

[24] NIST SP800-53 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.

[25] The 254 major applications were reported in CSAM as of October 2, 2012 at 8:49 a.m.

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 Standard baseline configurations defined? - Yes

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

2.1.3 Assessing for 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 4 of 13 agencies reviewed did not configure servers in accordance with the NIST requirements. Specifically, we found that over 50 percent of the settings on the Windows servers at two 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 have documented the reasons for those settings not being 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

[26] NIST SP 800-53, 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).

configurations for all approved software and hardware. Any changes to the baseline guides 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 CyberScope - FISMA Reporting? - No

We found that four of four agencies reviewed did not have a process for timely remediation of scan result deviations.[28] Specifically, OIG ran a commercially available vulnerability scan tool on 4,372 devices within the Department to verify that vulnerabilities were managed timely. We found 6,109 high and medium vulnerabilities were present and not corrected; 3,111 of these were over 6 months old. As a result, networks and devices within the Department are at increased risk of compromise.

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

NIST requires the organization to establish and document mandatory security configuration settings for information technology products employed within the information system. One such requirement is the Federal Desktop Core Configurations (FDCC) secure configurations for user workstations and laptops.[29] We found that two of three agencies reviewed did not fully implement FDCC secure configuration settings and document all deviations from baseline settings. Specifically, in the agencies tested we found a total of 1,175,172 FDCC settings that should have been implemented; however, 455,720 (38 percent) of the settings were not in compliance with FDCC standards. In one agency this was caused by moving to another environment that took much longer than anticipated. 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 to be an issue.

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

NIST requires the organization to document approve configuration-controlled changes to the system. We found 6 of 13 agencies reviewed had changes to hardware and software that were

[28] 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.

[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 (DoD), and the Department of Homeland Security (DHS).

not documented as required. Specifically in one agency, we found 11 of 18 change records had no documented approvals as required. As a result, malicious changes could be implemented in production systems without the knowledge of the approving official.

2.1.7 Process for timely and secure installation of software patches? - No

NIST requires the organization to identify and correct system flaws (known as vendor patches) and incorporate flaw remediation into the organizational configuration management process.[30] We found four of four agencies reviewed did not have an implemented process for timely and secure installation of software patches. Specifically, OIG found 397 high and medium vulnerabilities where the corrective action was to apply a vendor issued patch of which 246 were available for at least 6 months and the agency had not installed it.

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 the OCIO has exceeded its estimated completion date of June 15, 2011.

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

Department Manual 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 a 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 devices at all, and had not for over 9 months. Another agency only scanned 823 of 7,503 devices monthly. The agency only scanned 11 percent of its devices but reported 100 percent compliance to the Department.

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 to be an issue. In the FY 2010 FISMA report, OIG recommended that the Department ensure scanning for compliance to the baseline configurations and for vulnerabilities is performed as required by NIST. 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. No management decision has been reached for this recommendation.

[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 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 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 implement the recommended configuration settings. OIG found that 5 of 17 agencies reviewed did not remediate configuration vulnerabilities. Specifically, we found 2,799 configuration-related vulnerabilities on 195 network devices.[31] In addition, we found 1,055 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 not been reached.

2.1.10 Patch management process is fully developed, as specified in Organization policy or standards. (NIST 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 246 high and medium vulnerabilities were present on USDA devices where the patches were available for 6 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 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 800-53: AC-1)? - Yes

No exception noted. We found that the Department's current policy is substantially compliant and agencies' procedures met NIST SP 800-53.

3.1.2 Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 800-53, AC-2)? - Yes

No exception noted. We found that two out of the two agencies reviewed identified all users, including Federal employees, contractors, and others who access organization systems.

3.1.3 Identifies when special access requirements (e.g., multi- factor 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 two out of two agencies did not have multi-factor authentication properly implemented.[34] One agency stated it was not using the Departmental solution because of the length of time it currently takes for field users to receive their credentials.

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

We found that two of two agencies reviewed did not use multi-factor authentication linked to the Department's Personal Identification Verification (PIV) credentials program.[35] In addition, a contractor review found an additional agency that did not use multi-factor authentication that was linked to the PIV credentials program. One agency stated that it was not using it because many of its rural employees had difficulty receiving their PIV cards due to the employees' location. 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] Dual-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.

[35] 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 adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)? - Yes

No exception noted. OIG found that all agencies reviewed were able to provide Federal and Contractor employee HSPD-12 information regarding distribution of PIV cards.

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

OIG found that 2 of 17 agencies reviewed did not ensure that users were granted access based on need and separation of duties principles.[36] The agencies did not have automated mechanisms to enforce privileges or perform periodic reviews of user privileges and could not verify if account privilege reviews were performed by an authorized individual and followup occurred when necessary. As a result, accounts have excessive privileges which may result in the unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

3.1.7 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 two of two agencies reviewed were able to provide evidence that their Identity and Access Management program identified devices with Internet Protocol addresses that are attached to the network.

3.1.8 Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that 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.

