U.S. Department of Agriculture
Office of Inspector General

Audit Report

U. S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2010 Federal Information Security Management Act

Audit Report 50501-02-IT
November 2010

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

DATE: November 15, 2010

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

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2010 Federal Information Security Management Act Report (Audit Report 50501-2-IT)

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 /s/
Inspector General

Table of Contents

U. S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2010 Federal Information Security Management Act (FISMA) (Audit Report 50501-02-IT)

Executive Summary

Improvements have been made in the Department's information technology (IT) security in the last decade; however, many longstanding weaknesses remain. Since 2001, the Office of Inspector General (OIG) has reported material weaknesses in the design and effectiveness of the Department's overall IT security program. The Department of Agriculture (USDA) is a large and complex organization, including 31 separate agencies and staff offices, each with its own IT infrastructure. In 2009, we reported that in order to mitigate the continuing material weaknesses, the Department should rethink its policy of attempting to simultaneously achieve numerous goals in short timeframes. We recommended that the Department and its agencies, working in cooperation, define and accomplish one or two critical objectives prior to proceeding to the next set of priorities. During fiscal year (FY) 2010, we saw some evidence of coordination; however, we did not observe that the Department was making measurable progress in approaching this problem collaboratively. OIG continues to consider this change in direction the best course of action for the Department.

To begin mitigating these weaknesses, the Department developed several plans throughout the year. Once these plans become defined initiatives and are implemented, along with the required policies, procedures, and a continuous monitoring component, the security posture of the Department and its agencies should improve. One of the Department's initiatives was the 2010 Cyber Security Summit. This successful summit provided outreach and education to USDA executives, and to program and technical staff that were in attendance.

In addition, the Department was successful in the initial deployment of a software solution that provides real-time, continuous visibility and control for over 140,000 workstations and servers on its network. When complete, this system of security tools should allow the Department to enforce continuous compliance, respond in real time to threats anywhere on the network, and streamline multiple IT processes. In addition, the Department deployed a suite of network monitoring and detection tools at fiscal year-end, which should further enhance the security of USDA's networks. The suite is an integrated security solution, providing the foundation for enterprise-wide security monitoring, detection, and protection. Once these projects are completely implemented and continuous monitoring occurs, USDA's security posture should be greatly improved. The Department is also in the pilot stages of a solution that should help to mitigate the significant weaknesses in identity management that agencies have reported in their annual self-assessments.

This report constitutes OIG's independent evaluation of the Department's IT security program and practices, as required by the Federal Information Security Management Act (FISMA). OIG's review is based on Office of Management and Budget (OMB)-provided questions for the FY 2010 FISMA review, which are designed to assess the status of the Department's security posture in FY 2010. For the FY 2010 FISMA review, OMB's framework requires us to audit

processes, policies, and procedures that had already been implemented and documented, and were being monitored. While the Department's many planned activities may improve its security posture in the future, the planned initiatives could not be evaluated as part of the FY 2010 FISMA review because they were not fully operational at the time.

The following summarizes the key matters discussed in Exhibit A of this report. Exhibit A contains OIG's responses to the OMBs questions. The questions were defined in OMB Memorandum M-10-15, *Fiscal Year 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated April 21, 2010. The universe of systems and agencies reviewed varied during each audit or review reflected in this report. As part of FISMA, OIG reviewed systems and agencies, OIG contractors, agency annual self-assessments, and various OIG audits throughout the year. Since the scope of each review and audit differed, we could not use every review or audit to answer each question.

Agency officials are responsible for ensuring all systems meet Federal and Departmental requirements and documenting their agency's compliance in the Cyber Security Assessment and Management (CSAM) system.[1] The Office of the Chief Information Officer (OCIO) is responsible for ensuring that the agencies are compliant with Federal and Departmental guidance and are reporting aggregate results during the annual FISMA reporting cycle. CSAM has a powerful reporting capability that can be used to generate information covering: current Certification and Accreditation (C&A) status, completion of security control testing and review, and contingency plan testing results.[2] The Department has access to the same CSAM information that we evaluated during the FISMA review and should have been aware of each of the weaknesses we identified. The Department should use CSAM's capabilities more effectively in performing its oversight responsibilities. We continue to find the following:

- The Department was not completing the semi-annual inventory reconciliation as required by Department procedures.[3] The Department was unable to provide a reconciliation of inventory for FY 2010. For example, we found three systems with the status of operational and FISMA reportable in FY 2009; in FY 2010 their status had changed to

[1] 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.

[2] C&A is a process mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 28, 2000. The process requires that IT system controls be documented and tested by technical personnel and given the formal authority to operate by an agency official.

[3] *Standard Operating Procedure for Information Technology Inventory Reconciliation and Certification*, dated April 28, 2009. The SOP requires that the Department reconcile the CSAM inventory with the Enterprise Architecture Repository (EAR) and Electronic Capital Investment Management Repository System (eCPIC) systems inventory semi-annually.

operational but not FISMA reportable. No documentation was provided justifying this status change.[4]

- Agencies are not following National Institute of Standards and Technology (NIST) and Departmental[5] guidance when preparing C&A documentation. Agencies are required to submit their system C&A packages and all supporting documentation to the Department for an in-depth review (referred to as a concurrency review). During the concurrency review, the Department ensures that the documentation prepared to support system accreditation[6] is complete, accurate, reliable, and that it meets all NIST and other mandated documentation standards. We noted in four of the C&A concurrency reviews that the Department had concurred with the agencies' recommendations to accredit the systems, even though the agencies' security certification documentation did not support accreditation. We determined agencies had not followed NIST guidance in all four cases.

  Specifically, we found concurrency reviews were not: (1) adequately reviewing agency C&A documentation; (2) denying authority to operate for systems that did not have controls in place to protect the system; and (3) ensuring all documentation was accurate and complete. This occurred because the Department was not adequately overseeing the concurrency process. As a result, USDA cannot be assured that all system controls had been documented and tested, and systems were operating at an acceptable level of risk if controls were not implemented effectively.

  Additionally, we found 7 of 282 systems were granted a "Conditional" Authority To Operate (ATO).[7] The Department grants "Conditional" ATOs when the issues are considered minor, do not pose unacceptable risks to the security of the system, and can be resolved within a year. DM 3555-001 discusses an "Interim Authority to Operate" with a maximum allowable time to correct the deficiencies of 6 months. CSAM does not recognize "Conditional" ATOs; therefore, ensuring risks are resolved is difficult to monitor and track. As a result, the Department and agencies can not ensure their testing of security controls, documenting weaknesses, and tracking the mitigation of those weaknesses is complete and accurate.

- The Department has established and is maintaining a security configuration management program; however, it needs to make significant improvements. Specifically, we found that the Department has not established adequate procedures, made available standard

[4] There is no corresponding question in Exhibit A for this section. OMB did not ask this question, however, an accurate inventory is the first step in an effective security program; therefore, we reviewed OCIOs inventory reconciliation efforts.

[5] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004; Departmental Manual (DM) 3555-001, *Certification and Accreditation Methodology*, dated October 18, 2005.

[6] Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

[7] Authority to operate (ATO) is the last step in the C&A process. If the C&A is adequate and meets NIST requirements, and the agency determines risks are acceptable, then an ATO is granted by the Department for a period of 3 years.

baseline configurations for all operating systems in use, completed its hardware inventory, and completely scanned its networks and corrected its vulnerabilities. For example, we found 699 missing software vendor patches over 30 days old that had not been applied in three agencies we reviewed. These patches had not been installed in more than 27,000 machines. Furthermore, 194 of those patches had been available from Microsoft since 2008.

- The Department is not following its own policy and procedures in regard to incident response and reporting. Our review of 28 incidents that occurred during the year disclosed that all 28 incidents were not handled in accordance with Departmental procedures.[8] Additionally, United States Computer Emergency Readiness Team (US-CERT) has established timeframes for when the Department is required to notify them of incidents.[9] Testing identified 11 of 28 incidents that were not reported to US-CERT within the required timeframe. One of the 11 incidents included Personally Identifiable Information (PII) and was not reported to US-CERT for 38 days, rather than within 1 hour as required.

- Department policies and procedures met all the NIST requirements for security awareness training.[10] However, USDA lacks policies and procedures governing specialized security training for personnel with significant information security responsibilities. In addition, we found that not all personnel received the required specialized security training. For example, our review identified 5 of 20 employees who required specialized training but were not able to provide documented proof of training.

