



United States Department of Agriculture
Office of Inspector General





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



DATE: November 15, 2011

The Honorable Jacob Lew
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 2011 Federal Information Security Management Act Report
(Audit Report 50501-0002-12)

This report presents the results of our audits of the Department of Agriculture's (USDA) efforts to improve the management and security of its information technology (IT) resources. USDA and its agencies have taken actions to improve the security over their IT resources; however, additional actions are still needed to establish an effective security program.

Sincerely,

A handwritten signature in black ink, appearing to read "Phyllis K. Fong". The signature is fluid and cursive.

Phyllis K. Fong
Inspector General

Table of Contents

Executive Summary	1
Recommendation Summary.....	8
Background & Objectives	10
Background.....	10
Objectives.....	11
Scope and Methodology.....	12
Abbreviations	14
Exhibit A: Office of Management and Budget (OMB)/Department of Homeland Security (DHS) Reporting Requirements and U. S. Department of Agriculture (USDA) Office of Inspector General (OIG) Position.....	16
Exhibit B: Sampling Methodology and Projections: Audit Number 50501- 0002-12 FISMA FY2011	55

U. S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2011 Federal Information Security Management Act (FISMA) (Audit Report 50501-0002-12)

Executive Summary

The Department of Agriculture (USDA) has made improvements in its information technology (IT) security over the last decade, but many longstanding weaknesses remain. In our Federal Information Security Management Act (FISMA) audits for fiscal years (FY) 2009 and 2010, Office of Inspector General (OIG) made 33 recommendations for improving the overall security of USDA's systems. By the end of FY 2011, the Department had adequately remediated and closed only 6 recommendations, leaving 27 to be addressed. OIG has reported on many of these remaining recommendations since 2001 when we first detailed material weaknesses in the design and effectiveness of USDA's overall IT security program.

USDA is a large, complex organization that includes 33 separate agencies and staff offices, most with their own IT infrastructure. In 2009, in order to mitigate continuing material weaknesses, we reported that the Department should concentrate its efforts on a limited number of priorities instead of attempting to achieve numerous goals simultaneously in short timeframes. We recommended that USDA and its agencies work together to define and accomplish one or two critical objectives before proceeding to the next set of priorities. During FY 2011, we observed increased evidence of coordination, but the Department was not making measurable progress in approaching this problem collaboratively. For example, during FYs 2010 and 2011, the Office of the Chief Information Officer (OCIO) received increased budgetary authority to enhance USDA's IT security. The Department funded 14 separate projects with none of these projects being fully implemented during FY 2011; instead, funding was cut and nearly all of the projects were significantly scaled back, pushing implementation dates further into the future.¹ USDA needs to undertake a manageable number of its highest priority projects and it needs to show measureable progress towards the milestones for each active project. USDA's inability to complete projects in a timely manner continues to hinder its progress towards improving its security posture.

We acknowledge, though, that USDA has made progress through FY 2011 in several key areas; including system security documentation. The Department improved the overall quality of this documentation by issuing detailed guidance, strengthening its quality review process for reviewing that documentation, and ensuring more consistent formatting and recording when it updates that guidance. USDA also finished deploying a suite of network monitoring and detection tools, which should further enhance the security of its networks. The suite is an integrated security solution that provides the foundation for enterprise-wide security monitoring,

¹ We based this project count on information provided by the OCIO as part of a document request pertaining to audit: *U.S. Department of Agriculture (USDA) Audit of the Chief Information Officer's FY 2010 Appropriations* (Audit 88401-0001-12).

detection, and protection. Once USDA deploys adequate resources to properly configure and completely monitor these tools, the Department's security posture should greatly improve.

In addition, USDA has made progress in improving its identity and access management program by developing a system that, once completed, will integrate human resource systems, logical access security, and physical access security.² Currently, the system is integrated³ with 425 of 467 Department web applications—further integration is in development.⁴ The incident response and reporting documentation and tracking process also improved between our FY 2010 and FY 2011 FISMA audits. The Department decreased its error rate from 100 percent in FY 2010 to 44 percent in FY 2011 through increased adherence to documented procedures. This improvement is especially remarkable because OCIO personnel stated the incident response and reporting division's staff decreased from 13 to 6 full-time employees due to a reduced FY 2011 budget.

This report constitutes OIG's independent evaluation of the Department's IT security program and practices, as required by FISMA. OIG's review is based on the questions provided by the Office of Management and Budget (OMB)/Department of Homeland Security (DHS) for the FY 2011 FISMA review. These questions are designed to assess the status of the Department's security posture during FY 2011. For the FISMA review, OMB/DHS's framework requires OIG to audit processes, policies, and procedures that had already been implemented and documented, and were being monitored during FY 2011. While USDA's planned activities may improve its security posture in the future, we could not evaluate these initiatives as part of our FY 2011 FISMA review because they were not fully operational during the year.

The following summarizes the key matters discussed in exhibit A of this report, which contains OIG's responses to OMB/DHS' questions. These questions were defined in OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (September 14, 2011) and DHS Federal Information Security Memorandum 11-02, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (August 24, 2011). The universe of systems and agencies reviewed varied during each audit or review reflected in this report.

² NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (September 1996) states logical access is the ability to explicitly enable or restrict access. Logical access controls can prescribe not only who or what is to have access to a specific system resource but also the type of access that is permitted.

³ Integration is the merging of web applications with functions of the identity, credential, and access management system such as using a single access credential. This integration allows centralized account access rights and privileges to be monitored and tracked.

⁴ There can be multiple applications per system. Even though there are only 257 USDA systems, the number of applications running on those systems is greater.

To address the FISMA metrics, OIG reviewed systems and agencies, OIG independent contractor audits, annual agency self-assessments, and various OIG audits throughout the year.⁵ Since the scope of each review and audit differed, we could not use every review or audit to address each question.

Agency officials are responsible for ensuring all systems meet Federal and Departmental requirements and documenting agency compliance in the Cyber Security Assessment and Management (CSAM) system.⁶ OCIO is responsible for ensuring that agencies are compliant with Federal and Departmental guidance and are reporting aggregate results during the annual FISMA reporting cycle. The Risk Management Framework (RMF) is a new publication by the National Institute of Standards and Technology (NIST). The publication promulgates a common framework which is intended to improve information security, strengthen risk management, and encourage reciprocity between Federal agencies.⁷ The publication transforms the traditional Certification and Accreditation (C&A) process into a six-step RMF process.⁸ Although the process has changed, we continue to find:

- USDA does not have a RMF policy or fully developed procedures. According to the Department, this occurred because the governance team which was overseeing RMF was disbanded due to budget cuts. As a result, USDA cannot ensure that it has a consistent and effective approach to risk management that applies to all risk management processes and procedures. However, in August 2011, USDA did issue a guide that addresses parts of the six-step RMF process. The guide also clarifies the steps necessary to complete the C&A process. Agencies are required to submit their system C&A packages and all supporting documents to the Department for an indepth review (i.e., a concurrency review). During this review, USDA ensures that the documentation prepared to support system accreditation is complete, accurate, reliable, and meets NIST and other mandated standards.⁹

⁵ Agency annual self-assessments derive from OMB Circular A-123, which defines *Management's Responsibilities for Internal Control* in Federal agencies (December 21, 2004). The circular requires agency's management to annually provide assurances on internal control in Performance and Accountability Reports. During annual assessments, agencies take measures to develop, implement, assess, and report on internal controls, and take action on needed improvements.

⁶ 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 staff to: (1) manage system inventory, interfaces, and related system security threats and risks; (2) enter system security data into a single repository to ensure all system security factors are adequately addressed; (3) prepare annual system security documents, such as security plans, risk analyses, and internal security control assessments; and (4) generate custom and predefined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. This includes agency-owned systems as well as those operated by contractors on the agency's behalf.

⁷ NIST Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010), was developed by the Joint Task Force Transformation Initiative Working Group.

⁸ C&A is a process mandated by OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (November 28, 2000). The process requires that IT system controls be documented and tested by technical personnel and that the system be given formal authority to operate by an agency official.

⁹ 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 agreed-upon security controls.

- Overall, we found that the C&A process improved. USDA completed its indepth document reviews and appropriately returned C&As to agencies that did not meet NIST requirements. However, we did find that improvements are still needed. Specifically, the following C&A documentation did not meet NIST requirements: (1) systems were not properly categorized; (2) risk assessments did not adequately substantiate testing; (3) system security plan (SSP) controls were not implemented properly and did not sufficiently address each control; and (4) security assessment reports did not provide evidence to show that controls had been tested. As a result, USDA cannot be assured that all system controls had been documented and tested, and that systems were operating at an acceptable level of risk.
- Additionally, we found 15 of 55 systems were not recertified as required in FY 2011.¹⁰ This occurred because agencies had not submitted documents for recertification. As a result, these systems are operational but without proper certification, which leaves the agencies and the Department vulnerable because the systems have not been through proper testing.

USDA has established and is maintaining a security configuration management program, but further improvements are needed. Specifically, we found that the Department has established adequate policy and issued a memo stating that USDA will use the Federal standard baseline configurations for operating systems. However, agencies have not completely scanned their networks, corrected critical and high-risk vulnerabilities, or followed established baselines when configuring servers. For example, our review found that over 45 percent of the Department's Windows 2003 server configuration settings did not comply with current Federal guidelines.¹¹ We also found that one agency was not scanning over 1,600 machines on a monthly basis as required by Departmental guidance.¹² This occurred because the network and security groups were not communicating.¹³

Although USDA's incident handling has improved, we continue to find that the Department is not consistently following its own policy and procedures in regard to incident response and reporting. Our statistical review determined that 29 of 66 incidents that occurred during the year were not handled in accordance with Departmental procedures.¹⁴ Additionally, our review

¹⁰ 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. Recertification is required periodically or as part of a continuous monitoring program.

¹¹ Defense Information Systems Agency, *Windows 2003 Security Technical Implementation Guide Overview* (August 27, 2010). The NIST site incorporates checklists from various Federal entities including the Department of Defense.

¹² USDA Departmental Manual (DM) 3530-001, *USDA Vulnerability Scan Procedures* (July 20, 2005).

¹³ NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009).

¹⁴ 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).

determined that the Department has insufficient incident detection and monitoring coverage. From September 2010 through April 2011, USDA installed an incident detection toolkit, which alerts the Department to potential cyber-related incidents. During FY 2011, USDA had three employees who were responsible for monitoring the daily data, calibrating security tools, and analyzing incidents. The employees were able to analyze and process approximately 15 incidents per week. However, the Department stated that, with the appropriate resources, it would have been able to process up to 150 incidents per week. NIST SP 800-53 requires the organization to report suspected security incidents and related information to appropriate organizational authorities. USDA has assigned this responsibility to the Agriculture Security Operations Center (ASOC). According to the Department, it was aware of the up to 150 weekly security-related incidents and that it did not have sufficient resources to investigate or report the majority of them.