3.1.9 Ensures that accounts are terminated or deactivated once access is no longer required? - No

OIG found that 5 of 16 agencies did not ensure that accounts were terminated or deactivated once access was no longer required. We found 363 separated users in two agencies that still had active accounts. One agency stated that its goal was to keep the separated employees with active accounts to less than 3 percent. Department policy states that accounts should be disabled within

[36] Separation of duties is the concept of having more than one person required to complete a task, which helps prevent fraud and error. The concept of least privilege states that employees must be able to access only the information and resources that are necessary to complete their legitimate role or function.

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.

3.1.10 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 800-53: IR-1)? - No

USDA Incident Handling policies and procedures were unchanged from our findings during the FY 2011 FISMA review. During FISMA 2011, we found that the Department policy met all of the NIST requirements.[37] However, our review in FY 2011 identified that the day-to-day procedures were not accurately reflected in the documented Agriculture Security Operations Center (ASOC) Standard Operating Procedure (SOP).[38] As an example, we determined the SOP did not include the updated versions of incident checklists utilized by the incident response team. FY 2012 testing found no changes in the procedures. In addition, we determined that three of the three agencies tested for FISMA or during other audits did not have procedures that were fully developed or sufficiently detailed.

In the FY 2011 FISMA report, OIG recommended that the Department update its incident handling procedures to reflect current practice. No management decision has been reached.

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

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

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

Our review of incidents found that 32 of 75 were not handled in accordance with Departmental procedures.[39] Based on our overall sample results we estimate that 351 incidents (42.6 percent of the universe) were not handled in accordance with Departmental procedures.[40] 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 4 of the 32 incidents had either incomplete incident documentation or did not include the required documentation outlined in the procedures. For example, two of the checklists did not complete the Personally Identifiable Information (PII) checklist required.[41]

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

US-CERT requires USDA to notify them of incidents within specified timeframes, based on the category of the incident.[42] We reviewed a statistical sample of incidents that disclosed USDA had not reported 31 of 75 incidents to US-CERT within the required timeframe, 18 of which were the result of a lost or stolen device that was not promptly reported to OCIO's Incident Handling Division (IHD).[43] Based on our overall sample results, we estimate that 340 incidents (41.3 percent of the universe), were not reported to US-CERT as required.[44] For example, US-CERT requires that lost or stolen equipment incidents be reported within one hour; however, we found that an agency did not report a lost equipment incident to IHD (to forward to US-CERT) for 213 days.[45]

[39] We based our sample size on a 30 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 75 incidents for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

[40] We are 95 percent confident that between 261 (42.6 percent of the universe) and 441 (53.6 percent of the universe) FY12 incidents were not handled in accordance with departmental procedures. Additional sample design information is presented in Exhibit B.

[41] PII 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.

[42] 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 the Department of Homeland Security (DHS). NCSD was established by DHS to serve as the Federal Government's cornerstone for cyber security coordination and preparedness.

[43] We based our sample size on a 30 percent error rate and desired absolute precision of +/-10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 75 incidents for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

[44] We are 95 percent confident that between 251 (30.5 percent of the universe) and 430 (52.2 percent of the universe) incidents in FY12 were not reported to US-CERT as required. Additional sample design information is presented in Exhibit B.

[45] 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.

4.1.4 When applicable, reports to law enforcement within established timeframes (SP 800-86)? - Yes

No exception noted. We determined all incidents were properly reported to law enforcement officials when applicable.

4.1.5 Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage. (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)? - Yes

No substantial exception noted. The Departmental procedures require that if an incident is not closed after 30 days, the agency is required to open a POA&M.[46] OIG found that 1 of the 75 incidents was not resolved in a timely manner, and a POA&M was not created as required, when the incident remained open for more than 30 days. We consider this question to be substantially met.

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 Service Agreement and Incident Plan, we determined that USDA is not capable of managing risks in a virtual/cloud environment.[47] USDA lacks the ability to track cloud traffic, the cloud e-mail solution does not have its own Data Loss Prevention (DLP) solution deployed, and the service agreement between the USDA and its cloud service provider does not include the appropriate detail outlining the roles and responsibilities for each party.[48] A new Federal initiative requires agencies and cloud service providers to stipulate any specific incident reporting requirements, including who and how to notify the agency.[49] USDA's current cloud service providers are required to become compliant by June 2014.

[46] 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 in meeting the task, and scheduled completion dates for the milestones. The goal of a POA&M should be to reduce the risk of the weakness identified.

[47] 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.

[48] 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."

[49] 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 the Federal Information Security Management Act of 2002 (FISMA).

In the FISMA 2011 report, OIG recommended the Department deploy adequate resources to monitor and configure new security tools and then adequately report and close the related incidents. This recommendation has not reached management decision.

4.1.7 Is capable of correlating incidents? - No

Based on our testing, we determined that, although the Department has the capability to correlate incidents for the incident response and reporting within USDA, the current security tools do not see nor capture all network traffic. Additionally, the Department's correlation tool was not fully configured and capable of correlating incidents during FY 2012. As noted in an audit during FY 2012, USDA purchased security tools in FY 2010 and 2011 without proper planning and configuration.[50]

4.1.8 There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)? - Yes

No exception noted. Our review of the Department's incident monitoring and detection coverage determined the Department 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.