- The Department did not have effective policies and procedures for reporting IT security deficiencies in CSAM.[11] We found the Plan of Action and Milestones (POA&Ms) did not include all known security weaknesses. For example, the Department requires an agency to create a POA&M when an identified vulnerability cannot be remediated within 30 days.[12] However, testing at 3 agencies found 424 vulnerabilities that were over 30 days old without the required POA&Ms. This occurred because the Department security

[8] Agriculture Security Operations Center (ASOC) Computer Incident Response Team (CIRT), *Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents*, SOP-ASOC-001, June 9, 2009.
[9] The US-CERT provides response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCSD) at 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.
[10] DM 3545-001, *Computer Security Training and Awareness*, dated February 17, 2005.
[11] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated October 17, 2001, required each agency to submit to OMB by October 31, 2001 (with brief quarterly updates thereafter), "a plan of action with milestones" to address all weaknesses identified by program reviews and evaluations. It defines a POA&M as 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. The goal of a POA&M should be to reduce the risk of the weakness identified. CSAM is used as the USDA POA&M repository, and to track and report to OMB progress to mitigate the weaknesses.
[12] DM 3530-001, Appendix A, *Vulnerability Scan Procedures*, July 20, 2005.

manual did not include a policy for establishing a POA&M[13] process for reporting IT security deficiencies and tracking the status of remediation efforts. Although there were no formal policies, the Department had prepared a standard operating procedure (SOP)[14] covering the POA&M Management Process. Our review of the SOP determined it was written prior to the implementation of CSAM and requires updating to reflect the current POA&M process. In addition, our review of POA&Ms within CSAM found that 630 of 3,411 had a Scheduled Completion Date of "to-be-determined", instead of an actual date that could be tracked and monitored in compliance with NIST guidance. We also noted POA&Ms were not being timely remediated. We found that 533 of 1,830 POA&Ms that were closed during the year were not completed by the due date.

- The Department's remote access program needs significant improvements. Testing identified policies that did not meet NIST requirements.[15] Also, the Department stated that procedures are the responsibility of the agencies and; therefore, did not provide any to OIG. In addition, employees did not follow the policies that did exist. For example, the Department[16] requires multi-factor authentication[17] for all remote access. However, we found six of the seven agencies reviewed had not implemented multi-factor authentication.

- The Department had developed an account and identity management policy; however, it was not sufficiently detailed or consistently implemented. We found that USDA's policy did not meet NIST requirements, that the Department had not developed procedures for managing accounts, and that the Department had not implemented account management using the proper security. We found that four of the six agencies reviewed did not properly implement USDA's Active Directories. For example, we found separated employees with active accounts, excessively elevated account privileges granted to users, and administrator accounts that did not follow the principle of granting the fewest privileges users needed to perform their work. We found 12 of the 13 agencies reviewed could not identify all user and non-user accounts within their Active Directory. We also found that neither the Department nor three selected agencies had policy and procedures for unauthenticated network devices, and that the three agencies reviewed were unable to detect and properly authenticate all devices attached to their networks per NIST.[18]

---

[13] 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.

[14] *POA&M Management Process, Standard Operating Procedure*, dated February 27, 2008.

[15] NIST SP 800-46, revision 1, *Guide to Enterprise Telework and Remote Access Security*, dated June 2009.

[16] DR 3505-003, *Access Control Policy*, dated August 11, 2009.

[17] 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. In this context, the two factors involved are sometimes spoken of as *something you have* and *something you know*.

[18] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Rev 3, dated August 2009.

- The Department had not established a continuous monitoring program, as required by NIST, though it is planning to implement one by the end of FY 2011.

- The Department had contingency plan policies that were fully developed; however, it had not effectively implemented contingency procedures. We found that 2 of the 23 agency systems reviewed did not have a fully developed and consistently implemented procedure for contingency planning. For example, during an audit conducted this year, we identified 9 of 18 visited field sites that were unable to provide backup procedures. In addition to USDA not implementing effective procedures, the agencies were not testing contingency plans. During FY 2010, we found that agencies did not test their contingency plans for 48 of 279[19] systems reviewed, as required by NIST SP 800-53.

- The Department did not have policies and procedures to oversee systems operated on the agencies' behalf by contractors or other entities. In addition, we found the Department does not have an accurate inventory of contractor systems—12 systems were identified in the FY 2009 FISMA audit as contractor systems, but they were not listed as such on the inventory. During this year's audit, we found that 11 of those systems are still not identified as contractor systems. FISMA requires agencies to maintain an inventory of their information systems, which includes an identification of the interfaces between each system, and all other systems or networks, including those not operated by or under the control of the agency.[20] We found 22 of the 31 systems that we reviewed had incorrectly reported the interconnections to other systems not operated by the agency.

We received OCIO comments to this report on November 12, 2010 and have incorporated those comments into this report as appropriate. For example, we have recognized OCIO initiatives in the areas of planning, outreach, and security tools. OCIO disagreed with many of the findings in this report; however, after further review of its response we maintain our position. For example, OCIO stated that NIST guidance is not required to be followed and therefore several of our findings were invalid. However, OMB Memo 10-15 states that use of NIST publications is required for non-national security systems. In another example, they questioned our criteria on reporting to US-CERT and stated that there is no way to guarantee an absolute timeline on the investigation. However, these criteria come from US-CERT and are posted on its website, and are also included in the Department SOP. Finally, the OCIO stated they did not agree that they issued "Conditional" ATOs. However, the term "Conditional" ATO was derived from an interview with OCIO personnel in response to OIG's question of why some ATOs were granted for 1 year. We will follow-up with OCIO regarding each of the issues raised in their response.

Recommendations

1. Develop detailed procedures for the consistent use of CSAM. Those procedures should identify exactly where documents should reside, and which documents should be uploaded into CSAM. In addition, procedures should specify fields in CSAM to be populated and provide directions as to which data should be in the fields.

[19] Based on a CSAM report generated on October 22, 2010.
[20] FISMA of 2002, Title III *Information Security*, dated December 17, 2002.

2. Discontinue the use of "Conditional" ATO's and follow OMB requirements.

3. Ensure documented configuration management procedures are developed and consistently implemented across the Department. Include baseline configurations for all approved software and hardware. Any changes to the baseline guides should be documented and approved.

4. Ensure scanning for compliance to the baseline configurations and for vulnerabilities is preformed as required by NIST.

5. Develop automated procedures for the timely and secure installation of software patches.

6. Ensure all Departmental and agency policy and procedures adhere to NIST requirements.

7. Ensure that the Department's training repository is completely populated to ensure all required personnel receive the required training.

8. 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.

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

10. Complete the Departmental projects that will enforce multi-factor authentication and external media encryption.

11. Develop account and identity management policy and procedures that fully comply with NIST. These should include, but not be limited to, Active Directory procedures based on Microsoft Best Practices, periodic oversight and review of identity management within the Department, and best practices for network device authentication.

12. Develop policies, procedures, strategies, and implementation plans for continuous monitoring, including items such as vulnerability scanning, log monitoring, notification of unauthorized devices, and sensitive new accounts in accordance with NIST.

13. Develop ongoing assessments of selected security controls that have been performed, based on the approved continuous monitoring plans.

14. Ensure system authorizing officials and other key system officials are provided with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.

15. 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.

16. Perform an overall business impact assessment for the Department.

17. 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 exercise results. Periodically review CSAM to ensure agency compliance.

18. 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 is completed periodically.

19. Ensure contractor and non-contractor systems inventory and interfaces are accurate and updates are completed at least annually.

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, "Federal Information Security Management Act." 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, but it also included new provisions that further strengthened the Federal Government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems. NIST was tasked to work with agencies developing those standards as part of its statutory role in providing technical guidance to Federal agencies.

FISMA supplements 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 evaluation, 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). OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. The responsibilities include the authority to approve agencies' information security programs. OMB also requires the submittal of an annual report to Congress summarizing the results of each agency's evaluation of its information security programs.

Each agency must establish a risk-based information security program that ensures information security is practiced throughout the lifecycle of each agency's system. Specifically, the agency's CIO 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 to 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' CIOs, and compliance with FISMA;
- the agencies' system of internal controls over IT assets:
- the Department's progress in establishing a Departmentwide security program, which includes effective certifications and accreditations;
- the agencies' and Department's plan of action and milestones (POA&M) consolidation and reporting process; and
- the effectiveness of controls over configuration management, incident response, IT training, remote access management, identity and access management, continuous monitoring, contingency planning, and contractor systems.

Scope and Methodology

The scope of our review was Departmentwide and included agency IT audit work completed during FY 2010. 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 at USDA locations throughout the continental United States from June 2010 through October 2010. In addition, this report incorporates audits done throughout the year by OIG. Testing was conducted at offices in Washington, D.C, Kansas City, Missouri, and St. Louis, Missouri. Additionally, in this report, we included the results of IT control testing and compliance with laws and regulations performed by contract auditors at seven additional agencies. In total, our FY 2010 audit work covered 12 agencies and staff offices:

- Animal and Plant Health Inspection Service (APHIS),
- Agricultural Research Service (ARS),
- Natural Agricultural Statistics Service (NASS),
- Grain Inspection, Packers, and Stockyards Administration (GIPSA),
- Food Safety and Inspection Service (FSIS),
- Farm Service Agency (FSA),
- Food and Nutrition Service (FNS),
- Forest Service (FS),
- National Resource Conservation Service (NRCS),
- Office of the Chief Financial Officer (OCFO),
- Office of the Chief Information Officer (OCIO),
- Rural Development (RD), and
- Risk Management Agency (RMA).

These agencies and staff offices operate approximately 227 of the USDA's estimated 282 general support and major application systems within the Department.