Department policy met all NIST SP 800-53 requirements for annual security awareness training.¹⁵ However, USDA lacks policy and procedures to govern specialized security training for personnel with significant information security responsibilities. In addition, we found that not all personnel received the required annual security awareness training and specialized security awareness training.¹⁶ Specifically, of the three agencies reviewed, we did not find evidence that 1,383 of 10,904 users with login privileges had completed their annual security awareness training. We also found that 4 of 33 users identified as requiring specialized security training did not have documented proof that they received the training during FY 2011. As a result, USDA IT systems bear an increased risk of being compromised because users are allowed access to Department and agency information systems without the required training.

USDA did not have effective policy and procedures for reporting IT security deficiencies in CSAM. We found that plans of action and milestones (POA&Ms) did not include all known security weaknesses.¹⁷ For example, the Department requires an agency to create a POA&M when an identified vulnerability cannot be remediated within 30 days.¹⁸ However, our testing at 3 agencies showed 1,224 vulnerabilities that were over 30 days old without POA&Ms. In addition, our review of POA&Ms within CSAM found that agencies were not tracking the source (e.g., program review, Inspector General (IG) audit, etc.) of the security weaknesses as required by OMB.¹⁹ Specifically, we found that 721 POA&Ms (34.4 percent of the total POA&Ms in

¹⁵ DM 3545-001, *Computer Security Training and Awareness* (February 17, 2005).

¹⁶ NIST SP 800-53 requires organizations to provide basic security awareness training to all users. Additionally, it requires organizations to provide role-based specialized security training related to specific roles and responsibilities for: information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software. Organizations are to determine the appropriate content of security training and the specific requirements of the organization and the information systems to which personnel have authorized access.

¹⁷ A POA&M is a tool that identifies tasks needing to be accomplished to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. It details resources required to accomplish the elements of the plan, milestones for meeting the task, and scheduled completion dates for the milestones. The goal of a POA&M should be to reduce the risk of the weakness identified.

¹⁸ *Plan of Action and Milestones Management Standard Operating Procedures, CPO-SOP 002* (June 29, 2011).

¹⁹ OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

FY 2011) did not track the source of security weaknesses. We also found 674 of 1,774 POA&Ms had an associated cost of zero dollars to remediate the identified weakness, instead of the necessary amount to remediate the weakness as required by OMB M-04-25 guidance. Additionally, we noted that the Department is not tracking and reviewing POA&Ms as required by the Department's standard operating procedures (SOP). Finally, we were unable to verify that the Department completed the required reviews of closed POA&Ms in FY 2011 because there was inaccurate or inconsistent evidence supporting the reviews.

USDA's remote access program needs significant improvements. Our review identified policy that did not meet NIST requirements.²⁰ The Department stated that procedures were the responsibility of the agencies, but we found that five of seven agencies reviewed by independent contractors did not consistently implement remote access procedures. In addition, we found agencies did not follow the policy that did exist. For example, USDA requires multi-factor authentication for all remote access (i.e., two means of identification).²¹ However, we found that 8 of 10 agencies (reviewed by OIG, independent contractors, and agency annual self-assessments) did not have multi-factor authentication properly implemented for remote access. In addition, we found that agencies were not adequately encrypting laptop devices. For example, one agency had failed to encrypt 341 laptop devices because procedures were inadequate to ensure this was done for newly deployed hardware.

USDA developed an account and identity management policy, but it was not sufficiently detailed or consistently implemented.²² In particular, the Department's policy did not fully meet NIST SP 800-53 requirements; the Department procedures for managing accounts were not fully developed; and agencies had not implemented account management with the proper security settings.²³ The policy is in draft and the Department will begin developing the procedures next. As a result of the inadequate policy and procedures, agencies failed to consistently implement security settings. For example, we found former employees with active accounts, users with excessively elevated account privileges, and administrator accounts that did not follow the principle of granting the fewest privileges necessary for users to perform their work. Agencies have documented procedures, but are failing to follow them.

USDA has established an enterprise-wide continuous monitoring program that assesses the security state of information systems, but the Department needs to make significant improvements. Specifically, we found that USDA had not fully developed a strategy or plan for enterprise-wide continuous monitoring, and that ongoing assessments of security controls had not been performed. The Department's continuous monitoring policy is currently in draft and is expected to be released in December 2011. In addition, we found 48 of 257 systems where

²⁰ NIST SP 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security* (June 2009).

²¹ USDA Departmental Regulation (DR) 3505-003, *Access Control Policy* (August 11, 2009). Multi-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as "something you have" and "something you know."

²² DR 3505-003, *Access Control Policy* (August 11, 2009); DR 3180-001, *Information Technology Network Standards* (September 30, 2008); and DM 3535-001, *USDA's C2 Level of Trust* (February 2005).

²³ *USDA Identity, Credential and Access Management (ICAM) Identity Lifecycle Management Handbook* (June 2011).

ongoing assessments of selected security controls had not been performed in FY 2011 as required by NIST SP 800-53. The Department stated that it lacks the resources to implement robust, enterprise-wide continuous monitoring capabilities. As a result, the Department cannot effectively detect compliance and determine if implemented security controls within an information system are effective.

USDA has established and is maintaining an enterprise-wide business continuity/disaster recovery program, but it needs to make significant improvements. Specifically, the Department's contingency policy and procedures did not meet NIST 800-53 requirements because they have not been updated to include the new elements.²⁴ We found the template provided by the Department to the agencies for contingency planning purposes did not contain all of NIST's required elements.²⁵ We also found that contingency plans were incomplete. Based on our sample results for 3 agencies, we estimate that 22 systems (about 59 percent) had missing or incomplete contingency plans.²⁶ In addition, we identified 33 of 257 systems for which USDA system contingency plans were not tested during FY 2011.

USDA did not have policy and procedures to oversee systems that contractors or other entities operated on agencies' behalf. During our FY 2009 FISMA audit, we identified systems that should have been designated as contractor systems. In response, the Department stated that it would review the systems and change the designation to contractor systems if appropriate. Due to the missing policy and procedures, we found seven systems were still not included in the inventory of contractor systems. FISMA requires USDA to maintain an inventory of its information systems that, among other information, identifies interfaces between each system and all other systems or networks, including those not operated by, or under the control of, the agency.²⁷ During our review, we also found 18 of 18 systems had incorrectly reported their interconnections to other systems. Additionally, OIG found that USDA's new cloud email service was not included in the official Department inventory and was not designated as a contractor system.²⁸

Our testing of USDA's capital planning process determined that the Department has established and maintains a security capital planning and investment program for information security.²⁹ However, one exception was identified in the Departmental capital planning policy.³⁰ Specifically, the policy lacked a description of what constitutes a "major IT investment" according to the capital planning process.

²⁴ DM 3570-001, *Disaster Recovery and Business Resumption Plans* (February 17, 2005).

²⁵ *USDA Contingency Plan template* (March 2011).

²⁶ We are 95 percent confident that between 15 (40 percent) and 29 systems (78 percent) had missing or incomplete contingency plans. Additional sample analysis information is presented in exhibit B.

²⁷ FISMA of 2002, Title III *Information Security* (December 17, 2002).

²⁸ Cloud computing is a model for enabling network access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NIST SP 800-145, *The NIST Definition of Cloud Computing* (September 2011).

²⁹ Capital planning and investment control (CPIC) is a systematic approach to selecting, managing, and evaluating information technology investments. CPIC is mandated by the Clinger Cohen Act of 1996 and requires Federal agencies to focus more on the results achieved through IT investments while streamlining the Federal IT procurement process (www.ocio.usda.gov/cpic/index.html).

³⁰ DM 3560-000, *CPIC for Security Table of Content* (February 17, 2005) and DM 3560-001, *Security Requirements for CPIC* (February 17, 2005).

The below recommendations are new for FY 2011. Because 27 recommendations from FY 2009 and FY 2010 remain without final closure (or were closed improperly), we have not made any repeat recommendations.³¹ However, OIG noted that 25 of those recommendations have exceeded their estimated completion date. If the plans initiated to close out the FY 2009 and 2010 recommendations are no longer achievable due to budget cuts or other reasons, then OCIO needs to update those closure plans and request a change in management decision per Departmental guidance.³²

Recommendation Summary

1. Develop and implement an effective plan to mitigate the IT material weaknesses within the Department in cooperation with the agencies. Ensure the plan includes prioritized tasks, defined goals, and realistic timeframes. The Department and its agencies, working in cooperation, should define and accomplish one or two critical objectives prior to proceeding on to the next set of priorities.
2. Develop a Risk Management policy and associated procedures that fully comply with NIST.
3. Develop monitoring procedures to verify that monthly vulnerability scans are completed as required by Departmental guidance.
4. Develop monitoring procedures to verify that all Department and agency network devices are configured in accordance with NIST SP 800-53.
5. Update the current incident response and reporting procedures to reflect current practices. Additionally, the Department needs to allocate appropriate resources to the ASOC allowing it to operate effectively in mitigating cyber related incidents.
6. Deploy adequate resources to monitor and configure new security tools and then adequately report and close the related incidents.
7. Develop monitoring procedures to appropriately report the status of USDA employees being trained to meet their information security awareness needs.
8. Actively manage the POA&M process, which includes tracking and reviewing POA&Ms in accordance with its recently issued SOP.

³¹ We found that two recommendations were closed without final action truly being achieved. For example, the Department closed out the prior recommendation to prioritize and accomplish one or two tasks before moving forward with another task. However, as noted in this report, our review found that OCIO is still trying to accomplish many tasks simultaneously.

³² USDA Departmental Regulation (DR) 1720-001, *Audit Follow-up and Management Decision* (November 2, 2011).

9. Update the contingency plan template to adequately address all NIST SP 800-34 requirements.

10. Update USDA's Capital Planning policy to incorporate a definition of a "major IT investment" so that agencies have a documented description to use.

Background & Objectives

Background

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

On December 17, 2002, the President signed into law the e-Government Act (Public Law 107-347), which includes Title III, FISMA. FISMA permanently reauthorized the framework established by the *Government Information Security Reform Act (GISRA)* of 2000, which expired in November 2002. FISMA continued the annual review and reporting requirements introduced in GISRA, and also included new provisions that further strengthened the Federal Government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems. NIST was tasked to work with agencies in developing those standards as part of its statutory role in providing technical guidance to Federal agencies.

FISMA supplements the information security requirements established in the *Computer Security Act* of 1987, the *Paperwork Reduction Act* of 1995, and the *Clinger-Cohen Act* of 1996. FISMA consolidated these separate requirements and guidance into an overall framework for managing information security. It established new annual reviews, independent evaluations, and reporting requirements to ensure agencies implemented FISMA. It also established how OMB and Congress would oversee IT security.

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

Each agency must establish a risk-based information security program that ensures information security is practiced throughout the lifecycle of each agency's 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 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 compliance assessment. The evaluations are to be performed by the agency's IG or an independent evaluator, and the results of these evaluations are to be reported to OMB.