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

5.1.1 Documented and centrally accessible 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 developed risk management policy. The Department does have procedures that are centrally accessible but are lacking required elements, such as descriptions of roles and responsibilities of participants in the Risk Management Framework

[50] Audit Report 88401-01-12, *Audit of the Office of the Chief Information Officer's FYs 2010 and 2011 Funding Received for Security Enhancements* (August 2012).

(RMF) guide.[51] In addition, the Department has not addressed step six of the RMF process which is monitoring security controls. According to USDA, this occurred due to lack of resources for policy development and because the Department is in the process of making revisions and addressing missing requirements and enhancements to the procedures. Without a policy and adequate procedures, 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 not been reached.

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 800-37, Rev.1? - No

The Department does not have an organizational-wide risk management strategy developed that addresses risk from an organization 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 at the organizational perspective, as described in NIST 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, and an organizational risk management strategy. Therefore, it has not defined the risks from a mission and business process perspective in order to address them from an organizational perspective.

5.1.4 Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 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.

[51] USDA *Six Step Risk Management Framework Process Guide*, dated July 2011. NIST Special Publication 800-37 revision 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.

5.1.5 Categorizes information systems in accordance with government policies? - No

We generated a report from Cyber Security Assessment and Management (CSAM) which identified the impact level for each of the Department's systems.[52] The report included the impact levels for Confidentiality, Integrity, and Availability, which were categorized as high, moderate, and low. We compared the generated report to the recommendations in NIST and found 18 of 257 systems indicated a lower rating than was recommended without adequate justification for the reduction in categorization level.[53] Systems were not properly categorized. NIST requires that any adjustments to the recommended impact levels be documented and include justification for the adjustment.

5.1.6 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 controls required. Therefore, the incorrect categorization noted in 5.1.5 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 over protecting the information system (thereby wasting valuable security resources), or under protecting the information system and placing important operations and assets at risk.

5.1.7 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 5.1.5 led to inadequate controls being implemented for those 18 systems.

5.1.8 Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system? - No

We found that security controls are not implemented correctly. Specifically, the security controls were not implemented properly and did not sufficiently address each control. For example, for 6 of 11 systems, the control involving Security Awareness Training was described

[52] 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.

[53] The 257 major applications were reported in CSAM as of August 8, 2012. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Vol. 1 (August 2008).

as an inherited control. However, this control could not be inherited because procedures had to be developed by the agencies as required by Departmental policy. Additionally, we found controls that had not been assessed; and the agencies did not document reasons for the controls not being assessed.

5.1.9 Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable? - No

The Department does not authorize information system operation based on a determination of the risk to organizational operations and assets. We reviewed the Department's inventory of 251 FISMA reportable systems and found a parent system identified as in development, but this system had three child systems that were operational without Authorities to Operate (ATO).[54] We found six additional systems that were operational with no ATO.[55] Furthermore, the Department has 22 systems with expired ATOs, one system being CSAM, the Department's system repository. This occurred because the Department felt that the systems needed to be operational for business needs. As a result, the Department's organizational operations and assets are vulnerable.

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.[56] This recommendation reached final action; however, we found that the same issue still exists.

5.1.10 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 25 of 254 systems where ongoing assessments of selected security controls had not been performed in FY 2012.[57]

[54] Total number of systems generated out of CSAM as of October 1, 2012.

[55] A parent system owns, manages, and/or controls the child system. System inventory as of October 1, 2012.

[56] 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.

[57] The 254 major applications were reported in CSAM as of October 2, 2012 at 8:49 a.m.

5.1.11 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, and an organizational risk management strategy with defined risks in place. Therefore, we were unable to determine if the information specific risks were communicated to appropriate levels of the organization.

5.1.12 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.

5.1.13 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? - No

As noted in 5.1.1-5.1.4, the Department does not have a policy, adequate procedures, a governance structure, or an organizational risk management strategy with defined risks. Therefore, we were unable to determine if there is 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.

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

The System Security Plans (SSP) we reviewed were inadequate and not in accordance with Government policies.[58] We found 11 of 11 SSPs failed to meet the minimum security requirements required by NIST 800-53. Specifically, 6 of 11 of the systems' security controls did not include sufficient support for implementation. For instance, we found controls that had not been assessed and did not have evidence to support why the controls were not assessed.

The Department's Security Assessment Reports (SARs) we reviewed failed to meet the minimum security required by NIST SP 800-37.[59] Specifically, NIST SP 800-37 requires a Security Assessment Plan (SAP) to be included with the SAR, which provides the objectives for

[58] 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 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).

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

the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. We found during our review three of the three SAPs that had fully completed the 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.

5.1.15 Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies? - Yes

No exception noted. During our review of the security authorization packages (which include the SSP) to verify that system accreditation boundaries were accurately defined in accordance with Government policies, we found that 11 of 11 packages adequately explained the system boundaries.