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 of contractors performed for USDA's OIG. 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-10-15, *Fiscal Year 2010 Reporting Instructions for*

the Federal Information Security Management Act and Agency Privacy Management, dated April 21, 2010; and

- Performed detailed testing specific to FISMA requirements at selected agencies, as detailed in this report.

Testing results were compared against NIST controls, OMB guidance, e-Government Act requirements, and Departmental policies and procedures for compliance.

Abbreviations

ASOC	Agriculture Security Operations Center
ATO	Authority to Operate
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CS	Contractor Systems
CSAM	Cyber Security Assessment and Management
DHS	Department of Homeland Security
FCD1	Federal Continuity Device 1
FDCC	Federal Desktop Core Configurations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
ISA	Interconnection Security Agreement
IT	Information Technology
MOU/A	Memorandum of Understanding/Agreement
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
N/R	Not Reviewed
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of the Management and Budget
PIV	Personal Identity Verification
POA&M	Plans of Actions & Milestones
RA	Risk Assessment
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plans
TBD	To Be Determined
TT&E	Training, Testing, and Exercises
US-CERT	United States – Computer Emergency Readiness Team
USDA	Department of Agriculture

Exhibit A: Office of the Management and Budget (OMB) Reporting Requirements and U.S. Department of Agriculture (USDA) Office of Inspector General (OIG) Position

OMB's questions are set apart by boldface in each section. OIG checks items on OMB's list, boldfacing and underlining the relevant text. We answer direct questions with True, False, or Not Reviewed (NR).

The universe of systems and agencies reviewed varied during each audit or review reflected in this report. As part of FISMA, OIG reviewed systems and agencies, OIG contractors, agency annual self-assessments, and various OIG audits throughout the year. Since the scope of each review and audit differed, we could not use every review or audit to answer each question.

S1: Certification and Accreditation
Section 1: Status of Certification and Accreditation (C&A) Program

1. Check one:

a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.

2. Establishment of accreditation boundaries for agency information systems.

3. Categorizes information systems.

4. Applies applicable minimum baseline security controls.

5. Assesses risks and tailors security control baseline for each system.

6. Assessment of the management, operational, and technical security controls in the information system.

7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.

8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.

b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established a certification and accreditation program.

1a. If b. checked above, check areas that need significant improvement:

1a(1) Certification and accreditation policy is not fully developed. False

No exceptions noted.

1a(2) Certification and accreditation procedures are not fully developed, sufficiently detailed or consistently implemented. True

Based on the OIG reviews performed throughout FY 2010, we found that agencies were not following NIST and Departmental guidance when preparing C&A documentation. [21] Agencies are required to submit their system C&A packages and all supporting documentation to the Department for an in-depth review (referred to as a concurrency review). During the concurrency review, the Department should ensure that the documentation prepared to support system accreditation is complete, accurate, reliable, and satisfies all NIST and other mandated documentation standards. [22] We evaluated four C&A concurrency reviews where the Department had concurred with the agencies' recommendations to accredit the system. We found the agencies' security certification[23] documentation did not support accreditation, and we determined that agencies had not followed NIST guidance in all four cases. Specifically, we found concurrency reviews were not: (1) adequately reviewing agency C&A documentation; (2) denying authority to operate for systems that did not have controls in place to protect the system; and (3) ensuring all documentation was accurate and complete. This occurred because the Department was not adequately overseeing the concurrency process. As a result, USDA cannot be assured that all system controls had been documented and tested, and systems were operating at an acceptable level of risk if controls were not implemented effectively.

1a(3) Information systems are not properly categorized (FIPS 199/SP 800-60). True

NIST states that the overall impact level for any given system should be based on the highest impact level for the system security objectives.[24] The controls which are applied to the system are then based upon that impact level. NIST provides recommended settings for each of these levels.

[21] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004, DM 3555-001, *Certification and Accreditation Methodology*, dated October 18, 2005.
[22] Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.
[23] Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, which are made in support of security accreditation 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.
[24] NIST SP800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Vol. 1, dated August 2008.

We generated a report from Cyber Security Assessment and Management (CSAM) which identified the impact level for each of the Department's systems.[25] 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 24 of 282 systems indicated a lower categorization than was recommended during the C&A process without adequate justification for the reduction in categorization level. NIST requires that any adjustments to the recommended impact levels be documented and include justification for the adjustment.

1a(4) Accreditation boundaries for agency information systems are not adequately defined. False

No exceptions noted.

1a(5) Minimum baseline security controls are not adequately applied to information systems (FIPS 200/NIST SP 800-53). True

NIST recommends a set of minimum baseline security controls, based on the systems' overall categorization.[26] The lower the category, the fewer controls required. Therefore, the incorrect categorizations noted in 1a(3) led to inadequate controls being implemented for those 24 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.

1a(6) Risk assessments are not adequately conducted (NIST SP 800-30). True

NIST SP 800-30 states that risk assessments are the first step in the risk management methodology. The risk assessments determine the likelihood of a future adverse event. Threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the implemented controls for the IT system.[27] We found 12 of the 30 risk assessments (RA) reviewed were inadequately conducted. For example, all four RAs reviewed during this audit were not updated, based on testing done during the C&A process. Additionally, one of these RAs referred to a system which had nothing to do with the system being reviewed.

[25] CSAM is a comprehensive system developed by the Department of Justice, which can facilitate achieving Federal Information Security Management Act (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 or those operated by contractors on the agency's behalf.

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

[27] NIST SP800-30, *Risk Management Guide for Information Technology Systems*, dated July 2002.

1a(7) Security control baselines are not adequately tailored to individual information systems (NIST SP 800-30). True

NIST SP 800-53 recommends a set of minimum baseline security controls, based on the overall categorization of the system. The lower the category, the fewer controls are required. Therefore, the incorrect categorizations noted in 1a(3) led to inadequate controls being implemented for those 24 systems. NIST SP 800-60 states that an incorrect information system impact analysis can result in the agency either overprotecting the information system (thereby wasting valuable security resources), or under protecting the information system and placing important operations and assets at risk. In addition, we found that documentation for all four of the systems evaluated during our concurrency review process did not define how the agencies' systems had actually implemented the controls. In some instances the controls were taken verbatim from NIST documentation and did not specify how the controls were implemented in the system.

1a(8) Security plans do not adequately identify security requirements (NIST SP 800-18). True

NIST requires Federal agencies to adopt a minimum set of security controls to protect their information and information systems.[28] Federal agencies must meet the minimum security requirements defined in Federal Information Processing Standards (FIPS) 200 through the use of the security controls in NIST SP 800-53. However, we found 12 of the 30 System Security Plans (SSP) reviewed by OIG or outside contractors were inadequate.[29] Our review of the SSPs found the security controls did not include sufficiently detailed descriptions of how the controls were implemented. For example, if a specific control was not implemented, we found that there was no justification as to what would compensate for the control. Also, we found SSPs had controls listed as "planned," but did not state when the implementation would occur or if any compensating controls existed in the interim.

1a(9) Inadequate process to assess security control effectiveness (NIST SP 800-53A). True

NIST SP 800-53 requires security controls to be assessed and documented 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. Organizations conduct assessments for the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcomes, with respect to meeting the security requirement for the system. Agency self-assessments completed throughout the year identified 37 controls that were inadequately designed and implemented within 12 systems. Also, the SSP for all four of the systems reviewed during the evaluation of the concurrency reviews, did not include sufficient documentation stated in the SSP for the controls tested. For example, one SSP

[28] NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems,* Rev 1, dated February 2006.

[29] The SSP is a required C&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,* dated February 2006.

included a statement in the boundaries section that said "not sure where the four systems come from," while others referenced data from the Departmental template, instead of the actual information on the system. In addition, we found 68 systems did not have their security controls tested and reviewed in the past year.

1a(10) Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (NIST SP 800-37). True

NIST states the explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorization decision document conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. [30] We found 12 of 30 systems reviewed by OIG or outside contractors were granted an Authority to Operate (ATO), even though they did not have an adequate process in place to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate.[31] The C&A documents were the basis for this decision and, as noted in the questions above, C&A documents were missing, inaccurate, or incomplete. In addition, we found 13 of the 282 systems had an expired ATO.

1a(11) Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (NIST SP 800-37). True

NIST SP 800-37 states that Federal organizations must provide an effective method of tracking changes to information over time through strict configuration management and control procedures (including version control) in order to: (1) achieve transparency in the information security activities of the organization; (2) obtain individual accountability for security-related actions; and (3) better understand emerging trends in the organization's information security program. Audit work performed throughout the year by OIG and outside contractors found 8 of the 26 systems reviewed did not have a process to continuously track changes to information systems.

S2: Configuration Management
Section 2: Status of Security Configuration Management

2. Check one:

a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

[30] NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Rev 1, dated February 2010.
[31] Authority to operate (ATO) is the last step in the C&A process. If the C&A is adequate and meets NIST requirements, and the agency determines risks are acceptable, then an ATO is granted by the Department for a period of 3 years.