Objectives

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

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

Scope and Methodology

The scope of our review was Departmentwide and included agency IT audit work completed during FY 2011. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Fieldwork for this audit was performed remotely at USDA locations throughout the continental United States from May 2011 through October 2011. In addition, this report incorporates audits done throughout the year by OIG. Testing was conducted at offices in the Washington, D.C. area, and Kansas City, Missouri. Additionally, we included the results of IT control testing and compliance with laws and regulations performed by contract auditors at seven additional USDA agencies. In total, our FY 2011 audit work covered 15 agencies and staff offices:

- Agricultural Marketing Service (AMS),
- Animal and Plant Health Inspection Service (APHIS),
- Departmental Management (DM),
- Food and Nutrition Service (FNS),
- Forest Service (FS),
- Farm Service Agency (FSA),
- Food Safety and Inspection Service (FSIS),
- National Agricultural Statistics Service (NASS),
- National Finance Center (NFC),
- National Institute of Food and Agriculture (NIFA),
- National Information Technology Center (NITC),
- Natural Resources Conservation Service (NRCS),
- Office of the Chief Information Officer (OCIO),
- Rural Development (RD), and
- Risk Management Agency (RMA).

These agencies and staff offices operate approximately 200 of the Department's estimated 257 general support and major application systems.

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

- Consolidated the results and issues from our prior IT security audit work and the work contractors performed on our behalf. Contractor audit work consisted primarily of audit procedures found in the U.S. Government Accountability Office's (GAO) *Financial Information System Control Audit Manual*;
- 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 M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (September 14, 2011);
- Performed detailed testing specific to FISMA requirements at selected agencies, as detailed in this report; and
- Performed statistical sampling on testing where appropriate. Additional sample analysis information is presented in exhibit B.

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

Abbreviations

AMS	Agricultural Marketing Service
APHIS	Animal and Plant Health Inspection Service
ASOC	Agriculture Security Operations Center
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CIRT	Computer Incident Response Team
CSAM	Cyber Security Assessment and Management
CIO	Chief Information Officer
CISO	Chief Information Security Office
CPIC	Capital Planning & Investment Control
DHS	Department of Homeland Security
DM	Departmental Management or USDA Department Manual
DR	USDA Departmental Regulation
DoD	Department of Defense
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
FNS	Food and Nutrition Service
FS	Forest Service
FSA	Farm Service Agency
FSIS	Food Safety and Inspection Service
FY	Fiscal Year
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
HSPD-12	Homeland Security Presidential Directive-12
ICAM	Identity, Credential and Access Management
IG	Inspector General
ISA	Interconnection Security Agreement
IT	Information Technology
MOU	Memorandum of Understanding
NASS	National Agricultural Statistics Service

NCSD..... National Cyber Security Division
NFC..... National Finance Center
NIFA National Institute of Food and Agriculture
NIST..... National Institute of Standards and Technology
NITC National Information Technology Center
NRCS Natural Resources Conservation Service
OCIO..... Office of the Chief Information Officer
OIG Office of Inspector General
OMB Office of Management and Budget
PIV Personal Identify Verification
POA&M..... Plan of Action and Milestones
RD..... Rural Development
RMA Risk Management Agency
RMF Risk Management Framework
SAR..... Security Assessment Report
SOP Standard Operating Procedures
SP Special Publication
SSP System Security Plan
TT&E Test, Training, and Exercise
US-CERT US-Computer Emergency Readiness Team
USDA..... Department of Agriculture

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

OMB/DHS' questions are set apart by boldface in each section. OIG checks items on OMB/DHS' list, boldfacing and underlining the relevant text. We answer direct questions with True or False.

The universe of systems and agencies reviewed varied during each audit or review in this report. As part of Federal Information Security Management Act (FISMA), OIG reviewed systems and agencies, audit work conducted for OIG by independent public accounting firm contractors, annual agency self-assessments, and various OIG audits conducted throughout the year.³³ Since the scope of each review and audit differed, we could not use every review or audit to answer each question.

The audit team reviewed multiple areas of FISMA. We incorporated statistical sampling for four FISMA areas. Each of the four areas was represented by the relevant universe associated with it. The specific designs are summarized in exhibit B.

S1: Risk Management

Section 1: Risk Management

Check one: (1.a, 1.b, or 1.c)

1.a. The agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable National Institute of Standards and Technology (NIST) guidelines. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

1.a(1). Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

1.a(2). Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev. 1.

1.a(3). Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in

³³ Agency annual self-assessments are a result of OMB Circular A-123, *Management's Responsibility for Internal Control (December 21, 2004)* which defines management's responsibility for internal controls in Federal agencies. The Circular requires agencies' management to annually provide assurances on internal control in its Performance and Accountability Report. During the annual assessment, agencies take measures to develop, implement, assess, and report on internal control, and to take action on needed improvements.

NIST 800-37, Revision 1.

1.a(4). Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.

1.a(5). Categorizes information systems in accordance with government policies.

1.a(6). Selects an appropriately tailored set of baseline security controls.

1.a(7). Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.

1.a(8). Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

1.a(9). Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

1.a(10). Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

1.a(11). Information system-specific risks (tactical), mission/business-specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.

1.a(12). Senior officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).

1.a(13). Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

1.a(14). Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.

1.b. The agency has established and is maintaining a risk management program. However, the agency needs to make significant improvements as noted below.

1.c. The agency has not established a risk management program.

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

1.b(1). Risk management policy is not fully developed. True

We found the Department had not developed a risk management policy. According to the Department, this occurred because the governance team which was overseeing the risk management framework (RMF) was disbanded due to budget cuts. As a result, USDA cannot

ensure that it had a consistent and effective approach to risk management that applies to all risk management processes and procedures.

1.b(2). Risk management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53). True

We found that the Department did not have risk management procedures fully developed. As of August 8, 2011, the Department had a guide that addresses parts of the six-step RMF process. The guide also clarifies the steps necessary to complete the C&A process. Agencies are required to submit their system C&A packages and all supporting documents to the Department for an indepth review (i.e., a concurrency review). During this review, USDA ensures that the documentation prepared to support system accreditation is complete, accurate, reliable, and meets NIST and other mandated standards.³⁴ According to the Department, the procedures were not fully developed because the governance team which was overseeing the RMF was disbanded due to budget cuts. As a result, the Department could not ensure that it had a consistent and effective approach to risk management that applies to all risk management processes and procedures.

1.b(3). Risk management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53). True

We found that the Department did not fully develop risk management procedures (as stated in 1.b(2)). Because of this, we could not verify that procedures were consistently implemented in accordance with government policies.

1.b(4). A comprehensive governance structure and agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP 800-53). True

We found that the Department did not have a comprehensive governance structure or a fully developed agency-wide risk management strategy. Since the Department did not have a risk management policy (as stated in 1.b(1)) or fully developed procedures (as stated in 1.b(2)), we could not verify that a comprehensive governance structure and agency-wide risk management strategy existed.

1.b(5). Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53). True

We found the Department did not have a risk management policy that addressed the mission and business process perspective. Since the Department did not have a risk management policy (as stated in 1.b(1)) or fully developed procedures (as stated in 1.b(2)), we could not verify that the risks from a mission and business process perspective were addressed.

³⁴ Security accreditation is the official management decision made 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 agreed-upon security controls.

1.b(6). Information systems are not properly categorized (FIPS 199/SP 800-60). True

We generated a report from Cyber Security Assessment and Management (CSAM), which identified the categorization level for each of the Department's systems.³⁵ 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 SP 800-60 and found that 15 of 257 systems indicated a lower categorization than was recommended during the C&A process without adequate justification for the reduction in categorization level.³⁶ Therefore, systems were not properly categorized. NIST SP 800-60 requires that any adjustments to the recommended impact levels be documented and include justification for the adjustment. However, we found the provided justifications to be the same for all 15 systems, though the purposes of the systems were very diverse.

1.b(7). Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/SP 800-53). True

NIST SP 800-53 recommends a set of minimum baseline security controls contingent upon the system's overall categorization.³⁷ The lower the category, the fewer controls required. Therefore, the incorrect categorization noted in 1.b(6) led to inadequate controls being implemented for those 15 systems. NIST SP 800-60 states that an incorrect information system impact analysis could 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).

1.b(8). Risk assessments are not conducted in accordance with government policies (SP 800-30). True

The risk assessments we reviewed were not conducted in accordance with Government policies. Specifically, our review found 10 of 10 systems did not have sufficient documentation to substantiate the testing.³⁸ Based on the statistical sample results, we estimate that none of the

³⁵ CSAM is a comprehensive system developed by the Department of Justice, which can help in achieving FISMA compliance. CSAM provides a vehicle for the Department, agencies, system owners, and security staffs to (1) manage their system inventory, interfaces, and related system security threats and risks; (2) enter system security data into a single repository to ensure all system security factors are adequately addressed; (3) prepare annual system security documents, such as security plans, risk analyses, and internal security control assessments; and (4) generate custom and predefined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. This includes agency-owned systems or those operated by contractors on the agency's behalf.

³⁶ NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Vol. 1 (August 2008).

³⁷ NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Rev. 3 (August 2009).

³⁸ We selected a simple random sample of 25 systems for review, which would satisfy various possible combinations of error rates, confidence levels, and tolerable error rates. We would consider stop-or-go if for a given criterion there are zero plans with an exception after the first 15 plans are reviewed, or after the first 10 plans are reviewed, if all plans have an exception. Additional sample analysis information is presented in exhibit B.

55 risk assessments were conducted in accordance with Government policies.³⁹ This occurred because the system-generated documents that were being used did not encompass the primary steps required by NIST SP 800-30.⁴⁰ As a result, the Department could not ensure agencies were properly managing their IT-related mission risks.

1.b(9). Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53). True

NIST SP 800-53 recommends a set of minimum baseline security controls based on the system's overall categorization. The lower the category, the fewer controls required. Therefore, the incorrect categorization noted in 1.b(6) led to inadequate controls being implemented for those 15 systems. NIST SP 800-60 states that the value of information security categorizations is to enable agencies to proactively implement appropriate information security controls based on the assessed potential impact to information confidentiality, integrity, and availability.

1.b(10). The communication of information system-specific risks, mission/business-specific risks and organizational level (strategic) risks to appropriate levels of the organization is not in accordance with government policies. False

No exception noted. We found the Department communicated information system-specific risks, mission/business-specific risks, and organizational level (strategic) risks to appropriate levels of the organization in accordance with Government policies.

1.b(11). The process to assess security control effectiveness is not in accordance with government policies (SP 800-53A). False

No exception noted. We found that the Department had issued guidance to agencies on 33 key controls that should be tested annually.⁴¹

1.b(12). The process to determine risk to agency operations, agency assets, individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37). False

No exception noted. We found the Department had a process to determine the risk to agency operations, agency assets, and individuals, or to authorize information systems to operate.

³⁹ We are 95 percent confident that at least 76.3 percent of the risk assessments in our audit universe were not conducted in accordance with Government policies. Additional sample analysis information is presented in exhibit B.

⁴⁰ NIST SP 800-30, *Risk Management Guide for Information Technology Systems* (July 2002).