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 800-53: AT-1)? - No

We determined the Department's and two of two agencies' security awareness policies met the requirements outlined in NIST SP 800-53.[60] In addition, the Department's security awareness training procedures met the requirements of NIST SP 800-53. However, one of the two agencies we reviewed during this audit did not have adequate procedures in place to ensure employees and contractors received adequate security awareness training.

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

[60] Departmental SOP, *Information Security Training, SOP-ISD 022* (October 7, 2008) and *Information Security Awareness Training, SOP-CPPO-018* (April 21, 2011).

has exceeded the estimated completion date of September 30, 2012.

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 were not fully developed or sufficiently detailed.[61] Specifically, we found the Department's policy for specialized training did not include a definition of significant information security responsibilities. The Department's policy is currently in draft and was not released as of September 30, 2012. A guidance memo/bulletin was sent to the agencies on how to identify employees who need to complete the specialized training. Both agencies reviewed are following this memo until the official policy is developed and finalized.

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 is still open; OCIO has exceeded its estimated completion date of September 30, 2011.

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 45 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 Rev 3 requires agencies to document and monitor individual information system security training activities and to retain individual training records. During our review of the two agencies, we found 2 of 9,507 users (less than 1 percent) with login privileges without evidence that the users had completed the annual security awareness training. We considered this to have substantially met the requirements.

[61] 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 2010 FISMA report, OIG recommended that the Department ensure its training repository is completely populated to ensure all required personnel receive the required training. This recommendation is still open; OCIO has exceeded its 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 exception noted. NIST SP 800-53 requires agencies to provide role-based training. Agencies are 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 45 employees with significant security responsibilities found all 45 employees from the 2 sampled agencies had adequate role-based training to meet NIST requirements and had documented evidence of specialized training attendance.

6.1.6 Training material for security awareness training contains appropriate content for the Organization (SP 800-50, SP 800-53)? - Yes

No exception noted. We found that the training material for the security awareness 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 requiring remediation? - No

The Department's security manual did not include a policy establishing a POA&M process for reporting IT security deficiencies and for tracking the status of remediation efforts. The Department stated that it was in the process of finalizing a draft policy. In addition, the two agencies reviewed did not have POA&M policies. Instead, the agencies stated that they followed the Department's policy; however, the Department had not published an official POA&M policy.

Additionally, although there were no formal policies, the Department does have established procedures. Our review of the POA&M SOP determined it was updated to include OMB 04-25 outlined criteria, and that it reflected the current POA&M process.[62] However, we found that both of the selected agencies did not have established POA&M procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.

In the FY 2010 FISMA report, OIG recommended that the Department develop POA&M policy and procedures that adhere to Federal requirements. The policy and procedures should include detailed instructions for the use of CSAM, an effective closure review process, and periodic reviews of the information in CSAM. Final action was achieved May 30, 2012. However, we found the Department's POA&M policy is still in draft and not yet finalized.

7.1.2 Tracks, prioritizes and remediates weaknesses? - Yes

No exception noted. We found the Department's POA&M program 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. 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. We found all POA&Ms, as of September 12, 2012, had an identified priority level. Additionally, we determined that weaknesses were remediated throughout the fiscal year.

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 69 POA&Ms that were closed during FY 2012, and found 11 were closed without documented remediation plans.[63] Based on our sample results, we estimate 176 POA&Ms (15.9 percent of the universe) were closed in FY 2012 with remediation actions that did not sufficiently address the identified weaknesses in accordance with Government policies.[64] Additionally, of the POA&M closures reviewed by the Department, 17 of 94 closures were not acceptable, due to insufficient documentation to support remediation or the closure procedures were not followed.

[62] Departmental SOP, *Plan of Action and Milestones Management SOP* (June 29, 2011).

[63] 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 69 POA&Ms for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

[64] We are 95 percent confident that between 81 (7.4 percent) and 271 (24.5 percent) of closed POA&Ms in FY12 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.

In the FY 2009 FISMA report, OIG recommended that the Department develop and implement an effective process to ensure POA&Ms are entered, tracked, and closed properly. The process should include the required link to budgetary resources. Final action was achieved on May 30, 2012; however, we continue to find that POA&Ms are not being closed properly. Additionally, in order to achieve final action OIG stated that OCIO needed to provide copies of the CSAM User's Guide and the POA&M policy. However, we found the Department's POA&M policy is still in draft and not yet finalized.

7.1.4 Establishes and adheres to milestone remediation dates? - No

We found that 995 of the 3,606 (28 percent) milestones completed in FY 2012 were not completed by the planned milestone finish date. We found that milestone dates are being established but the remediation dates are not always adhered to.

7.1.5 Ensures resources are provided for correcting weaknesses? - No

We found weaknesses that were not being remediated due to inadequate resources. We identified 228 delayed POA&Ms as of September 12, 2012. We determined 53 of the 228 POA&Ms were delayed due to inadequate resources for one of the following reasons:

- Funds not allocated or insufficient funding;
- Personnel shortage; or
- Assigned funds withdrawn.

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and requiring 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.[65] The Department's SOP requires an agency to create a POA&M when an identified weakness cannot be remediated within 30 days. However, we found POA&Ms had not been created for the 10 FY 2011 FISMA Departmental audit recommendations. Also, an internal control audit identified one agency that was not creating POA&Ms for vulnerabilities identified from scan results.