1. Documented policies and procedures for configuration management.
2. Standard baseline configurations.
3. Scanning for compliance and vulnerabilities with baseline configurations.
4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented.
5. Documented proposed or actual changes to the configuration settings.
6. Process for the timely and secure installation of software patches.

b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established a security configuration management program

2a. If b. checked above, check areas that need significant improvement:

2a(1) Configuration management policy is not fully developed. True

We found that the Department's configuration management policy meets NIST SP 800-53 requirements; however, we found two of nine agencies' policies reviewed by OIG or outside auditors did not meet the NIST requirements.

2a(2) Configuration management procedures are not fully developed or consistently implemented. True

NIST SP 800-53 requires that the organization develop formal documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. OIG or outside auditors found that five of eight agencies did not fully or consistently develop configuration management procedures. One of the five agencies was unable to provide any documented procedures. In addition, the annual self assessment identified 11 agencies that had configuration management weaknesses in 28 systems.

2a(3) Software inventory is not complete (NIST SP 800-53: CM-8). True

NIST SP 800-53 requires the organization to develop, document, and maintain an inventory of information system components which accurately reflects the current information system and is available for review and audit by designated organizational officials. We found that one of five agencies reviewed did not have a complete software inventory.

2a(4) Standard baseline configurations are not identified for all software components (NIST SP 800-53: CM-8). True

NIST SP 800-53 requires the organization to develop, document, and maintain under configuration control, a current baseline configuration of the information system. The Department did not maintain a current baseline configuration guide for all operating systems in use at USDA. For example, our reviews of four agencies found a total of 21 different operating systems in use. However, 17 did not have the required configuration guides available.

2a(5) Hardware inventory is not complete (NIST SP 800-53: CM-8). True

NIST requires that the organization develop, document, and maintain an inventory of information system components which accurately reflects the current state of the information system and is available for review and audit by designated organizational officials. We found that one of the four agencies reviewed did not maintain a complete hardware inventory.

2a(6) Standard baseline configurations are not identified for all hardware components (NIST SP 800-53: CM-2). True

We found that neither the Department nor the three agencies reviewed during the audit were able to provide standard baseline configurations for hardware components.

2a(7) Standard baseline configurations are not fully implemented (NIST SP 800-53: CM-2). True

Our review found that 763,417 of 1,647,432 (over 46 percent) Windows 2003 configuration settings did not comply with current Federal guidelines.[32]

2a(8) FDCC is not fully implemented (OMB) and/or all deviations are not fully documented. False\

No exceptions noted. OMB required that agencies with Windows Vista or Windows XP operating systems, or plans to upgrade to these operating systems, adopt standard security configurations on workstations by February 1, 2008.[33] The standard security configurations were developed by NIST, the Department of Defense, and the Department of Homeland Security and are commonly referred to as the Federal Desktop Core Configuration (FDCC). Our reviews found over 88 percent of all required settings on workstations were compliant. In addition, our review at five agencies found all deviations from the FDCC had fully documented required waivers. This is a vast improvement from FY 2009, when only 8 percent of the Department computers complied with FDCC settings or had deviations documented.

2a(9) Software scanning capabilities are not fully implemented (NIST SP 800-53: RA-5, SI-2). True

The Department requires all agencies to establish and implement procedures for accomplishing vulnerability scanning of all networks, systems, servers, and desktops for which they have responsibility.[34] This includes performing monthly scans and remediating vulnerabilities found as a result of the scans. We found six of seven agencies did not scan all devices and did not correct critical vulnerabilities in a timely manner.

---

[32] Defense Information Systems Agency, *Windows 2003 Security Technical Implementation Guide*, dated August 27, 2010.
[33] OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, dated March 22, 2007.
[34] DM 3530-001, *USDA Vulnerability Scan Procedures*, dated July 20, 2005.

2a(10) Configuration-related vulnerabilities have not been remediated in a timely manner (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2). True

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. Our review of four agencies disclosed that configuration vulnerabilities were not being mitigated and remediated timely. Specifically, we found that 42 network device settings were not configured in accordance with NIST SP 800-53.

2a(11) Patch management process is not fully developed (NIST SP 800-53: CM-3, SI-2). True

NIST requires Federal agencies to incorporate vendor software flaw remediation (patches) into the organizational configuration management process. Our review at three agencies identified 699 missing patches that were over 30 days old and that had not been applied to 27,813 machines. Furthermore, 194 of those patches had been available from the vendor since 2008.

3. Identify baselines reviewed:

Apple Mac OS X
Cisco Catalyst
Cisco IOS
Microsoft Exchange Server 2003
Microsoft Windows Mobile 6
Microsoft Windows Server 2000
Microsoft Windows Server 2003
Microsoft Windows Vista Enterprise Edition
Microsoft Windows XP Professional
Oracle Database 10g
Redhat Enterprise Linux 4
Research In Motion Blackberry
Sun Solaris 10
Other

S3: Incident Response and Reporting
Section 3: Status of Incident Response & Reporting Program

4. Check one:

a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. **Documented policies and procedures for responding and reporting to incidents.**
2. **Comprehensive analysis, validation and documentation of incidents.**

3. When applicable, reports to US-CERT within established timeframes.
4. When applicable, reports to law enforcement within established timeframes.
5. Responds to and resolves incidents in a timely manner to minimize further damage.

b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established an incident response and reporting program.

4a. If b. checked above, check areas that need significant improvement:

4a(1) Incident response and reporting policy is not fully developed. True

We compared the Departmental and selected agency incident handling policies with NIST requirements in order to ensure all necessary elements were addressed.[35] We found that Department policy generally met all of the NIST requirements, but all three agencies' policies we reviewed were missing required elements. For example, we found that the three agencies did not have a detailed list of the reasons incidents should be declared, classifications of different types of incidents, and roles and responsibilities of agency personnel.

4a(2) Incident response and reporting procedures are not fully developed, sufficiently detailed or consistently implemented. True

Our review of incidents throughout the year found that all 28 of the incidents we reviewed were not handled in accordance with Departmental procedures.[36] 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 all 28 incidents had either incomplete incident documentation or did not include the required documentation outlined in the procedures. For example, one incident involving personal information had marked "not applicable" on the Departmental form which asked whether it was in regard to personal information.

4a(3) Incidents were not identified in a timely manner (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). True

Our review found that the Department did not identify 1 of 15 incidents in a timely manner. That incident was reported timely to the Department, but Departmental employees took seven days to create the incident report and respond back to the agency. This particular category of

[35] NIST 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Rev 3, August 2009; and NIST SP-800-61, *Computer Security Incident Handling Guide*, March 2008.
[36] Agriculture Security Operations Center (ASOC) Computer Incident Response Team (CIRT), *Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents*, SOP-ASOC-001, June 9, 2009.

incident is required to be reported to The US-Computer Emergency Readiness Team (US-CERT) within one day.[37]

4a(4) Incidents were not reported to US-CERT as required (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). True

US-CERT requires USDA to notify it of incidents within specified timeframes, based on the category of the incident. Our review of incidents disclosed USDA did not report 11 of 28 incidents to US-CERT within the required timeframe. For example, US-CERT requires that breaches of personally identifiable information (PII) be reported within one hour; however, we found that USDA did not report five incidents in this category within this timeframe. One PII incident was not reported for 38 days.

4a(5) Incidents were not reported to law enforcement as required. True

NIST SP 800-61 and Departmental procedures require evidence of contact with a local police department if the incident is of a certain category. One of 15 incidents reviewed was for a stolen computer, but we found no evidence that USDA reported the incident to local law enforcement, as required.

4a(6) Incidents were not resolved in a timely manner (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). True

Based on testing conducted for 4a(4) and 4a(7), we found that USDA did not resolve 2 of 15 incidents timely.

4a(7) Incidents were not resolved to minimize further damage (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). True

The Department's SOP requires that IT employees immediately remove a computer containing prohibited software from the network and uninstall the software before the computer is returned to production. We found, however, that IT employees did not follow this SOP in 1 of the 15 incidents reviewed during this audit. In this particular case, the prohibited software was still on the computer the next day when it was again reported as an incident.

4a(8) There is insufficient incident monitoring and detection coverage (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). True

The Department has relied on US-CERT to monitor and detect incidents; however, on September 27, 2010, the Department implemented a suite of network monitoring and detection

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

devices which should greatly enhance the Department's ability to detect fraudulent or illegal activity, prior to the Department being notified by US-CERT.

Additionally, for an organization to have a sufficient incident monitoring and detection program, NIST requires that Federal agencies train personnel in their incident response roles and responsibilities and that the organization test its incident response capability with the use of automated mechanisms. Our review of the Department's policies and procedures and our discussions with Departmental personnel indicated the Department does not have a training program in place nor does it perform training exercises with the aid of automated mechanisms.

S4: Security Training
Section 4: Status of Security Training Program

5. Check one:

a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

> **1. Documented policies and procedures for security awareness training.**
> **2. Documented policies and procedures for specialized training for users with significant information security responsibilities.**
> **3. Appropriate training content based on the organization and roles.**
> **4. Identification and tracking of all employees with login privileges that need security awareness training.**
> **5. Identification and tracking of employees without login privileges that require security awareness training.**
> **6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.**

b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established a security training program.