⁴¹ OCIO established a working group to help select financially significant, key system, and common controls for the Department for annual testing. Security controls were selected from the 17 control families of NIST SP 800-53, Rev. 3.

1.b(13). The process to continuously monitor changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37). True

NIST SP 800-53 states that the organization will assess the security controls in an information system as part of the testing/evaluation process. However, we identified 48 of 257 systems where ongoing assessments of selected security controls had not been performed in FY 2011.

1.b(14). Security plan is not in accordance with government policies (SP 800-18, SP 800-37). True

The System Security Plans (SSP) we reviewed were inadequate and not in accordance with Government policies.⁴² Specifically, the security controls were not implemented properly and did not sufficiently address each control. For example, 12 of 12 systems stated the control involving Security Awareness Training was an inherited control. However, this control could not be inherited because procedures had to be developed by the agencies as required by Departmental policy. Based on the statistical sample results, we estimate that all 55 SSPs are inadequate.⁴³ If all controls were not implemented effectively, systems may be inadequately protected.

1.b(15). Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37). True

The Department's Security Assessment Reports (SARs) we reviewed failed to meet the minimum security required by NIST SP 800-37.⁴⁴ Our review of SARs found that 10 of 10 were not conducted in accordance with Government policies. For example, our review found no evidence that the required controls had been tested. Additionally, NIST SP 800-37 requires a security assessment plan to be included with the SAR which provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. We found during our review that security assessment plans were not included in the Department's SARs. Based on the sample results, we estimate that all 55 SARs failed to meet the minimum NIST security requirements.⁴⁵ As a result, USDA cannot be assured that all system controls had been documented and tested, and that systems were operating at an acceptable level of risk.

⁴² 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* (February 2006).

⁴³ We are 95 percent confident that at least 80.3 percent of the SSPs for systems in the audit universe are inadequate. Additional sample analysis information is presented in exhibit B.

⁴⁴ NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010).

⁴⁵ We are 95 percent confident that at least 76.4 percent of the SARs for systems in the audit universe are inadequate. Additional sample analysis information is presented in exhibit B.

1.b(16). Accreditation boundaries for agency information systems are not defined in accordance with government policies. False

No exception noted. We found all 18 systems reviewed met NIST SP 800-18 accreditation boundaries.⁴⁶

S2: Configuration Management

Section 2: Configuration Management

Check one: (2.a, 2.b, or 2.c)

2.a. The agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

2.a(1). Documented policies and procedures for configuration management.

2.a(2). Standard baseline configurations defined.

2.a(3). Assessing for compliance with baseline configurations.

2.a(4). Process for timely, as specified in agency policy or standards, remediation of scan result deviations.

2.a(5). For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

2.a(6). Documented proposed or actual changes to hardware and software configurations.

2.a(7). Process for timely and secure installation of software patches.

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

2.c. The agency has not established a security configuration management program.

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

**2.b(1). Configuration management policy is not fully developed (NIST 800-53: CM-1).
False**

No exception noted. We found that the Department's configuration management policy met NIST SP 800-53 requirements.

⁴⁶ NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* (February 2006).

2.b(2). Configuration management procedures are not fully developed (NIST 800-53: CM-1). 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 and independent contractors found that three of six agencies reviewed did not have configuration management procedures or the procedures were not fully developed. For example, one of the agencies was unable to provide any documented procedures and a second agency did not have all required NIST SP 800-53 elements in its procedure.

2.b(3). Configuration management procedures are not consistently implemented (NIST 800-53: CM-1). True

As noted in 2.b(2), OIG and independent contractors found that three of six agencies either did not have configuration management procedures or that the procedures were not consistently implemented.

2.b(4). Standard baseline configurations are not identified for software components (NIST 800-53: CM-2). False

No exception noted. NIST SP 800-53, under configuration control, requires the organization to develop, document, and maintain a current baseline configuration of the information system. The Department had issued a memo on May 26, 2011, stating that NIST SP 800-70 would be the official baseline configuration guide repository for operating systems in use at USDA.⁴⁷ Our review of three agencies found them using the NIST baseline configurations for all current operating systems.

2.b(5). Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2). True

Federal Information Processing Standard (FIPS) 200 requires the organization to establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.⁴⁸ We found 3 of 12 systems did not adequately develop hardware baseline configurations. Also, one agency was identified by independent contractors as not having a standard baseline configuration for all hardware.

⁴⁷ NIST SP 800-70 rev. 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers* (February 2011).

⁴⁸ FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006), states that organizations must: (1) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (2) establish and enforce security configuration settings for information technology products employed in organizational information systems.

2.b(6). Standard baseline configurations are not fully implemented (NIST 800-53: CM-2). True

We found that five of seven agencies were not following standard baseline configurations. For example, our review identified that over 45 percent of the Department's Windows 2003 server configuration settings did not comply with current Federal guidelines.⁴⁹

2.b(7). FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6). False

No exception noted. OMB required agencies with—or planning to update—Windows Vista or Windows XP operating systems to adopt standard security configurations on workstations by February 1, 2008.⁵⁰ The standard security configurations were developed by NIST, DoD, and DHS and are commonly referred to as the Federal desktop core configuration (FDCC). Our reviews at 3 agencies found less than 7 percent of all required settings on workstations were not compliant and that all deviations from the FDCC had fully documented waivers.

2.b(8). Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2). True

The Department required all agencies to establish and implement procedures for accomplishing monthly vulnerability scanning of all networks, systems, servers, and desktops for which it was responsible.⁵¹ This includes performing monthly scans and remediating vulnerabilities found as a result of the scans. OIG and independent contractors determined that three of six agencies reviewed did not scan all devices and did not correct critical vulnerabilities in a timely manner. For example, we found that one agency was not scanning over 1,600 machines on a monthly basis as required. This occurred because the network and security groups were not communicating.

2.b(9). Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in agency policy or standards. (NIST 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 deployed within the information system, and to implement the recommended configuration settings. Our review of seven agencies disclosed that configuration vulnerabilities were not being mitigated and remediated timely. Specifically, we found that 75 of 216 network device settings were not configured in accordance with NIST SP 800-53.

⁴⁹ Defense Information Systems Agency, *Windows 2003 Security Technical Implementation Guide Overview* (August 27, 2010). The NIST site incorporates checklists from various Federal entities including the Department of Defense (DoD).

⁵⁰ OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* (March 22, 2007).

⁵¹ USDA Department Manual (DM) 3530-001, *USDA Vulnerability Scan Procedures* (July 20, 2005).

2.b(10). Patch management process is not fully developed, as specified in agency policy or standards. (NIST 800-53: CM-3, SI-2). False

No exception noted. NIST SP 800-53 requires Federal agencies to incorporate vendor software flaw remediation (patches) into the organizational configuration management process. Our review of three agencies identified that over 90 percent of all patches had been applied as required.

S3: Incident Response and Reporting

Section 3: Incident Response and Reporting

Check one: (3.a, 3.b, or 3.c)

3.a. The agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

- 3.a(1). Documented policies and procedures for detecting, responding to, and reporting incidents.**
- 3.a(2). Comprehensive analysis, validation and documentation of incidents.**
- 3.a(3). When applicable, reports to US-CERT within established timeframes.**
- 3.a(4). When applicable, reports to law enforcement within established timeframes.**
- 3.a(5). Responds to and resolves incidents in a timely manner, as specified in agency policy or standards, to minimize further damage.**
- 3.a(6). Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.**
- 3.a(7). Is capable of correlating incidents.**

3.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.

3.c. The agency has not established an incident response and reporting program. If 3.b. is checked above, check areas that need significant improvement:

3.b(1). Incident response and reporting policy is not fully developed (NIST 800-53: IR-1). False

No exception noted. We found that Department policy met all of NIST's requirements.⁵² The Department has developed a new incident policy, which is in draft. As of September 30, 2011, the policy had not yet been finalized.

⁵² NIST SP-800-61, *Computer Security Incident Handling Guide* (March 2008).

3.b(2). Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1). True

Our review identified that the day-to-day procedures were not accurately reflected in the documented Agriculture Security Operations Center (ASOC) Standard Operating Procedure (SOP).⁵³ As an example, we determined the SOP did not include the updated versions of incident checklists utilized by the incident response team. In addition, audit work done by OIG and independent contractors determined that three of four agencies did not have procedures that were fully developed or sufficiently detailed. For example, two agencies had not developed procedures, while the other two agencies' procedures did not include the classification of the types of incidents or the reporting requirements for the specific incident categories.

3.b(3). Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev. 1). True

Our review of 66 incidents found that 7 were not handled in accordance with Departmental procedures.⁵⁴ Based on our overall statistical sample results, we estimate that 139 incidents (9.4 percent of the universe) were not handled in accordance with Departmental procedures.⁵⁵ Specifically, agencies were required to submit documentation to the Department, detailing the steps taken to close out the incident. Specific documents and completed forms were required to be returned to the Department; however, we found that all seven incidents had either missing or incomplete documentation. For example, all 7 incidents did not complete the 24-hour response checklist as required by the Department's SOP for incident reporting.

Additionally, we noted an incident that was identified at an agency which was not reported to ASOC as required by Departmental incident response procedures.⁵⁶ An agency employee allowed an unauthorized individual to access her Federal computer. This unauthorized individual subsequently modified system hardware and software characteristics without the owner's knowledge and deployed malicious software on the computer. Though the agency was notified of these malicious actions and was aware that the employee granted unauthorized access, the agency failed to notify the Department. As of September 30, 2011, this incident was over 6 months old and not reported to the Department, as required.

3.b(4). Incidents were not identified in a timely manner, as specified in agency policy or standards (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). False

No exception noted.

⁵³ 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).

⁵⁴ Stratum 1 is a census stratum of two incidents. For Stratum 2, the sample size of 64 incidents was based on an expected error rate of 20 percent and a desired absolute precision of +/-10 percent of the audit universe, when reporting a 95 percent confidence level. Additional sample design information is presented in exhibit B.

⁵⁵ We are 95 percent confident that between 33 (2.3 percent of the universe) and 244 (16.6 percent of the universe) incidents were not handled in accordance with Departmental procedures. Additional sample design information is presented in exhibit B.

⁵⁶ DM 3505-001, *Cyber Security Incident Handling Procedure* (March 20, 2006).

3.b(5). Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). True

The US-Computer Emergency Readiness Team (US-CERT) requires USDA to notify it of incidents within specified timeframes that are based on the category of the incident.⁵⁷ Our review of incidents disclosed the Department did not report 5 of 66 incidents to US-CERT within the required timeframe. Based on our statistical sample results, we estimate that 115 incidents (7.8 percent of the universe) were not reported to US-CERT as required.⁵⁸ For example, US-CERT requires that lost or stolen equipment incidents be reported within 1 hour; however, we found that the Department did not report a stolen laptop incident to US-CERT for 27 hours. In addition, there were three incidents that we could not verify if US-CERT was notified according to policy because the proper documents were not provided. We found that the email audit logging feature for the incident tracking server was not activated until June 1, 2011. Therefore, any emails automatically sent to US-CERT before that date, were not retrievable.