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 27 of 532 (5 percent) POA&Ms that did not have costs associated. Because of the significant progress the Department has made (down from 38 percent in FY 2011) we consider the FY 2012 number to be insignificant.

[65] OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

7.1.8 Program officials and contractors 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, and OMB M-04-25)? - No

The Department's SOP requires that a POA&M closure review be performed at least once per quarter. This includes a review of all closed POA&Ms resulting from a GAO or OIG audit. In addition, the Department is required to review another 10 percent of non-audit related, closed POA&Ms. We found the required reviews were not being completed by the Department. For example:

- OCIO was not completing a quarterly review of closed POA&Ms as required by its SOP;
- OIG found that not all closed POA&Ms resulting from a GAO or OIG audit were subjected to the closure review process; and
- OIG found that the Department had not met the requirement to review a minimum of 10 percent of all closed non-audit POA&Ms.

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 has not reached 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 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. There were two policy areas that were not addressed in the Departmental policy as outlined by NIST.[66] 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 fully developed. This occurred because

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

they both depended on the Departmental policy which was not sufficient. 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 a 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? - No

We found, or the agencies self-reported, that three out of three agencies' remote access programs were not protected against unauthorized connections or subversion of authorized connections. This occurred because they either relied on their general network access logging to capture events or they had logs and were unable to provide any documentation that log reviews had occurred.

8.1.3 Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1)? - No

We found two agencies out of the two reviewed were not using multi-factor authentication for remote access as required, which hampers the program from uniquely identifying and authenticating users. This occurred because the Departmental solution had not been implemented and the telework policy was insufficient.

8.1.4 Telecommuting policy is fully developed (NIST 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 the two agencies reviewed did not have a fully developed telecommuting policy. This occurred because the agencies 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; 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 800-46, Section 2.2, Section 3.3)? - No

DR 3505-003 specifies that agencies will implement multi-factor authentication for all forms of remote access to agency information systems. We found, or agencies self-reported, that while multi-factor authentication for remote access is required by Departmental policy, four of the four agencies reviewed did not have it properly implemented. This occurred because there are several problems with going exclusively to PIV cards and agencies are using alternative solutions. One issue with the cards is it can take weeks for new employees, or existing employees who lose their cards, to receive a new one.

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 PIV cards for remote access authentication, it would satisfy all the NIST requirements, including strength mechanisms.[67] As reported in item 8.1.5 above, we found that while multi-factor authentication for remote access is required by Departmental policy, four agencies of the four 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 the two agencies reviewed had defined and implemented encryption requirements for information transmitted across public networks.

8.1.8 Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re- authentication are required? - Yes

No exception noted. We reviewed two agencies' remote access session time-out settings and found they were compliant with OMB, and timed-out after 30 minutes of inactivity, after which re-authentication was required.[68]

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST 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 that 18 of 20 incidents of lost or stolen remote access devices were not reported appropriately within the required timeframe.

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

No exception noted. We reviewed two agencies' rules of behavior agreements, and found they

[67] NIST SP 800-63, *Electronic Authentication Guideline* (April 2006).
[68] OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

were in accordance with Government policies.

8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 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.

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 800-53: CP-1)? - No

NIST SP 800-53 states that the organization should develop, disseminate, and review/update a formal, documented contingency planning policy. We found that the Department's contingency planning policy did not meet these requirements. For example, the policy did not address alternate telecommunications providers. This occurred because the Department's policy has not been updated with the new NIST elements.

In the FY 2010 FISMA report, we recommended that the Department ensure that agencies have developed effective contingency planning policy and procedures in accordance with NIST. The policy and procedures should address suitable alternate processing sites, backup tape storage locations, and backup testing. OCIO has exceeded its estimated completion date of September 30, 2011. The Department has stated that it has updated the template and it is currently in the approval process. In the FY 2011 FISMA report, OIG recommended that the Department update the contingency plan template to adequately address all NIST 800-34 requirements.[69] The recommendation is still open; OCIO has exceeded its estimated completion date of September 30, 2012. However, OCIO stated that Cyber Policy and Oversight (CPO) are in the process of drafting a new contingency plan policy to comply with NIST requirements and officials stated

[69] NIST SP 800-34, *Contingency Planning Guide For Federal Information Systems* (May 2010).

that they are actively working on the template.[70]

9.1.2 The Organization has performed an overall Business Impact Analysis (BIA) (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. The Department's guide on developing contingency plans requires that a BIA be completed for each system. We found one of two agencies did not have a BIA for any of its systems.

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

We found all contingency plans—18 of 18 from our sampled agencies—had addressed the key information required by NIST SP 800-34.

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 plan's effectiveness, and the organization's readiness to execute the plan, and initiate corrective actions. We identified 42 of 247 systems for which USDA system contingency plans had not been tested or for which documentation had not been updated during FY 2012.[71]

9.1.5 The documented business continuity and disaster recovery plans 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 could not be implemented when necessary. For example, four of eight contingency plans we reviewed had not completed testing or fully developed training plans and exercises. Also, 9 of 58 sampled systems from the Department did not have evidence of effective ongoing testing.[72] Based on our sample results, we estimate that 32 (15.5 percent of the universe) systems in our universe did not have evidence of ongoing testing.[73]

[70] USDA *Contingency Plan Template* (March 2011).