5a. If b. checked above, check areas that need significant improvement:

5a(1) Security awareness training policy is not fully developed. True

We determined the Department's security awareness policy met all requirements of NIST SP 800-53.[38] However, one of three agencies reviewed did not have any policies to ensure that all employees and contractors attended security awareness training.

[38] DM 3545-001 *Computer Security Training and Awareness*, dated February 17, 2005.

5a(2) Security awareness training procedures are not fully developed, sufficiently detailed or consistently implemented. True

We determined the Department's security awareness training procedures met all requirements of NIST SP 800-53. However, one of three agencies' procedures we reviewed during this audit did not have all of the required elements to ensure employees and contractors received adequate role-based security awareness training.

5a(3) Specialized security training policy is not fully developed. True

We determined that the Department's policy for specialized security training was not fully developed or sufficiently detailed.[39] We found the Department's policy for specialized training did not include a definition of significant information security responsibilities. Without a definition, agencies have interpreted the requirement inconsistently. In one agency, only security staff employees were required to attend specialized training, not all personnel with significant information security responsibilities (such as server administrators). As of September 30, 2010, the Department was working on a draft policy, including a formal definition.

5a(4) Specialized security training procedures are not fully developed or sufficiently detailed (NIST SP 800-50, NIST SP 800-53). True

We determined the Departmental procedures for specialized security training were not fully developed or sufficiently detailed.[40] In addition, audit work done by OIG and outside contractors determined that three of nine agency procedures did not include sufficient detail to ensure personnel with significant security responsibilities obtained specialized training every year.

5a(5) Training material for security awareness training does not contain appropriate content for the Agency (NIST SP 800-50, NIST SP 800-53). False

No exceptions noted.

5a(6) Identification and tracking of employees with login privileges that require security awareness training is not adequate (NIST SP 800-50, NIST SP 800-53). True

NIST SP 800-53 requires agencies to document and monitor individual information system security training activities and to retain individual training records. Both OIG and outside contractors found four of nine agencies did not have adequate identification and tracking of employees with login privileges. Specifically, we found 344 of 8,060 employees with login privileges did not have evidence that they had completed the annual security awareness training.

[39] DM 3545-002 *USDA Information System Security Program*, dated March 28, 2006.
[40] Departmental Standard Operating Procedure, *Information Security Training*, dated October 7, 2008.

5a(7) Identification and tracking of employees without login privileges that require security awareness training is not adequate (NIST SP 800-50, NIST SP 800-53). True

NIST SP 800-53 requires agencies to document and monitor individual information system security training activities and to retain individual training records. Our review during this audit found four of nine agencies did not adequately identify and track employees without login privileges, which require security awareness training. We found 106 of 414 employees without login privileges did not have documented evidence that they had completed the annual security awareness training.

5a(8) Identification and tracking of employees with significant information security responsibilities is not adequate (NIST SP 800-50, NIST SP 800-53). True

NIST SP 800-53 requires agencies to document and monitor individual information system security training activities and to retain individual training records. Contractor testing on behalf of OIG identified one of seven agencies that did not have sufficient identification and tracking of employees with significant information security responsibilities.

5a(9) Training content for individuals with significant information security responsibilities is not adequate (NIST SP 800-53, NIST SP 800-16). True

NIST SP 800-53 requires agencies to provide role-based training. Contractor testing on behalf of OIG identified one of seven agencies did not have sufficient training content for individuals with significant information security responsibilities.

5a(10) Less than 90% of employees with login privileges attended security awareness training in the past year. False

No exceptions noted. Our testing identified 344 of 8,060 users (4 percent) with login privileges who did not have evidence of completion of the annual security awareness training. Therefore, 96 percent of users with login privileges attended security awareness training in the past year.

5a(11) Less than 90% of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year. True

NIST SP 800-53 requires agencies to document and monitor individual information system security training activities and to retain individual training records. Our testing of 20 employees with significant security responsibilities found 15 (75 percent) employees had documented evidence of specialized training attendance.

S5: POA&M

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

6. Check one:

a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

> **1. Documented policies and procedures for managing all known IT security weaknesses.**
> **2. Tracks, prioritizes and remediates weaknesses.**
> **3. Ensures remediation plans are effective for correcting weaknesses.**
> **4. Establishes and adheres to reasonable remediation dates.**
> **5. Ensures adequate resources are provided for correcting weaknesses.**
> **6. 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 POAM activities at least quarterly.**

b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established a POA&M program.

6a. If b. checked above, check areas that need significant improvement:

6a(1) POA&M policy is not fully developed. True

The Department's security manual did not include a policy for establishing a POA&M process for reporting IT security deficiencies and for tracking the status of remediation efforts.[41] The Department stated that it is currently in the process of developing a draft policy, which has not yet been finalized. In addition, the three agencies reviewed did not have a POA&M policy.

6a(2) POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented. True

Although there were no formal policies, the Department had prepared a standard operating procedure (SOP)[42] concerning the POA&M Management Process. Our review of the SOP determined it was written prior to the implementation of CSAM and requires updating to reflect the current POA&M process. We compared the Department's and agencies' procedures for the

[41] A POA&M is a tool that identifies tasks that need 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 task, and scheduled completion dates for the milestones. The goal of a POA&M should be to reduce the risk of the weakness identified.
[42] *POA&M Management Process, Standard Operating Procedure*, dated February 27, 2008.

use and management of POA&Ms to OMB requirements.[43] We determined the Department and the three agencies did not include all the required criteria elements OMB outlines. For example, the Department lacked procedures on linking to budgetary resources,[44] and the agencies lacked procedures on preparing POA&Ms for all IT security weaknesses.

In addition to reviewing policies and procedures for compliance, we tested to ensure the POA&M procedures were being properly implemented. Departmental procedures state all POA&Ms should contain the relevant security controls from NIST SP 800-53.[45] However, we found that 210 of 2,226 POA&Ms with a status of open during FY 2010 did not include the required NIST relevant security control. Departmental procedures also require the use of a closure checklist. The checklist must then be uploaded into CSAM as an artifact of the POA&M with which it is associated. This information is then used by the Department to ensure that POA&Ms were properly closed. Our review found that 107 of 1,830 POA&Ms that were closed in FY 2010 did not have the closure checklist uploaded.

Finally, Departmental procedures require requests for POA&M due date changes to be sent to and approved by the Department.[46] Once approved, only the CSAM administration team is authorized to make changes to the due date; however, our review found that five agencies had personnel with the access privileges necessary to make these changes.

6a(3) POA&Ms do not include all known security weaknesses (OMB M-04-25). True

We found POA&Ms did not include all known security weaknesses. For example, the Department requires an agency to create a POA&M when an identified vulnerability cannot be remediated within 30 days.[47] However, testing at three agencies found 424 vulnerabilities that were over 30 days old without the required POA&M.

6a(4) Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls). True

OMB M-04-25 specifies that a milestone will identify specific requirements to correct an identified weakness. We determined that four of nine agencies reviewed by OIG or outside contractors did not have POA&Ms which contained a documented resolution that sufficiently addressed the documented weakness. For example, one of the agencies we reviewed had a closed POA&M that was supposed to ensure that all devices were scanned monthly. A closed

[43] OMB M-04-25, *Fiscal Year 2004 Reporting Instructions for the Federal Information Security Management Act*, August 23, 2004.
[44] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated October 17, 2001, states that "to promote greater attention to security as a fundamental management priority, OMB continues to take steps to integrate security into the capital planning and budget process," and requires each POA&M to be linked to its budgetary and capital planning by including the unique project identifier on all POA&Ms.
[45] Standard Operating Procedure, *Plan of Action and Milestones Closure Review*, dated February 17, 2009.
[46] The Departmental Memo, *Continuous Monitoring of Plans of Actions and Milestones (POA&M)*, dated February 3, 2010.
[47] DM3530-001, Appendix A, *Vulnerability Scan Procedures*, July 20, 2005.

POA&M should signify that the weakness was corrected, but our audit work during the year found the agency was still not scanning all its devices monthly.

6a(5) Initial date of security weaknesses are not tracked (OMB M-04-25). True
OMB M-04-25 requires agencies to prepare and submit POA&Ms for all programs and systems where an IT security weakness has been found. We found the Department did not create POA&Ms at the time weaknesses were identified. For example, two of five agencies reviewed by OIG and outside contractors during the year found that agencies were not tracking the initial date of the security weakness. Also, the OIG FISMA report for FY 2009 provided numerous findings and 14 recommendations. The POA&Ms for these recommendations were not created until July and August 2010. The Department stated it did not create POA&Ms until management decision had been reached, rather than when the weakness was identified. OIG notes, however, that USDA has not reached management decision for these recommendations as of the date of this report's publication.[48]

6a(6) Security weaknesses are not appropriately prioritized (OMB M-04-25). True

OMB M-04-25 specifies that the purpose of a POA&M is to assist agencies in prioritizing the progress of corrective efforts for security weaknesses found in programs and systems. Our review of POA&Ms within the Department found 7 of 31 agencies were not appropriately categorizing security weaknesses. For example, the Department considers 29 security controls to be critical and requires the agencies to test, report the results of that testing, and create POA&Ms on weaknesses found with these controls on an annual basis. We found nine POA&Ms associated with these key controls were prioritized as low or very low, instead of a higher priority.