3.b(6). Incidents were not reported to law enforcement as required (SP 800-86). True

We found 2 of the 66 incidents were not reported to OIG as required by DM 3505-001. Additionally, we identified that the automated email notification, which alerts OIG of cyber-related security incidents, did not do so for over three months.

3.b(7). Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). True

If an incident was not resolved after 30 days, the Department's procedures require the agency to open a plan of action and milestones (POA&M).⁵⁹ We found that 6 of the 66 incidents were not resolved within 30 days and no POA&Ms were created for the incidents. Based on our sample results, we estimate 138 incidents (9.4 percent of the universe) were not resolved in a timely manner.⁶⁰

⁵⁷ US-CERT provides response support and defense against cyber attacks for the Federal Civil Executive Branch (i.e., ".gov") and information sharing and collaboration with State and local government, industry, and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. NCSD was established by DHS to serve as the Federal Government's cornerstone for cyber security coordination and preparedness.

⁵⁸ We are 95 percent confident that between 18 (1.2 percent of the universe) and 212 (14.4 percent of the universe) incidents were not reported to US-CERT as required. Additional sample design information is presented in exhibit B.

⁵⁹ 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.

⁶⁰ We are 95 percent confident that between 32 (2.2 percent of the universe) and 243 (16.5 percent of the universe) incidents were not resolved in a timely manner. Additional sample design information is presented in exhibit B.

3.b(8). Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). True

NIST SP 800-61 states incident response teams should use information gained during incident handling to better prepare for future incidents and to provide stronger protections for systems and data. We found that 14 of the 66 incidents were not resolved to minimize further damage. Based on our statistical sample results, we estimate 322 incidents (21.8 percent of the universe) were not resolved to minimize further damage.⁶¹ For example, a user had unauthorized software installed on his computer. The remediation action taken by the agency was to contact the user and tell him to uninstall the software without any additional follow-up.

3.b(9). There is insufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). True

Our review of the Department's incident monitoring and detection capability determined the Department had insufficient incident detection and monitoring coverage. From September 2010 to April 2011, USDA installed an incident detection toolkit, which alerts the Department to potential cyber-related incidents. During FY 2011, USDA had three employees who were responsible for monitoring the daily data, calibrating security tools, and performing incident analysis. The individuals were able to analyze and process approximately 15 incidents per week. However, the Department stated that with the appropriate resources, it would have been able to process up to 150 incidents per week. NIST SP 800-53 requires the organization to report suspected security incidents and related information to appropriate organizational authorities. USDA has assigned this responsibility to the ASOC. According to the Department, it was aware of the up to 150 weekly security-related incidents and that it did not have sufficient resources to investigate or report the majority of them.

3.b(10). The agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment. True

NIST SP 800-53 requires the organization to track and document information security-related incidents, no matter where the Federal information resides. Over the past two years, the Department had implemented a cloud-based email solution.⁶² In discussions with Departmental officials and a review of the agreement between USDA and the contractor, we were unable to verify that USDA was prepared to track and manage incidents in this environment. We found that these responsibilities were not adequately addressed in the agreement between the Department and the cloud contractor. As a result, there was an increased risk of incidents occurring within the cloud environment, which are not being identified and tracked by USDA.

⁶¹ We are 95 percent confident that between 172 (11.7 percent of the universe) and 471 (32 percent of the universe) incidents were not resolved to minimize further damage. Additional sample design information is presented in exhibit B.

⁶² Cloud computing is a model for enabling network access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST SP 800-145, *The NIST Definition of Cloud Computing* (September 2011).

3.b(11). The agency does not have the technical capability to correlate incident events.

False

No exception noted. ASOC possesses the technical capability to correlate incidents across USDA's network through the use of network analysis tools. However, as noted in 3.b(9), the Department stated it did not have the resources to adequately process the number of incidents it was currently monitoring.

S4: Security Training

Section 4: Security Training

Check one: (4.a, 4.b, or 4.c)

4.a. The agency has established and is maintaining a security training program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

4.a(1). Documented policies and procedures for security awareness training.

4.a(2). Documented policies and procedures for specialized training for users with significant information security responsibilities.

4.a(3). Security training content based on the organization and its roles, as specified in agency policy or standards.

4.a(4). Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training.

4.a(5). Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other agency users) with significant information security responsibilities that require specialized training.

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

4.c. The agency has not established a security training program.

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

4.b(1). Security awareness training policy is not fully developed (NIST 800-53: AT-1).

False

No exception noted. We determined the Department's security awareness policy met all the requirements outlined in NIST SP 800-53.⁶³

⁶³ DM 3545-001, *Computer Security Training and Awareness* (February 17, 2005).

4.b(2). Security awareness training procedures are not fully developed and sufficiently detailed (NIST 800-53: AT-1). True

We determined the Department's security awareness training procedures met all NIST SP 800-53 requirements.⁶⁴ However, one of three agencies we reviewed did not have procedures in place to ensure employees and contractors received adequate security awareness training.

4.b(3). Security awareness training procedures are not consistently implemented in accordance with government policies (NIST 800-53: AT-2). True

We determined the Department's security awareness training procedures met all NIST SP 800-53 requirements. However, as stated in 4.b(7), procedures were not consistently implemented. In the 3 agencies reviewed, we found 1,383 of 10,904 users with login privileges did not have evidence indicating they had completed their annual security awareness training.

4.b(4). Specialized security training policy is not fully developed (NIST 800-53: AT-3). True

We determined that the Department's policy and two of three agencies' policies for specialized security training were not fully developed.⁶⁵ We found the Department's policy for specialized training was in draft form and did not include a definition of significant information security responsibilities. Without a definition, agencies have interpreted the requirement inconsistently. The Department's policy was not finalized as of September 30, 2011.

4.b(5). Specialized security training procedures are not fully developed or sufficiently detailed in accordance with government policies (SP 800-50, SP 800-53). True

We determined the Department's and two of three agencies' procedures for specialized security training were not fully developed or sufficiently detailed. As noted in 4.b(4), specialized security training policies did not include a definition of significant information security responsibilities. Therefore, agencies interpreted the requirement inconsistently and not all users who required specialized training received it. As a result, the Department increases its risk of compromise by allowing users to access information system resources without the required training.

⁶⁴ Departmental Standard Operating Procedure (SOP), *Information Security Training, SOP-ISD 022* (October 7, 2008).

⁶⁵ NIST SP 800-53 requires the organization to provide basic security awareness training to all users. Additionally, it requires the organization to identify and provide information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software with role-based specialized security training related to their specific roles and responsibilities. The organization is to determine the appropriate content of security training and the specific requirements of the organization and the information systems to which personnel have authorized access.

4.b(6). Training material for security awareness training does not contain appropriate content for the agency (SP 800-50, SP 800-53). False

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

4.b(7). Identification and tracking of the status of security awareness training for personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training is not adequate in accordance with government policies (SP 800-50, 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 found all three agencies did not adequately identify and track employees with login privileges. Specifically, of the 3 agencies reviewed, we found that 1,383 of 10,904 users with login privileges did not have evidence that they completed their annual security awareness training.

4.b(8). Identification and tracking of the status of specialized training for personnel (including employees, contractors, and other agency users) with significant information security responsibilities is not adequate in accordance with government policies (SP 800-50, SP 800-53). False

No exception noted. All three agencies provided OIG with a list of employees that required specialized training. They also identified the course each user completed.

4.b(9). Training content for individuals with significant information security responsibilities is not adequate in accordance with government policies (SP 800-53, SP 800-16). True

NIST SP 800-53 requires agencies to provide specialized training to security professionals. Our testing at 3 agencies found that 4 of 33 users identified as requiring specialized security training did not have documented proof they received the training during FY 2011. For example, two of the four employees identified non-specialized iPad and iPhone user training as their specialized security training.

4.b(10). Less than 90 percent of personnel (including employees, contractors, and other agency users) with access privileges completed 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 3 sample agencies identified only 9,521 of 10,904 users with login privileges (87 percent) had evidence of completing the annual security awareness training.

4.b(11). Less than 90 percent of employees, contractors, and other users with significant security responsibilities completed 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 employees with significant security responsibilities in 3 agencies found only 29 of 33 (88 percent) had documented evidence of specialized training.

S5: POA&M
Section 5: POA&M

Check one: (5.a, 5.b, or 5.c)

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

5.a(1). Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.

5.a(2). Tracks, prioritizes and remediates weaknesses.

5.a(3). Ensures remediation plans are effective for correcting weaknesses.

5.a(4). Establishes and adheres to milestone remediation dates.

5.a(5). Ensures resources are provided for correcting weaknesses.

5.a(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 POA&M activities at least quarterly.

5.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.

5.c. The agency has not established a POA&M program.

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

5.b(1). POA&M Policy is not fully developed. True

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

5.b(2). POA&M procedures are not fully developed and sufficiently detailed. True

Although there were no formal policies, the Department distributed an updated SOP in August 2011.⁶⁶ Our review of the SOP determined it was updated to include OMB-outlined criteria, and that it reflected the current POA&M process. We found that of the eight agencies that OIG, independent contractors, and annual agency self-assessments reviewed, seven did not have fully developed or sufficiently detailed procedures and six of the agencies had no procedures at all.

5.b(3). POA&M procedures are not consistently implemented in accordance with government policies. True

We found that procedures were not consistently implemented, as noted in 5.b(4)-(12). Without adequate policies and procedures at both the Department and agency levels, there is no basis for a consistent POA&M process.

5.b(4). POA&Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation (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. However, our testing at 3 agencies found 1,224 vulnerabilities over 30 days old for which no POA&M had been created. We also found that agencies were only creating one POA&M for all outstanding vulnerabilities, instead of grouping the vulnerabilities to effectively manage weaknesses and ensure remediation efforts were tracked and recorded. Additionally, we found 6 incidents that were open for over 30 days for which no POA&M was created as required by Departmental SOP. Based on our statistical sample results, we estimate 138 incidents (9.4 percent of the universe) were not closed timely and did not have a POA&M created to address them.⁶⁷

5.b(5). Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls). True

OMB specifies that effective remediation of IT security weaknesses is essential to achieve a mature and sound IT security program, and for securing information and systems.⁶⁸ We determined that 8 of 43 POA&Ms closed in FY 2011 were closed without documented remediation plans.⁶⁹ Based on our sample results, we estimate 190 POA&Ms (19 percent of the

⁶⁶ Departmental SOP, *Plan of Action and Milestones Management CPO SOP 002* (June 29, 2011).

⁶⁷ We are 95 percent confident that between 32 (2.2 percent of the universe) and 243 (16.5 percent of the universe) incidents were not resolved in a timely manner. Additional sample design information is presented in exhibit B.