[71] The 247 major applications were reported in CSAM as of October 2, 2012.

[72] We selected a simple random sample of 58 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 30 percent error rate with +/-10 percent precision. Additional sample design information is presented in Exhibit B.

[73] We are 95 percent confident that between 15 (7.4 percent) and 48 systems (23.6 percent) are non-compliant with this criterion. Additional sample design information is presented in Exhibit B.

9.1.6 Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53)? - 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 plan's effectiveness, and the organization's readiness to execute the plan and initiate corrective actions. However, we found that, of the 8 systems from two agencies, 4 had not fully implemented training, testing, and exercise programs.

9.1.7 Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans 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 and to review the contingency plan test/exercise results and initiate corrective actions. We found that one of our selected agencies did not have documented evidence of its contingency plan tests. The other agency had 7 of 15 systems with persistent issues that were not being remediated from year to year after contingency plan testing.

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, which includes actions taken, and problems encountered during recovery and reconstitution efforts. An after-action report with lessons learned should be documented and updated. Our review found one of two agencies 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)? - No

NIST SP 800-53 requires alternate processing sites to be established for information systems in case of a disaster. We sampled 58 systems and found 3 of those systems did not meet the requirement to provide an alternate processing site.[74] Based on our sample results, we estimate that 11 systems (5.2 percent of the universe) in our universe did not meet the requirements to provide an alternate processing site.[75]

In the FY 2010 FISMA report, we recommended that the Department ensure that all required contingency planning documents are in CSAM, and all required fields are properly populated. This should include recovery strategies, plans, and procedures, as well as testing, training, and

[74] We selected a simple random sample of 58 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 30 percent error rate with +/-10 percent precision. Additional sample design information is presented in Exhibit B.

[75] We are 95 percent confident that between 3 (actual found; 1.5% percent of audit) and 21 systems (10.1 percent) are non-compliant with this criterion. Additional sample design information is presented in Exhibit B.

exercise results. As part of this recommendation, we also suggested that the Department periodically review CSAM to ensure compliance. OCIO has exceeded its estimated completion date of September 30, 2011.

9.1.10 Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53)? - No

As noted in 9.1.9, we found 3 of 58 systems did not have alternate processing sites. Based on our sample results, we estimate that 11 systems (5.2 percent of the universe) in our universe did not meet the requirements to provide an alternate processing site.[76]

9.1.11 Backups of information are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53)? - No

NIST SP 800-53 states that the organization should conduct user-level, system-level, and information system documentation backups. We found 4 of 12 agencies reviewed by OIG, independent contractors, and during annual agency self-assessments had not performed backups in a timely manner. For example, three systems from one agency had failed backups. For one of those systems the backup was not completed successfully until three days later and another was not completed at all for the requested date.

9.1.12 Contingency planning that consider supply chain threats? - No

We found contingency plans in one of two agencies we tested did not consider its supply chain threats. This occurred because Disaster Recovery Plans had not been completed.

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 exception noted. OIG was able to observe two different contingency plan table top exercises. Both exercises were successful at noting issues that need to be addressed and were positive training opportunities for those involved. There were no major issues to report. However, it should be noted that the facilitator for one exercise incorrectly suggested to the participants that live events be recorded and written up in the form of after-action reports so that they did not have to complete contingency plan testing each year. One agency self-reported that it did not meet the NIST requirements to provide initial contingency planning training to personnel; it failed to define the training frequency and to provide refresher training.

[76] We are 95 percent confident that between 3 (actual found; 1.5% percent of audit) and 21 systems (10.1 percent) are non-compliant with this criterion. Additional sample design information is presented in Exhibit B.

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 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 the 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. These 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 2 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? - No

As noted in 10.1.3 below, we found operational contractor systems in CSAM that did not have a current ATO, did not sufficiently document its interconnections, or did not have a signed SSP. Based upon 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 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 public cloud. We found one contractor system was not in the Department's inventory, four contractor systems had insufficient interconnection documentation, and one cloud system was in production for 15 months before being documented in CSAM. We also reviewed a random sample of 40 non-contractor systems and found 10 had insufficient interconnection documentation.[77] Based on our sample results, we estimate 57 non-contractor systems (25.0 percent of the universe) had insufficient interconnection documentation.[78]

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 30, 2011.

10.1.4 The inventory identifies interfaces between these systems and Organization-operated systems (NIST 800-53: PM-5)? - No

We reviewed interconnection documentation for 10 operational and reportable contractor systems in CSAM and found that 4 did not have adequately identified or documented interfaces in CSAM.

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 30, 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.

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 four contractor systems that did not have adequately identified or documented interfaces in CSAM.

[77] We based our sample size on a 15 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 40 systems for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

[78] We are 95% confident that between 28 (12.3 percent) and 85 (37.7 percent) non-contractor systems may have insufficient interconnection documentation in CSAM. Additional sample design information is presented in Exhibit B.