6a(7) Estimated remediation dates are not reasonable (OMB M-04-25). True

Department procedures required POA&Ms with a Scheduled Completion Date of "to be determined" (TBD) to be reviewed and estimated completion dates populated.[49] Our review of 3,411 of USDAs POA&Ms found that 630 of the Scheduled Completion Dates were marked TBD. Unless a POA&M has a completion date, the Department cannot ensure that the problem is mitigated timely.

6a(8) Initial target remediation dates are frequently missed (OMB M-04-25). True
Our review of POA&Ms closed during FY 2010 found 533 of 1,830 were not completed by the due date. Of the 533 POA&Ms that were not completed by the due date, we were able to determine that:

- 369 POA&Ms were completed within 89 days,
- 73 POA&Ms were completed 90 to180 days late,
- 91 POA&Ms were completed over 180 days late, and

[48] Management decision is reached on an OIG recommendation when both the agency and OIG agree on the corrective actions to be taken.
[49] "*Changes in the Due Dates of Plan of Actions and Milestones (POA&M),"* dated March 10, 2009.

- 1 POA&M was completed 547 days late.

As of September 30, 2010, an additional 148 POA&Ms were overdue. We also found that three Departmental POA&Ms with an end date of September 30, 2010 were changed to September 30, 2011 without any documented reasons.

6a(9) POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25). True

CSAM prohibits users from changing the Scheduled Completion Date field once it has been entered. Departmental procedures require special authorization to change the Scheduled Completion Date. According to the Department, only members of the CSAM Administration team within OCIO have the ability to change the Scheduled Completion Date. This change can only be made once OCIO approves the request and forwards to the CSAM administration team a request to implement the date change. Departmental guidance requires that an actual date be entered in order to enforce adherence to the POA&M timeline. As noted in 6a(7), we found 630 of the 3,411 POA&Ms had a Scheduled Completion Date of TBD, instead of an actual date that could be tracked and monitored. In addition, 6 of 10 POA&Ms reviewed by OIG for this audit were delayed without any documented reasons. One of those was cancelled without an explanation.

6a(10) Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25). True

We found that USDA has not met OMB's requirement[50] to link budgetary resources to POA&Ms. Of 1,830 POA&Ms closed in FY 2010, we found that 201 did not have the required budgetary link field populated in CSAM. In addition, OMB M-04-25 requires each POA&M to include the associated amount of estimated funding to resolve the weakness. We found 728 of 1,830 POA&Ms closed in FY 2010 listed $0 for the cost of correcting the weakness.

.

6a(11) Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25). True

The Department's SOP states all POA&Ms resulting from an audit are subject to the closure review process. In addition, the SOP requires the Department to review 10 percent of the non-audit related closed POA&Ms. We found 30 closed audit POA&Ms that the Department did not review. Also, we found that the Department only reviewed approximately 1.8 percent of closed POA&Ms in FY 2010.

[50] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated October 17, 2001, states that "to promote greater attention to security as a fundamental management priority, OMB continues to take steps to integrate security into the capital planning and budget process," and requires each POA&M to be linked to its budgetary and capital planning by including the unique project identifier on all POA&Ms.

S6: Remote Access Management
Section 6: Status of Remote Access Program

7. Check one:

a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.
2. Protects against unauthorized connections or subversion of authorized connections.
3. Users are uniquely identified and authenticated for all access.
4. If applicable, multi-factor authentication is required for remote access.
5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.
6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.
7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.

b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established a program for providing secure remote access.

7a. If b. checked above, check areas that need significant improvement:

7a(1) Remote access policy is not fully developed. True

Although the Department has a remote access policy,[51] we found it did not meet all NIST requirements.[52] We found that the Department's policy did not address key areas such as the administration of remote access servers and periodic reassessment of the telework device policies.

7a(2) Remote access procedures are not fully developed, sufficiently detailed or consistently implemented. True

The Department did not provide any procedures. The Department stated that it was responsible for creating policy, but that it was the agencies' responsibility to create procedures to ensure the policy is implemented.

[51] USDA Departmental Manual (DM) 3525-003, *Telework and Remote Access Security*, dated February 17, 2005.
[52] NIST SP 800-46, revision 1, *Guide to Enterprise Telework and Remote Access Security*, dated June 2009.

7a(3) Telecommuting policy is not fully developed (NIST SP 800-46, Section 5.1). True

As noted in 7a(1), we found the Departmental policy did not meet NIST guidance.

7a(4) Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46, Section 5.4). True

As noted in 7a(2), the Department did not provide any procedures.

7a(5) Agency cannot identify all users who require remote access (NIST SP 800-46, Section 4.2, Section 5.1). True

We found that three of the eight agencies reviewed by OIG or outside contractors did not identify all users who required remote access. This occurred due to inadequate policies and procedures, which resulted in agencies only tracking their remote access devices, not the employees who were using those devices.

7a(6) Multi-factor authentication is not properly deployed (NIST SP 800-46, Section 2.2, Section 3.3). True

Departmental Regulation 3505-003 requires multi-factor authentication[53] for all remote access.[54] However, we found six of seven agencies reviewed by OIG or outside contractors did not have multi-factor authentication implemented. This occurred because the agencies were waiting on the Departmental project to implement multi-factor authentication, which has a scheduled completion date of September 30, 2011.

7a(7) Agency has not identified all remote devices (NIST SP 800-46, Section 2.1). True

We found that one of five agencies reviewed for this audit did not have an inventory of its remote access devices. This agency stated that everyone in the agency has remote access capabilities if they have a laptop and an account, but the agency did not provide an inventory of its laptop devices. Additionally, the Departmental inventory of handheld devices with remote access was reviewed as part of an audit performed earlier this year. The audit determined that the agencies did not maintain a comprehensive inventory of wireless handheld devices.

7a(8) Agency has not determined all remote devices and/or end user computers have been properly secured (NIST SP 800-46, Section 3.1 and 4.2). True

As noted in 7a(6), USDA did not implement multi-factor authentication Departmentwide. We also found that agencies were not encrypting removable media in five of seven agencies

[53] 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. In this context, the two factors involved are sometimes spoken of as *something you have* and *something you know*.
[54] DR 3505-003, *Access Control Policy*, dated August 11, 2009.

reviewed. This occurred because agencies were waiting for the completion of Departmental projects in order to implement these security measures. In another audit, conducted during FY 2010, our review of 277 wireless handheld devices found that none of those devices were adequately secured. Finally, OMB requires remote access to be timed out after 30 minutes of inactivity.[55] We found two of three agencies reviewed during this audit did not disconnect users after 30 minutes of inactivity.

7a(9) Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST SP 800-46, Section 3.2). True

We found that three of four agencies reviewed were not adequately monitoring remote devices when connected to the agency's networks remotely, as required by NIST SP 800-46. This occurred because agencies relied on general network access logging to capture events. Inadequate security controls over remote access logging could lead to unauthorized access, use, disclosure, modification, or destruction of information.

7a(10) Lost or stolen devices are not disabled and appropriately reported (NIST SP 800-46, Section 4.3, US-CERT Incident Reporting Guidelines). True

During an OIG audit performed this year, we found that agencies had deployed devices which could not be remotely disabled when lost or stolen. This occurred because the Department had not established policies and procedures over wireless handheld devices.

7a(11) Remote access rules of behavior are not adequate (NIST SP 800-53, PL-4). True

We found that all four agencies reviewed by OIG or outside auditors did not have adequate rules of behavior for remote access. This occurred because all agencies relied on the general rules of behavior, which did not specifically refer to remote access. As a result, inadequate security concerning remote access could lead to unauthorized access, use, disclosure, disruption, modification, or destruction of information.

7a(12) Remote access user agreements are not adequate (NIST SP 800-46, Section 5.1, NIST SP 800-53, PS-6). True

We found four agencies reviewed by OIG or outside contractors did not have adequate remote access user agreements. The agencies did not have user agreements for remote access and relied on the general rules of behavior, which did not specifically refer to remote access. As a result, inadequate security of remote access could lead to unauthorized access, use, disclosure, disruption, modification, or destruction of information.

S7: Identity and Access Management
Section 7: Status of Account and Identity Management Program

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

8. Check one:

a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for account and identity management.
2. Identifies all users, including federal employees, contractors, and others who access Agency systems.
3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary.
4. If multi-factor authentication is in use, it is linked to the Agency's PIV program.
5. Ensures that the users are granted access based on needs and separation of duties principles.
6. Identifies devices that are attached to the network and distinguishes these devices from users.
7. Ensures that accounts are terminated or deactivated once access is no longer required.

b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below

c. The Agency has not established an account and identity management program.