⁶⁸ OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

⁶⁹ We based the sample size on a very low expected error rate. If 0 errors were found, and we desired a 5 percent chance or less of the error rate in the universe to exceed 5 percent, then our sample size would be 76 POA&Ms. We selected a simple random sample of 76 POA&Ms for review with a possible stop or go decision point at 43 POA&Ms reviewed. Additional sample design information is presented in exhibit B.

universe) were closed in FY 2011 without sufficient remediation actions to address the identified weaknesses in accordance with government policies.⁷⁰

5.b(6). Source of security weaknesses are not tracked (OMB M-04-25). True

OMB M-04-25 specifies that agencies should identify the source (e.g., program review, IG audit, GAO audit, etc.) of the weakness. Our review of a statistical sample of POA&Ms open during FY 2011 found that 32 of 93 POA&Ms did not track the source of the security weakness. Based on our sample results, we estimate 721 POA&Ms (34.4 percent of the universe) did not track the source of the security weakness.⁷¹

5.b(7). 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 40 of 93 POA&Ms had security weaknesses that were not appropriately prioritized. Based on our statistical sample results, we estimate 90 POA&Ms (43 percent of the universe) had security weaknesses that were inappropriately prioritized.⁷² For example, the Department considers 33 security controls to be critical, and requires agencies to test, report the results of that test, and create POA&Ms for weaknesses found with these controls on an annual basis. We found 18 POA&Ms associated with these key controls were prioritized as low or very low, instead of being assigned a higher priority. This occurred due to agencies not updating the required priority field within CSAM, which automatically defaulted to low or very low.

5.b(8). Milestone dates are not adhered to (OMB M-04-25). True

We found 65 of the 93 POA&Ms reviewed did not adhere to the POA&Ms milestone dates. Based on our overall sample results, we estimate 1,464 POA&Ms (70 percent of the universe) did not adhere to the milestone dates.⁷³

5.b(9). Initial target remediation dates are frequently missed (OMB M-04-25). True

OMB M-04-25 specifies that a POA&M should include a scheduled completion date for resolving the identified weakness. Our review of FY 2011 POA&Ms found 409 of 2,094 were not completed by the scheduled date. Of the 409 POA&Ms that were not completed by the scheduled completion date, we were able to determine, as of July 14, 2011:

⁷⁰ We are 95 percent confident that between 69 (7 percent) and 312 (30 percent) of closed POA&Ms in FY11 had remediation actions that did not sufficiently address the identified weaknesses in accordance with government policies. Additional sample design information is presented in exhibit B.

⁷¹ We are 95 percent confident that between 519 (about 25 percent) and 922 (44 percent) of the POA&Ms did not track the source of the security weakness. Additional sample design information is presented in exhibit B.

⁷² We are 95 percent confident that between 691 (33 percent) and 1,111 (53 percent) of the FY11 POA&Ms had security weaknesses that were not appropriately prioritized. Additional sample design information is presented in exhibit B.

⁷³ We are 95 percent confident that between 1,269 (60 percent) and 1,658 (79 percent) of POA&Ms did not adhere to milestone dates. Additional sample design information is presented in exhibit B.

- 218 POA&Ms were 1-89 days past due
- 96 POA&MS were 90-179 days past due
- 70 POA&Ms were 180-365 days past due
- 25 POA&Ms were over 365 days past due

We determined that USDA was not estimating reasonable remediation dates when generating POA&Ms. This occurred because agencies were not developing detailed project plans for remediation prior to creating POA&Ms.

5.b(10). POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25). True

Departmental procedures require that open POA&Ms be monitored on a routine basis and the status of each POA&M should be updated no less than quarterly to demonstrate progress in mitigating weaknesses. We found 15 of 93 POA&Ms had not been updated timely. Based on our sample results, we estimate 338 POA&Ms (16 percent of the universe) were not updated in a timely manner in accordance with Departmental procedures.⁷⁴ For example, we identified 10 POA&Ms that had not been updated in the past six months.

5.b(11). Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25). True

We found that USDA had not met OMB M-04-25's requirement that each POA&M include the estimated amount of funding needed to remediate the weakness. We found 674 of 1,774 POA&Ms in FY 2011 had an associated cost of zero dollars for weakness remediation.

5.b(12). 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 were subject to review by the OCIO during the closure review process. In addition, the SOP requires the Department to review another 10 percent of non-audit related, closed POA&Ms. We determined that POA&Ms were not effectively tracked and reviewed by the Department. For example:

- OCIO was unable to provide an accurate list of all closed POA&Ms it reviewed;
- OCIO did not upload the required closure review checklist for 40 percent of the audit POA&Ms reviewed;
- OCIO was not reviewing closed POA&Ms the same quarter in which they were closed, as required;
- OIG was unable to verify that all audit POA&Ms had been reviewed. There was no automated process to track audit POA&Ms. Instead, the Department has a manual process without proper tracking and oversight; and

⁷⁴ We are 95 percent confident that between 182 (about 9 percent) and 494 (about 24 percent) of the POA&Ms were not updated in a timely manner. Additional sample design information is presented in exhibit B.

- OIG could not verify that 10 percent of all closed, non-audit POA&Ms were being reviewed by the Department, due to inaccurate and inconsistent evidence provided to OIG.

S6: Remote Access Management
Section 6: Remote Access Management

Check one: (6.a, 6.b or 6.c)

6.a. The agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

- 6.a(1). Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.**
- 6.a(2). Protects against unauthorized connections or subversion of authorized connections.**
- 6.a(3). Users are uniquely identified and authenticated for all access.**
- 6.a(4). If applicable, multi-factor authentication is required for remote access.**
- 6.a(5). Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.**
- 6.a(6). Defines and implements encryption requirements for information transmitted across public networks.**
- 6.a(7). Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.**

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

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

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

6.b(1). Remote access policy is not fully developed (NIST 800-53: AC-1, AC-17). True

Although the Department had a remote access policy, we found it did not meet all NIST requirements.⁷⁵ 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.⁷⁶ Specifically, there were two policy areas that were not addressed in the Departmental policy as outlined by NIST SP 800-46. One area was the administration of remote access servers and the other was periodic reassessment of telework device policies. We also found one of three agencies reviewed did not have a remote access policy fully developed.

⁷⁵ NIST SP 800-46, Rev. 1, *Guide to Enterprise Telework and Remote Access Security* (June 2009).

⁷⁶ DM 3525-003 *Telework and Remote Access Policy* (February 17, 2005).

6.b(2). Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1, AC-17). True

The Department did not provide any remote access 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 was implemented. We found the agencies did not have fully developed or sufficiently detailed remote access procedures. For example, one agency's handbook provided policy guidance for remote access and teleworking, but it did not provide procedures for ensuring the policies were enforced.

6.b(3). Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1, AC-17). True

As noted in 6.b(2), remote access procedures were not fully developed or sufficiently detailed; thus, they were not consistently implemented in accordance with government policies. We found that of the seven agencies that OIG, independent contractors, and annual agency self-assessments reviewed, five did not have remote access procedures implemented consistently. As a result, inadequate security for remote access could result in the unauthorized access, use, disclosure, disruption, modification, or destruction of information. For example, one agency's handbook provided policy guidance for remote access and teleworking, but it did not provide procedures for ensuring the policies were enforced.

6.b(4). Telecommuting policy is not fully developed (NIST 800-46, Section 5.1). True

As noted in 6.b(1) above, we found that Departmental policy did not meet NIST SP 800-46 guidance. We found two of the three agencies reviewed did not have a fully developed telecommuting policy.

6.b(5). Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4). True

We found all three agencies reviewed did not have fully developed telecommuting procedures. For example, one agency was able to provide policies, but did not have detailed remote access procedures.

6.b(6). Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1). False

No exception noted. We found that of the seven agencies reviewed by OIG and independent contractors, seven were able to identify all users requiring remote access.

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

Departmental Regulation 3505-003 specifies that agencies must implement multi-factor authentication for all forms of remote access to agency information systems.⁷⁷ We found that of the 10 agencies that OIG, independent contractors, and annual agency self-assessments reviewed, 8 did not have multi-factor authentication properly implemented for remote access. The agencies were not using the Departmental solution because they had not received all of their identification cards.⁷⁸ This caused them to employ interim solutions that did not use two-factor authentication for remote access.

6.b(8). Agency has not identified all remote devices (NIST 800-46, Section 2.1). False

No exception noted. Our review and reviews conducted by independent contractors found five agencies had identified all remote devices.

6.b(9). Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2). True

USDA had not implemented multi-factor authentication Department-wide, as noted in 6.b(7). We also found two of three agencies reviewed had not completely implemented encryption on all their remote access devices (including removable media) while waiting for the Departmental solution to be implemented. For example, OIG found one agency had failed to encrypt 341 laptop devices because procedures were inadequate to ensure this was done for newly deployed hardware.

6.b(10). Agency does not adequately monitor remote devices when connected to the agency's networks remotely in accordance with government policies (NIST 800-46, Section 3.2). True

We found that two of five agencies reviewed were not adequately monitoring remote devices while they were connected to the agency's networks, as required by NIST SP 800-46. One agency conducted only general network logging, and did not conduct specialized remote access logging. Due to the dangers inherent in remote access, more stringent logging and review should be initiated.

⁷⁷ USDA Departmental Regulation (DR) 3505-003, *Access Control Policy* (August 11, 2009). Multi-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as “something you have and something you know.”

⁷⁸ USDA LincPass ID cards (Homeland Security Presidential Directive-12 (HSPD-12) credentials).

6.b(11). Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines). False

No exception noted. Our review found that all lost or stolen devices were disabled and appropriately reported.

6.b(12). Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4). True

NIST SP 800-53 requires that agencies provide users with a Rules of Behavior document, and that it be signed prior to allowing access to the system. We found one of four agencies reviewed did not have adequate remote access Rules of Behavior. This occurred because one agency was not aware it was required to have a Rules of Behavior document signed prior to allowing the user access to the system.

6.b(13). Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6). False

No exception noted. We reviewed four agencies and found all four had adequate remote access user agreements.

6.b(14). Other. True

Remote access sessions, in accordance to OMB M-07-16, are not timed out after 30 minutes of inactivity, after which re-authentication is required.

6.b(14ex). Explanation for Other

NIST SP 800-46 requires remote sessions to be timed-out after 30 minutes of inactivity. Our review found that 2 of 3 agencies did not require sessions to be timed-out after 30 minutes of inactivity. One agency had a time-out setting of 240 minutes.

S7: Identity and Access Management

Section 7: Identity and Access Management

Check one: (7.a, 7.b or 7.c)

7.a. The agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and identifies users and network devices. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

7.a(1). Documented policies and procedures for account and identity management.

7.a(2). Identifies all users, including federal employees, contractors, and others who access agency systems.

- 7.a(3). Identifies when special access requirements (e.g., multi-factor authentication) are necessary.
- 7.a(4). If multi-factor authentication is in use, it is linked to the agency's PIV program where appropriate.
- 7.a(5). Ensures that the users are granted access based on needs and separation of duties principles.
- 7.a(6). Identifies devices that are attached to the network and distinguishes these devices from users.
- 7.a(7). Ensures that accounts are terminated or deactivated once access is no longer required.
- 7.a(8). Identifies and controls use of shared accounts.

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

7.c. The agency has not established an identity and access management program.