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

We found that the inventory reconciliation had not been performed for 3 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 30, 2011.

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

We found eight contractor systems with expired ATOs, four contractor systems with missing interconnection agreements, and five contractor systems with missing SSP signatures. We also found a cloud system with incomplete documentation and another that was not included in the Department's inventory.

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? - No

We reviewed Capital Planning policies and procedures at the Departmental and agency levels to determine if all critical elements were included in the documents. One of seven criteria identified in the OMB A-11 and NIST 800-65 guidance was not included in the Departmental Manuals. This occurred because the Capital Planning Division (CPD) was not aware the criteria needed to be included in the Departmental policy. As a result, agencies lack formal guidance on the definition of a major information technology investment. The CPD has updated its policy guidance to incorporate the regulatory criteria missing; however, as of October 1, 2012, CPD had not implemented the updated policy.

Additionally, our review of CPIC policy and procedures at the agency level determined that one of two agencies was not adhering to the appropriate Departmental policies pertaining to information technology capital investments.

In the FY 2011 FISMA report, OIG recommended that the Department update its Capital Planning policies to incorporate a definition of a "major IT investment" so that agencies have a documented description to use. The recommendation is still open; OCIO has exceeded its estimated completion date of September 30, 2012.

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 the two selected agencies as part of the annual budgeting process.[79] 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 two of the two agencies selected for testing could not provide adequate supporting documentation for the amounts submitted on their annual Exhibit 53B. This occurred because the agencies were unaware of the need to retain adequate supporting documentation used for the budgeting process. As a result, USDA lacks justification for the IT security costs portion of its budgetary request.

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

We reviewed the Exhibit 53B documentation submitted by USDA and the two selected agencies as part of the annual budgeting process. Our testing determined USDA's security capital planning and investment program establishes a discrete line item for information security in organizational programming and documentation based on information submitted on the Exhibit 53Bs by USDA and agencies selected for testing. However, as noted in 11.1.2, detailed testing determined two of the two agencies selected could not provide supporting documentation for the amounts submitted on their annual Exhibit 53B.

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

We reviewed a sample of Exhibit 300 documents submitted by agencies within USDA to verify that the Exhibit 300 was accompanied by OMB required supporting documentation.[80] Our testing determined that USDA does not consistently employ business cases across Exhibit 300s based on the absence of required documentation for four of the six Exhibit 300s reviewed. As a result, the Major IT investments within USDA lack the required supporting documentation that outlines the investments planning, funding, and implementation progress. This occurred because

[79] 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).

[80] Exhibit 300s 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).

the CPD did not require all supporting documentation to be submitted.

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 two 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 agency 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 all supporting documentation to be submitted. 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 50501-0003-12. 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' IT programs, and compliance with FISMA;
- Agencies' system of internal controls over IT assets;
- Department's progress in establishing a Departmentwide security program, which includes effective assessment and authorization;
- 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. Statistical sampling was incorporated in four FISMA areas, and each of the four areas was represented by a different universe. The specific designs are summarized below for each of the four audit areas.

1. Incident Response and Reporting

Universe:

The audit universe consisted of 823 incidents reported for FY 2012, as of April 3, 2012. Each incident had a unique identifier (incident number) and was categorized based on incident type into 1 of 8 categories. A listing and counts of the different categories are presented in the sample design section below.

Sample Design:

Each 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.

We selected a simple random sample of 75 incidents for review. The sample size of incidents was based on an error rate of 30 percent and a desired absolute precision of +/-10 percent of the audit universe, when reporting a 95 percent confidence level.

The resulting sample design and universe counts are summarized in the table below.

Table 1: Incidents universe and sample counts by category

Incident Type	Universe	Sample
USCERT CAT0 - Exercise/Network Defense Testing Count	124	10
USCERT CAT1 - Unauthorized Access Count	46	4
USCERT CAT3 - Malicious Code Count	225	18
USCERT CAT4 - Improper Usage Count	11	1
USCERT CAT5 - Scans/Probes/Attempted Access Count	19	2
USCERT CAT6 - Investigation Count	77	7
USDA CAT8 (USCERT CAT1) - Loss, Theft, Missing Count	199	20
USDA CAT9 - Block List Count	122	13
Total:	823	75

Results:

Results are projected to the audit universe of 823 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.[81]

The audit team tested a variety of criteria--Did the incident:

- Include the required PII checklist?
- Get reported to US-CERT within the required timeframe?
- Include the proper checklist and was it completed correctly, and; if not complete, did IHD accept the incident?
- Include a fully completed Incident Identification Form?
- Include the required incident category checklist?
- Have a POA&M created if it was open for over 30 days?

We used a projection for whether all checklists were completed, as required by SOP, and an overall projection, which was based on the number of incidents found in our sample with at least one exception, based on all criteria tested. We are reporting actual findings for the rest of the criteria tested.

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

[81] Scheaffer, Mendenhall, Ott, *Elementary Survey Sampling*, Fourth Edition (Chapter 5), Duxbury Press, c1990.