8a. If b. checked above, check areas that need significant improvement:

8a(1) Account management policy is not fully developed. True

Although the Department developed an account and identity management policy, it was not fully developed, sufficiently detailed, or consistently implemented. The Department policy did not contain all controls required in NIST SP 800-53. For example, the Department was unable to provide a policy for the identification and authentication of devices on the network, as required by NIST SP 800-53. In addition, two of the three agencies reviewed during this audit did not have a formal policy for account management.

8a(2) Account management procedures are not fully developed, sufficiently detailed or consistently implemented. True

We found that the Department had developed an account and identity management program, but it had not developed procedures as required by NIST SP 800-53. This occurred because the Department stated it was only responsible for creating policy and that the development and implementation of the procedures was the agencies' responsibility. Our review of the three selected agencies found that the agencies did not have formal procedures meeting all NIST requirements.

8a(3) Active Directory is not properly implemented (NIST SP 800-53, AC-2). True

We found four of the six agencies reviewed by OIG or outside contractors had not properly implemented Active Directories, as required by NIST SP 800-53.[56] For example, our review of one agency found that an excessive number of accounts had administrator level access. NIST states users requiring administrative privileges on information system accounts receive additional scrutiny and administrator accounts should employ the concept of least privilege. Microsoft best practices describe an Enterprise Administrator as being "[r]esponsible for top-level service administration across the enterprise,"[57] yet we found 46 of these accounts in one agency's Active Directory. Also, Microsoft best practices describe a Domain Administrator as being "[r]esponsible for top-level service administration across the domain" and "should contain only a small, manageable number of trusted administrators," yet we found 870 of these accounts in the agency's Active Directory. In addition, we found there were no Departmental or agency policy and procedures for implementing the Active Directory. Our review identified an excessive number of elevated privileged user accounts, which could result in unauthorized access, use, disclosure, disruption, modification, or destruction of information.

8a(4) Other Non-Microsoft account management software is not properly implemented (NIST SP 800-53, AC-2). N/R

Not reviewed.

8a(5) Agency cannot identify all User and Non-User Accounts (NIST SP 800-53, AC-2). True

We found that 12 of 13 agencies reviewed by OIG, outside contractors, or during annual self-assessments could not identify all user and non-user accounts as required by NIST SP 800-53. NIST specifies that organizations should identify authorized users, deactivate temporary accounts when no longer needed, and deactivate the accounts of terminated or transferred users. We found the Department and its agencies were not meeting this control. For example, in one review performed this year, we identified 148 active accounts for employees who had separated from the agency. In addition, during the annual self-assessments performed, eight agencies identified weaknesses in deactivating separated employee accounts. Agencies were not reviewing user accounts within Active Directory and were not following user account policy and procedures, such as deactivating or removing separated employees. As a result, user accounts remained active after an employee left service and could lead to unauthorized access, use, disclosure, disruption, modification, or destruction of information.

8a(6) Accounts are not properly issued to new users (NIST SP 800-53, AC-2). True

We found that 8 of the 12 agencies reviewed by OIG or outside contractors were not properly issuing accounts to new users, as required by NIST SP 800-53. NIST specifies that

[56] Active Directory is a software component of Microsoft products that facilitates authenticating users and controlling access to network resources.

[57] Microsoft provides best practice guides to assist organizations in enhancing the security of their Active Directory systems.

organizations should establish conditions for group membership, identify authorized users, specify access privileges, require appropriate approval for establishing accounts, and grant access, based on need. In addition, during the annual self-assessments performed, four agencies identified weaknesses for properly issuing new user accounts. Agencies were not properly documenting and approving new user requests, in accordance with their own policies and procedures.

8a(7) Accounts are not properly terminated when users no longer require access (NIST SP 800-53, AC-2). True

Departmental regulations require that, when an individual is terminated, the account should be deleted or disabled within 48 hours of that person's departure.[58] As noted in 8a(5), we found that 12 of the 13 agencies reviewed by OIG, outside contractors, or during annual self-assessments, did not properly terminate users when their access was no longer required. For example, in one review performed this year, we found 148 active accounts for employees who had separated from the agency. Agencies were not reviewing user accounts within the Active Directory and were not following user account policy and procedures, such as deactivating or removing separated employees. As a result of these reviews, we found user accounts that remained active after an employee left service and that could result in unauthorized access, use, disclosure, disruption, modification, or destruction of information.

8a(8) Agency does not use multi-factor authentication where required (NIST SP 800-53, IA-2). True

As noted in 7a(6), we found six of seven agencies reviewed by OIG or outside contractors that did not require multi-factor authentication.

8a(9) Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01). True

We found that two of three agencies reviewed had not issued all individuals the Homeland Security Presidential Directive (HSPD)-12 credentials.[59] Currently, none of the three agencies are requiring HSPD-12 for multi-factor authentication to systems; although one agency reported that all of its employees have been issued the credentials. Each of the three agencies we reviewed reported they are waiting for the Department project to implement the multi-factor authentication. Although the original implementation date was scheduled for September 30, 2009, this project is now scheduled to be completed on September 30, 2011.

---

[58] USDA Departmental Regulation, DR 3505-003, *Access Control Policy*, dated August 11, 2009.

[59] FIPS Publication 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors states that Homeland Security Presidential Directive 12 (HSPD-12), entitled *Policy for a Common Identification Standard for Federal Employees and Contractors*, provides for a Federal standard for secure and reliable forms of identification for Federal employees and contractors. Implementation of the HSPD-12 specifies that the credential is an integrated circuit card. The card must store personalized identity information for the person to whom the card was issued. The cards will be used for electronic verification for logical access to information resources. For example, a cardholder may log in to their agency network using the PIV card; the identity established through this authentication process can be used for determining access to file systems, databases, and other services available on the network.

8a(10) Privileges granted are excessive or result in capability to perform conflicting functions (NIST SP 800-53, AC-2, AC-6). True

We found that 11 of the 13 agencies reviewed this fiscal year by OIG, outside contractors, or during annual self-assessments had granted users excessive privileges, or otherwise allowed them the capacity to perform conflicting functions. These agencies did not ensure that users were granted their access based on their work needs, and did not follow separation of duty principles, as required by NIST SP 800-53.

NIST states organizations should identify authorized users of information systems and specify access privileges, require appropriate approval, grant access based on need, periodically review accounts, provide additional scrutiny of administrative accounts, follow separation of duty principles, and utilize the concept of least privilege. We found, however, that nine agencies reported weaknesses in granting excessive privileges; six reported weaknesses in separation of duty principles; and six reported a lack of a periodic review of user accounts during their annual self-assessments.

8a(11) Agency does not use dual accounts for administrators (NIST SP 800-53, AC-5, AC-6). True

We found that six of nine agencies reviewed this fiscal year were not using dual accounts for administrators, as required by NIST SP 800-53. NIST states that a privileged user should have a second non-privileged account to support the principle of least privilege. This is commonly referred to as dual accounts for administrators. For example, in our review of one agency's Active Directory, we found 15 administrators who did not have dual accounts. In addition, the annual agency self assessments found that two other agencies had administrators without a second non-privileged user account. Our review of Departmental Regulation 3505-003 found the policy did not address dual accounts.

8a(12) Network devices are not properly authenticated (NIST SP 800-53, IA-3). True

We found that none of the six agencies reviewed by OIG or outside contractors were able to identify and properly authenticate all devices attached to its networks, as required by NIST SP 800-53. NIST states that a system should uniquely identify and authenticate devices before establishing connections. The Department was not able to provide policy or procedures to support the identity and authentication of network devices. Also, the three agencies reviewed for this audit did not provide policy or procedures. The agencies stated they could only discover a rogue device if it was connected to its network during the monthly discovery scans.[60]

S8: Continuous Monitoring Management
Section 8: Status of Continuous Monitoring Program

[60] A rogue device is one attached to the network without the agency's permission.

9. Check one:

a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

> **1. Documented policies and procedures for continuous monitoring.**
> **2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.**
> **3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.**
> **4. Provides system 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.**

b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established a continuous monitoring program. (Details of the findings are included in 9a below)

9a. If b. checked above, check areas that need significant improvement:

9a(1) Continuous monitoring policy is not fully developed. True

The Department did not have a continuous monitoring policy and the program is not scheduled for full implementation until the end of FY 2011. In addition, we found that all three agencies reviewed during this audit did not have a fully developed continuous monitoring policy that met NIST SP 800-53 requirements.

9a(2) Continuous monitoring procedures are not fully developed or consistently implemented. True

The Department and the three agencies reviewed during this audit were not able to provide procedures governing continuous monitoring. NIST SP 800-53 requires that organizations establish a continuous monitoring strategy and implement a continuous monitoring program. This includes a configuration management process for the information system and its constituent components, as well as a determination of the security impact of changes to the information system and environment of operation.

9a(3) Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST SP 800-37). True

NIST states that an organization should formulate a strategy or plan which is fully developed for entity-wide continuous monitoring.[61] The plan should consist of a comprehensive governance structure and organization-wide risk management strategy, which includes the techniques and methodologies the organization plans to employ to assess information system security risks. The strategy and plans the Department provided for developing an entity-wide continuous monitoring plan were in draft and are estimated to be completed September 2011.