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

7.b(1) Account management policy is not fully developed (NIST 800-53: AC-1). True

We found that the Department's identity and account management policy did not contain all controls required by NIST SP 800-53.⁷⁹ For example, Department policies did not address the authorizing and monitoring of guest/anonymous, emergency, and temporary accounts. In addition, two of the three agencies reviewed did not have a fully developed formal policy for identity and account management. The Department's new policy is in draft and is currently in the clearance process.

7.b(2) Account management procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1). True

We found that the Department issued a handbook for identity and account management procedures.⁸⁰ However, the handbook was for a new identity and account management program that had not been fully implemented, and the handbook did not contain all controls required by NIST SP 800-53. The Department plans to develop procedures after the implementation of the new policy. Our review of the three selected agencies found that they also did not have formal procedures meeting all NIST SP 800-53 requirements.

⁷⁹ DR 3505-003, *Access Control Policy* (August 11, 2009); DR 3180-001, *Information Technology Network Standards* (September 30, 2008); and DR 3535-001, *USDA's C2 Level of Trust* (February 2005).

⁸⁰ USDA Identity, Credential and Access Management (ICAM) Identity Lifecycle Management Handbook (June 2011).

7.b(3) Account management procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-2). True

We found that of the nine agencies that OIG, independent contractors, and annual agency self-assessments reviewed, seven did not consistently implement account management procedures. See questions 7.b(5)-(10).

7.b(4) Agency cannot identify all user and non-user accounts (NIST 800-53, AC-2). False

No exception noted.

7.b(5) Accounts are not properly issued to new users (NIST 800-53, AC-2). True

We found that of the 11 agencies that OIG, independent contractors, and annual agency self-assessments reviewed, 5 were not properly issuing accounts to new users, as required by NIST SP 800-53. NIST specifies that 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 agency annual self-assessments performed, five agencies identified weaknesses in their processes for properly issuing new user accounts. Agencies were not properly documenting and approving new user requests, in accordance with their own policies and procedures.

7.b(6) Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2). True

Departmental regulations require accounts to be deleted or disabled within 48 hours of a user's separation.⁸¹ We found that of the nine agencies that OIG, independent contractors, and annual agency self-assessments reviewed, eight did not properly terminate user accounts when access was no longer required. For example, one agency's policy stated emergency and temporary access will be removed within 7 days and routine termination of user accounts will occur within 30 calendar days. Another agency did not have a timely way of reporting separated employees, which allowed the accounts to remain active 30 days past the separation date. As a result of these reviews, we found 28 user accounts that remained active after the user had left Federal service, which could result in unauthorized access, use, disclosure, disruption, modification, or destruction of information.

7.b(7) Agency does not use multi-factor authentication where required (NIST 800-53, IA-2). True

As noted in 6.b(7), we found 8 of the 10 agencies that OIG and independent contractors reviewed did not require multi-factor authentication.

⁸¹ DR 3505-003, *Access Control Policy* (August 11, 2009).

7.b(8) Agency has not adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). True

We found that the Department had not adequately planned for implementing Personal Identification Verification (PIV) cards for logical access in accordance with government policies.⁸² The status report published on the USDA website reported only 66 percent of the required PIV cards have been activated. Our review also found that of the six agencies that OIG, independent contractors and annual agency self-assessments reviewed, three did not adequately plan for the implementation of PIV for computer access. Department-wide implementation had been delayed due to problems with the timely issuance of the PIV cards. In addition, one agency was unable to provide the status of its PIV implementation. As a result, the mandatory implementation of the PIV card, which was first introduced in 2005, was still pending within the Department and may result in unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

7.b(9) Privileges granted are excessive, or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6). True

We found that of the 10 agencies that OIG, independent contractors, and annual agency self-assessments reviewed, 7 had granted users excessive privileges, allowing them the capability to perform conflicting functions. These agencies did not ensure that users were granted access based on their work needs, and did not follow separation of duty principles, as required by NIST SP 800-53.

NIST states that 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 use the concept of least privilege. We found three agencies reported weaknesses in granting excessive privileges and separation of duties in their annual self-assessments.

7.b(10) The agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6). True

We found that of the seven agencies that OIG, independent contractors, and annual agency self-assessments reviewed, five were not using dual accounts for administrators, as required by

⁸² FIPS Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March 2006) states that 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 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, when a cardholder logs in to an 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.

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 access listing, we found 14 administrators who did not have dual accounts and 6 users who had dual accounts but had the same elevated privilege granted to both accounts.

7.b(11) Network devices are not properly authenticated (NIST 800-53, IA-3). False

No exception noted.

7.b(12) The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies. False

No exception noted.

7.b(13) Use of shared privileged accounts is not necessary or justified. False

No exception noted.

7.b(14) When shared accounts are used, the agency does not renew shared account credentials when a member leaves the group. True

Our review found that of five agencies that OIG, independent contractors, and annual agency self-assessments reviewed, one did not renew shared account credentials when a member leaves the group.⁸³ One agency reported when a member of a shared account leaves the group, the account credentials were not immediately changed. Instead, the shared account credentials may not have expired for 90-180 days. As a result, these shared accounts were vulnerable to unauthorized access, which may result in misuse, disclosure, disruption, modification, or destruction of information.

S8: Continuous Monitoring Management

Section 8: Continuous Monitoring Management

Check one: (8.a, 8.b or 8.c)

8.a. The agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

⁸³ A shared account is a set of users assigned to a security group. The security group is assigned appropriate permissions to access specific resources such as administrative functions. This simplifies administration so that permissions are assigned once to the group instead of multiple times to each individual user. When a user is added to an existing group, the user automatically assumes the rights and permissions assigned to that group.

8.a(1). Documented policies and procedures for continuous monitoring.

8.a(2). Documented strategy and plans for continuous monitoring.

8.a(3). Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.

8.a(4). Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans.

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

8.c. The agency has not established a continuous monitoring program.

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

8.b(1). Continuous monitoring policy is not fully developed (NIST 800-53: CA-7). True

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

8.b(2). Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7). 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. The program should include a configuration management process for the information system and its constituent components. It also requires a determination of the security impact of changes to the information system and environment of operation.

8.b(3). Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev. 1, Appendix G). True

As noted in 8.b(2), continuous monitoring procedures were not provided and therefore could not be consistently implemented. The Department has stated it lacks the resources to implement robust, enterprise-wide, continuous monitoring capabilities. As a result, the Department cannot effectively detect compliance and determine if security controls within an information system are effective.

8.b(4). Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev. 1, Appendix G). True

NIST SP 800-37 states that an organization should formulate a robust strategy or plan for entity-wide continuous monitoring. 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. We found the strategy and plans the Department provided for developing an entity-wide continuous monitoring plan were in draft and are estimated to be completed by December 2011. Although the plan has not been fully developed, during the year the Department deployed powerful monitoring tools which, when fully operational, would be a large part of the continuous monitoring program.

8.b(5). Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A). True

NIST SP 800-53 states that the organization will assess the security controls in an information system as part of the testing/evaluation process. We identified 48 of 257 systems in which ongoing assessments of selected security controls had not been performed in FY 2011.

8.b(6). The following were not provided to the 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 800-53, NIST 800-53A). True

We found two of three agencies did not provide the system-authorizing official or other key system officials with security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms. This occurred because policies and procedures had not been issued, and agencies were unaware that these documents should have been provided to the authorizing official.

S9: Contingency Planning

Section 9: Contingency Planning

Check one: (9.a, 9.b, or 9.c)

9.a. The agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

9.a(1). Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.

9.a(2). The agency has performed an overall Business Impact Analysis (BIA).

9.a(3). Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

9.a(4). Testing of system-specific contingency plans.

9.a(5). The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.

9.a(6). Development of test, training, and exercise (TT&E) programs.

9.a(7). Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

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

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

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

9.b(1). Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (NIST 800-53: CP-1). True

NIST SP 800-53 states that the organization develops, disseminates, and reviews/updates a formal, documented contingency planning policy. We found that the Department's contingency planning policy did not meet these requirements.⁸⁴ For example, the policy did not address alternate telecommunications providers. This occurred because the Department's policy has not been updated with the new NIST SP 800-53 elements. We also found that of the 18 policies that OIG, independent contractors, and annual agency self-assessments reviewed, 5 did not meet these requirements.

9.b(2). Contingency planning procedures are not fully developed (NIST 800-53: CP-1). True

We found three of three agencies reviewed were following the Department's template for developing contingency plans.⁸⁵ However, our review found that the template did not contain all of the required NIST SP 800-53 elements. Specifically, it did not cover the need for alternate telecommunications providers. This occurred because the Department's policy has not been updated with the new NIST SP 800-53 elements. A total of 9 out of 17 systems failed to address alternate telecommunications providers because the element was not in the Department's template.

9.b(3). Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34). True

NIST SP 800-53 requires the agency to have formal, documented procedures to facilitate the implementation of a contingency planning policy and associated contingency planning controls.

⁸⁴ DM 3570-001, *Disaster Recovery and Business Resumption Plans* (February 17, 2005).

⁸⁵ USDA *Contingency Plan Template* (March 2011).

We found three of three agencies were not consistently implementing contingency planning procedures. For example, two agencies were not backing up data, and one agency was not testing its contingency plan as required.

9.b(4). An overall business impact assessment (BIA) has not been performed (NIST SP 800-34). True

NIST SP 800-34 states that conducting the BIA is a key element in a comprehensive information system contingency planning process.⁸⁶ The Department's guide on developing contingency plans requires that a BIA is completed for each system. We found 2 of 17 systems did not have a BIA.

9.b(5). Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34). False

No exception noted.

9.b(6). A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34). False

No exception noted.

9.b(7). A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34). True

NIST SP 800-53 requires the agency to have formal, documented procedures to facilitate the implementation of its contingency planning policy and associated controls. We found that three of three agencies had developed business continuity/disaster recovery plans; however, one agency had not fully implemented the plan. The agency's contingency plan was in the process of being rewritten to reflect a major system change and was not completed by September 30, 2011.⁸⁷

9.b(8). 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 that 10 of 17 systems had

⁸⁶ NIST SP 800-34, *Contingency Planning Guide For Federal Information Systems*, (May 2010).

⁸⁷ The application developers and the agency CIO did not see any reason to test an obsolete contingency plan.

incomplete contingency plans.⁸⁸ For example, nine plans failed to address alternate telecommunication providers. Based on our sample results, for the 3 agencies, we estimate that 22 systems (about 59 percent) had missing or incomplete contingency plans.⁸⁹

This occurred because the plans utilized the template set forth by the Department which did not meet NIST SP 800-53 standards. In one instance the contingency plan was being updated to the new template. As a result of not having complete contingency plans, agency information systems were at risk of not being able to restore mission critical and business operations in the event of a disaster.

9.b(9). 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 contingency plans for information systems, using organization-defined tests or exercises. This is done to determine the plan's effectiveness, and the organization's readiness to execute the plan and initiate corrective actions. We identified 33 of 257 systems for which USDA system contingency plans had not been tested during FY 2011.