Table 2: Incident Response and Reporting Projections

Description of estimate for tested criteria	Estimate	Standard Error	95% Confidence Interval		Coefficient of Variation	Population Size	Sample Size	Achieved Precision
			Lower	Upper				
Incidents that were not reported to US-CERT within the required timeframe.	340	44.914	251	430	.132	823	75	11%
Incidents with at least one exception in all criteria tested	351	45.111	261	441	.128	823	75	11%

Based on our sample results:

- We estimate that 340 incidents (about 41 percent of the audit universe) were not reported to US-CERT within the required timeframe. We are 95 percent confident that between 251 (30 percent) and 430 (52 percent) incidents in the audit universe are non-compliant with this criterion.
- We estimate that 351 incidents (about 43 percent of the audit universe) had at least one exception in the tested criteria. We are 95 percent confident that between 261 (32 percent) and 441 (54 percent) incidents in the audit universe were not handled in accordance with Departmental procedures.

2. POA&Ms

POA&Ms (Closed)

Universe:

The universe of POA&Ms consisted of 1,106 closed POA&Ms.

Sample Design:

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 69 POA&Ms for review, and selected them by choosing a simple random sample.

Results:

Results for all criteria are projected to the audit universe of 1,106 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.[82]

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

Table 3: POA&M (closed) Projections

Description of estimate for tested criteria	Estimate	Standard Error	95% Confidence Interval		Coefficient of Variation	Population Size	Sample Size	Achieved Precision
			Lower	Upper				
POA&Ms with remediation actions that did not sufficiently address the identified weaknesses.	176	47.542	81	271	.270	1106	69	9%

Based on our sample results, we estimate that 176 (about 16 percent of the universe) POA&Ms in our universe had remediation actions that did not sufficiently address the identified weaknesses. We are 95% confident that between 81 (7 percent) and 271 (25 percent) POA&Ms in the audit universe are non-compliant with this criterion.

3. System / Contingency Planning

Universe:

Our universe consisted of 204 FISMA reportable systems for all agencies within USDA that were reviewed as of August 25, 2012. Each system is to have a contingency plan that contains very specific recovery information for the agency in the event of a disaster.

Sample Design:

We selected a simple random sample of 58 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 30 percent error rate, with +/-10 percent precision. Our simple random sample included at least one contingency plan from each agency, so we did not use stratification.

Results:

The audit team reviewed the 58 system contingency plans selected in the sample. Results are projected to the audit universe of 204 systems. Achieved precision, relative to the universe, is reported for each criterion. The corresponding lower and upper bounds of the 95 percent

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

confidence interval are also included. For two criteria, 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.[83]

Projections are shown in the Table 4. 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	Population Size	Sample Size	Achieved Precision
			Lower	Upper				
Systems that did not have evidence of CP testing.	28	7.882	12	44	.280	204	58	8%
Systems that did not have evidence of ongoing testing.	32	8.276	15	48	.261	204	58	8%
Systems that did not meet the requirements to provide an alternate processing site.	11	5.063	3*	21	.480	204	58	5%

* Actual number found.

Based on our sample results:

- We estimate that 28 (about 14 percent of the universe) systems in our universe did not have evidence of Contingency Plan testing. We are 95 percent confident that between 12 (6 percent) and 44 systems (22 percent) are non-compliant with this criterion.
- We estimate that 32 (about 16 percent of the universe) systems in our universe did not have evidence of ongoing testing. We are 95 percent confident that between 15 (7 percent) and 48 systems (24 percent) are non-compliant with this criterion.
- We estimate that 11 systems (about 5 percent of the universe) in our universe did not meet the requirements to provide an alternate processing site. We are 95 percent confident that between 3 (actual number found, which represents about 1.5 percent of the universe) and 21 systems (10 percent) are non-compliant with this criterion.

[83] Ibid.

4. Non-contractor systems in CSAM

Universe:

Our universe consisted of 226 non-contractor systems found in CSAM that were operational and FISMA-reportable. We excluded systems from two agencies included in the FISMA review – the Agricultural Research Service and the Foreign Agricultural Service, as well as any OIG systems. The two agencies in the FISMA review were excluded because we had already reviewed 100 percent of those systems as part of the audit.

Sample Design:

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

Results:

The audit team reviewed all 40 systems selected in the sample and found none that were misidentified. Based on this result, we are 95% confident that less than 7% of the systems in our audit universe might be misidentified.

Auditors reviewed documentation and found 10 non-contractor systems with insufficient interconnection documentation. Based on this sample result, we project that 57 systems in the universe of 226 have this issue. We are 95% confident that between 28 and 85 non-contractor systems may have insufficient documentation. The table below shows the parameters for this projection:

Description of estimate for tested criteria	Estimate	Standard Error	95% Confidence Interval		Coefficient of Variation	Population Size	Sample Size	Achieved Precision
			Lower	Upper				
Systems with insufficient interconnection documentation	57	14.216	28	85	.252	226	40	13%

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

Email: usda.hotline@oig.usda.gov
Phone: 800-424-9121   Fax: 202-690-2474

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