9a(4) Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST SP 800-53, NIST SP 800-53A). True

NIST SP 800-53 states that Federal agencies will assess the security controls in an information system as part of the testing/evaluation process. We identified 23 of 282 systems for which the Department had not performed ongoing assessments of selected security controls in FY 2010
.

9a(5) The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST SP 800-53, NIST SP 800-53A). True

We identified one of seven agencies that did not provide the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessments reports, and POA&Ms.

S9: Contingency Planning
Section 9: Status of Contingency Planning Program

10. Check one:

a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

> **1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.**
> **2. The agency has performed an overall Business Impact Assessment.**
> **3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.**
> **4. Testing of system specific contingency plans.**

[61] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004.

5. The documented business continuity and disaster recovery plans are ready for implementation.
6. Development of training, testing, and exercises (TT&E) approaches.
7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.

c. The Agency has not established a business continuity/disaster recovery program.

10a. If b. checked above, check areas that need significant improvement:

10a(1) Contingency planning policy is not fully developed. True

We found that the Department's contingency planning policy meets NIST SP 800-53 requirements. However, we found that 1 of 22 agencies' policies reviewed did not meet NIST requirements.

10a(2) Contingency planning procedures are not fully developed or consistently implemented. True

We found that 2 of 23 agency systems we reviewed did not have fully developed and consistently implemented procedures for contingency planning. For example, during one audit conducted this year, we found that 9 of 18 field sites did not have or were unable to provide backup procedures.

10a(3) An overall business impact assessment has not been performed (NIST SP 800-34). True

The USDAs Office of Homeland Security did not provide OIG a business impact assessment.

10a(4) Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34). True

NIST states that recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption.[62] We identified 20 of 279[63] systems for which the Department had not developed organization, component, or infrastructure recovery strategies
.

10a(5) A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34). False

[62] NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, dated June 2002.
[63] Based on a CSAM run date of October 22, 2010.

No exceptions noted.

10a(6) A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34). True

We found that all 30 systems we reviewed had developed business continuity/disaster recovery plans; however, one plan had not been fully implemented.

10a(7) System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53). True

NIST SP 800-53 requires Federal agencies to develop a formal, documented contingency plan that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities in planning controls. We identified 17 of 279 systems for which the contingency plan field in CSAM was marked as "not applicable" or "in progress" and was therefore not complete

.

10a(8) Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53). True

NIST SP 800-53 requires Federal agencies to test and exercise the contingency plan for information systems, using organization-defined tests or exercises to determine the plan's effectiveness and the organization's readiness to execute the plan and initiate corrective actions. We identified 48 of 279 critical systems for which USDA had not tested its contingency plans.

10a(9) Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34,NIST SP 800-53). True

NIST SP 800-53 requires Federal agencies to test and exercise the contingency plan for the information system, using organization-defined tests or exercises to determine the plan's effectiveness and the organization's readiness to execute the plan and initiate corrective actions. We found 6 of 25 systems reviewed by OIG or outside contractors for which USDA had not fully developed training, testing, and exercise approaches.

10a(10) Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53). True

NIST SP 800-53 requires Federal agencies to test and exercise the contingency plan for the information system, using organization-defined tests or exercises to determine the plan's effectiveness and the organization's readiness to execute the plan and initiate corrective actions. Our review found that USDA had not fully implemented training, testing, and exercise approaches for 8 of 30 systems. For example, one system was last tested in 2008 and another had TBD in the Contingency Test Date Completed field

10a(11) Disaster recovery exercises were not successful revealed significant weaknesses in the contingency planning. (NIST SP 800-34). True

NIST SP 800-34 states that recovery strategies should provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger organization-level contingency plans. Our review found that USDA did not have disaster recovery exercises which were successful at revealing significant weaknesses in the contingency plan for 3 of 30 systems.

10a(12) After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34). True

NIST SP 800-34 states that all recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts. An after-action report with lessons learned should be documented and updated. Our review found that USDA did not have after-action plans that addressed issues identified during the disaster recovery exercises for 4 of 30 systems.

10a(13): Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). False

No exceptions noted.

10a(14) Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53). True

NIST SP 800-34 states that when selecting an offsite storage facility for backups, the Federal agency should select the offsite storage site in a different geographic area far enough from the organization's primary site so that the storage site will not be affected by the same disaster as the organization's primary site. During one audit conducted during FY 2010, OIG found that 16 of 18 alternate processing sites were subject to the same risks as the primary sites.

10a(15) Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). False

No exceptions noted.

10a(16) Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53). True

NIST SP 800-53 states that the organization should test backup information to verify media reliability and information integrity. During an audit conducted during the year, we found that 17 of 18 field sites had not performed regular recovery tests. In addition, for this agency, we found that only two documented backup/recovery tests were completed for over 2,400 field sites.

10a(17) Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53). False

No exceptions noted.

S10: Contractor Systems
Section 10: Status of Agency Program to Oversee Contractor Systems

11. Check one:

a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

> **1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.**
> **2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities.**
> **3. The inventory identifies interfaces between these systems and Agency-operated systems.**
> **4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that is owns and operates.**
> **5. The inventory, including interfaces, is updated at least annually.**
> **6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.**

b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.

c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities. (Details of the findings are included in 11a below)

11a. If b. checked above, check areas that need significant improvement:

11a(1) Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed. True

We found the Department did not have policies to oversee systems operated on the agency's behalf by contractors or other entities. The Department is in the process of drafting a memo on overseeing contractors' systems.

11a(2) Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed or consistently implemented. True

We found the Department did not have procedures to oversee systems operated on the agency's behalf by contractors or other entities. The Department stated that the agencies are responsible for developing their own procedures.

11a(3) The inventory of systems owned or operated by contractors or other entities is not sufficiently complete. True

We found that the Department did not have a complete inventory of its contractor systems. During the FY 2009 FISMA audit, we identified 12 systems which should have been designated as contractor systems. In FY 2010, we found that only one system designation had been changed to a contractor system. In response to the FY 2009 FISMA audit, the Department stated that it would review the systems and change the designation to contractor systems if appropriate. We found that the Department had not accomplished this review. During this audit, the Department did respond that at least 6 of those systems should have been identified as contractor systems.

11a(4) The inventory does not identify interfaces between contractor/entity-operated systems to Agency-owned and -operated systems. True

FISMA requires agencies to maintain an inventory of information systems, which includes an identification of the interfaces between each system, and all other systems or networks, including those not operated by, or under the control of, the agency.[64]

We found that the Department was not maintaining an accurate inventory of interfaces in CSAM. We reviewed 31 SSPs and then compared the list of interfaces to those documented in CSAM. We found that the Department was not accurately reporting interface/interconnections with other systems for 22 of 31 systems. Agencies were responsible for accurately documenting interface data in CSAM, but they failed to account for all interconnections. Since interfaces allow the exchange of data between two systems, it is important that security controls in each interconnected system accurately reflect the risk of inadvertent disclosure of information. Without proper documentation and testing of those interfaces, the confidentiality, integrity, and availability of the exchanged data could have been compromised without discovery.

11a(5) The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually. True

NIST specifies that organizations should review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure they are operating properly and are providing appropriate levels of protection.[65] As noted in 11a(3), the Department did not update its inventory of contractor systems in FY 2010. In addition, as noted in 11a(4), we found that the Department had not identified all interfaces.

[64] FISMA of 2002, Title III, *Information Security*, dated December 17, 2002.
[65] NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, dated August 2002.

11a(6) Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., certification and accreditation requirements). True

Departmental procedures require that deactivated systems which have reached the final phase in the System Development Life Cycle (SDLC) should be retired. Agencies must contact OCIO in writing, specifically stating that the retired/deactivated system is no longer processing any transactions or information, and has been completely removed from the network.[66] All information, including the deactivation date, must be completed for the system inventory update. During our review, we found that the documented reason for one system's retirement was "services to the end user and partner agencies will continue unabated as the contracted service will continue to operate without change. This retirement is strictly an administrative change in status in the CSAM and EAR repositories." According to this statement, the change is to remove the system from CSAM and FISMA reporting.

11a(7) Systems owned or operated by contractors and entities do not meet NIST and OMB's FISMA requirements (e.g., certifications and accreditation requirements). True

As noted in 11a(6), we did note one system that appears to be a contractor system that is still operating but that was removed from CSAM.

11a(8) Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained. True

We found that the Department did not maintain an inventory of interface agreements. NIST SP 800-47 states that a Memorandum of Understanding (MOU) defines the responsibilities of the participating organizations and that the joint planning team should identify and examine all relevant technical, security, and administrative issues surrounding the proposed interconnection. This information may be used to develop an Interconnection Security Agreement (ISA) and a Memorandum of Understanding or Agreement (MOU/A) (or an equivalent document). Twenty-two of the 31 systems reviewed during this audit did not have the required MOU/ISA.

[66] SOP-ISD-007, *Information Technology Inventory Reconciliation and Certification-Standard Operating Procedure*, April 28, 2009.