9.b(10). Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-34, NIST 800-53). True

We found one of the three agencies that OIG and independent contractors reviewed had not fully developed training, testing, and exercise approaches.

9.b(11). Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53). True

We found that of the 18 agencies OIG, independent contractors, and annual agency self-assessments reviewed, 4 had not fully implemented training, testing, and exercise programs.

9.b(12). After-action report did not address issues identified during contingency/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 recovery and reconstitution efforts. An after-action report with lessons learned should be documented and updated. Our review found

⁸⁸ We selected a simple random sample of 25 contingency plans for review. Our simple random sample included at least one contingency plan from each of the three selected agencies, so we did not use stratification. An expected error rate of 100 percent was used. The achieved confidence intervals were wider than targeted in the design because only the first 17 system contingency plans were reviewed. All projections were made using the normal approximation to the binomial as reflected in standard equations for a simple random sample. Additional sample design information is presented in exhibit B.

⁸⁹ We are 95 percent confident that between 15 (40 percent) and 29 systems (78 percent) had missing or incomplete contingency plans. Additional sample analysis information is presented in exhibit B.

that 1 of 17 systems did not have an after-action report that addressed issues identified during the disaster recovery exercise.

9.b(13). Systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). True

NIST SP 800-53 requires alternate processing sites to be established for information systems in case of a disaster. External contractors identified that one of five agencies did not have an alternate processing site established for information systems.

9.b(14). Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53). False

No exception noted.

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

NIST SP 800-53 states that the organization should conduct user level, system level, and information system documentation backups. We found 3 of 17 systems that OIG reviewed were not performing backups in a timely manner. For example, one agency could not find the system on the network in order to start the backup. Based on the results of our statistical sample, we estimate that seven systems (about 18 percent) did not perform backups in a timely manner.⁹⁰

9.b(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. We found that 5 of 17 systems had not performed regular backup recovery tests.⁹¹ For example, one agency we reviewed did not include backup and testing as part of its annual testing. Based on our sample results, we estimate that backups for 11 systems in our audit universe (about 29 percent) were not appropriately tested.⁹²

9.b(17). Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53). True

NIST SP 800-53 states that the organization should protect the confidentiality and integrity of backup information at the storage location. OIG and the agency annual self-assessments found 2 of 13 agencies were not properly securing and protecting backups. For example, one agency was not aware that they were required to document and track weekly backup tapes.

⁹⁰ We are 95 percent confident that backups for up to 12 systems (33 percent) were not performed in a timely manner. Additional sample analysis information is presented in exhibit B.

⁹¹ Regular is considered to be at least annually during the contingency plan testing.

⁹² We are 95 percent confident that up to 17 systems' backups (47 percent) were not appropriately tested. Details of this design and additional sample analysis information are presented in exhibit B.

9.b(18). Contingency planning does not consider supply chain threats. False

No exception noted.

S10: Contractor Systems

Section 10: Contractor Systems

Check one: (10.a, 10.b or 10.c)

10.a. The agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including agency systems and services residing in the cloud external to the agency. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

10.a(1). Documented policies and procedures for information security oversight of systems operated on the agency's behalf by contractors or other entities, including agency systems and services residing in public cloud.

10.a(2). The agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and agency guidelines.

10.a(3). A complete inventory of systems operated on the agency's behalf by contractors or other entities, including agency systems and services residing in public cloud.

10.a(4). The inventory identifies interfaces between these systems and agency-operated systems.

10.a(5). The agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

10.a(6). The inventory of contractor systems is updated at least annually.

10.a(7). Systems that are owned or operated by contractors or entities, including agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

10.b. The agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including agency systems and services residing in public cloud. However, the agency needs to make significant improvements as noted below.

10.c. The agency does not have a program to oversee systems operated on its behalf by contractors or other entities, including agency systems and services residing in public cloud.

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

10.b(1). Policies to oversee systems operated on the agency's behalf by contractors or other entities, including agency systems and services residing in public cloud, are not fully developed. True

We found the Department did not have a policy 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.

10.b(2). Procedures to oversee systems operated on the agency's behalf by contractors or other entities, including agency systems and services residing in public cloud, are not fully developed. 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 were responsible for developing their own procedures. We found that two of three agencies we reviewed had not developed procedures and the remaining agency's procedures were not sufficiently detailed.

10.b(3). Procedures to oversee systems operated on the agency's behalf by contractors or other entities, including agency systems and services residing in public cloud, are not consistently implemented. True

As noted in 10.b(2), neither the Department nor the agencies reviewed had procedures that were adequate; therefore, there is no basis to evaluate consistent implementation.

10.b(4). The inventory of systems owned or operated by contractors or other entities, including agency systems and services residing in public cloud, is not complete in accordance with government policies (NIST 800-53: PM-5). True

The Department did not have an accurate inventory of contractor systems for all agencies. During the FY 2009 and FY 2010 FISMA audit, we identified systems which should have been designated as contractor systems. In response, the Department stated that it would review the systems and change the designation to contractor systems, if appropriate. During this year's audit, we found seven systems were still not included in the inventory of contractor systems. This occurred because there were no policies, or procedures, for the oversight of contractor systems.

OIG also found that the Department's new cloud email service was not included in the official USDA inventory and was not designated as a contractor system.

10.b(5). The inventory does not identify interfaces between contractor/entity-operated systems to agency owned and operated systems. True

FISMA requires the Department to maintain an inventory of information systems, including 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.⁹³ We found agencies were not maintaining an accurate inventory of interfaces. We reviewed 18 SSPs and then compared the list of interfaces to those documented in CSAM. We found that all 18 systems incorrectly reported interconnections to other systems not operated by the agency (i.e. contractors' systems). Agencies were responsible for accurately documenting interface data in CSAM, but failed to account for all interconnections. Since interfaces allow for the exchange of data between two systems, it is important that security controls in each interconnected system accurately reflect the risk of inadvertent information disclosure. Without proper documentation and testing of those interfaces, the confidentiality, integrity, and availability of the exchanged data could be compromised without discovery.

10.b(6). The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually. True

NIST specifies that organizations should review security controls for interconnection at least annually, or whenever a significant change occurs, to ensure they are operating properly and are providing appropriate levels of protection.⁹⁴ As noted in 10.b(4), the Department did not update its inventory of contractor systems in FY 2011. In addition, as noted in 10.b(5), we found that the Department had not identified all interfaces.

10.b(7). Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., security requirements). False

No exception noted. We reviewed the contract executed between USDA and its cloud email services vendor and determined that the executed agreement included clauses requiring the contractor to adhere to NIST and FISMA requirements.

10.b(8). Systems owned or operated by contractors and entities do not meet NIST and OMB's FISMA requirements (e.g., security requirements). True

We found 18 of 18 contractor systems had not been updated in accordance with government policies, and did not meet NIST SP 800-53 and OMB's FISMA requirements.⁹⁵ In addition, OIG performed physical and environmental control reviews at the cloud email contractor's primary and backup data center. We found all reviewed controls in place and operating effectively.

10.b(9). Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained. True

We found 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

⁹³ FISMA of 2002, Title III, *Information Security* (December 17, 2002).

⁹⁴ NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* (August 2002).

⁹⁵ OMB M 11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (September 14, 2011).

all relevant technical, security, and administrative issues surrounding the proposed interconnection. This information may be used to develop an Interconnection Security Agreement (ISA) and/or an MOU (or an equivalent document). Specifically, we found 17 of the 18 systems reviewed during this audit did not have the required MOU/ISA.

S11: Security Capital Planning
Section 11: Security Capital Planning

Check one: (11.a, 11.b or 11.c)

11.a. The agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by OIG, the program includes the following attributes:

11.a(1). Documented policies and procedures to address information security in the capital planning and investment control process. False

We reviewed capital planning policies and procedures at the Department and agencies to determine if all critical elements were included in the documents.⁹⁶ We determined that the policy and procedures at the Department and agency levels included all required criteria for the capital planning process with one exception. One of seven criteria required by OMB and NIST guidance was not included in the Departmental guidance.⁹⁷ Specifically, the policy lacked a description of what constitutes a major IT investment according to the capital planning process. This occurred because the Capital Planning Division was not aware the criterion needed to be included in the Departmental policy.

11.a(2). Includes information security requirements as part of the capital planning and investment process. True

No exception noted.

11.a(3). Establishes a discrete line item for information security in organizational programming and documentation. True

No exception noted.

⁹⁶ Capital Planning and Investment Control (CPIC) is a systematic approach to selecting, managing, and evaluating information technology investments, which is mandated by the Clinger Cohen Act of 1996 and requires federal agencies to focus more on the results achieved through IT investments while streamlining the federal IT procurement process (www.ocio.usda.gov/cpic/index.html).

⁹⁷ OMB A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets* (July 2010); NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process* (January 2005); DM 3560-000, *Capital Planning & Investment Control (CPIC) for Security Table of Content* (February 17, 2005); and DM 3560-001, *Security Requirements for CPIC* (February 17, 2005).

11.a(4). Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required. True

No exception noted.

11.a(5). Ensures that information security resources are available for expenditure as planned. True

No exception noted.

11.b. The agency has established and maintains a capital planning and investment program. However, the agency needs to make significant improvements as noted below.

11.c. The agency does not have a capital planning and investment program.

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

11.b(1). CPIC information security policy is not fully developed.

11.b(2). CPIC information security procedures are not fully developed.

11.b(3). CPIC information security procedures are not consistently implemented.

11.b(4). The agency does not adequately plan for IT security during the CPIC process (SP 800-65).

11.b(5). The agency does not include a separate line for information security in appropriate documentation (NIST 800-53: SA-2).

11.b(6). Exhibits 300/53 or business cases do not adequately address or identify information security costs (NIST 800-53: PM-3).

11.b(7). The agency does not provide IT security funding to maintain the security levels identified.

Exhibit B: Sampling Methodology and Projections: Audit Number 50501-0002-12 FISMA FY2011

Objective:

This sample was designed to support OIG audit number 50501-0002-12. The objective of this audit was to evaluate the status of USDA's overall IT security program based on the following overarching criteria:

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

FISMA Audit Universes and Sample Designs:

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

1. Incident Response and Reporting

Universe:

The audit universe consisted of 1,473 incidents reported for FY 2011 as of May 31, 2011. Each incident had a unique identifier (incident number) and was categorized based on incident type into 1 of 9 categories. A listing and counts of the different categories are presented in the sample design section below.

Sample Design:

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

We selected a stratified design of 66 incidents. We had two incident types with only one instance each and we wanted to ensure those two incidents were examined. Therefore, Stratum 1 is a census stratum of those two incidents; their outcomes are counted in the results but do not project to other incident types.

Because we are not making individual category projections, we placed all other incident categories, containing a total of 1,471 incidents, into Stratum 2. For Stratum 2, the sample size of 64 incidents was based on an error rate of about 20 percent and a desired absolute precision of +/-10 percent of the audit universe, when reporting a 95 percent confidence level.

The resulting sample design is summarized in the table below, with two incidents in Stratum 1 and 64 incidents selected with equal probability of selections in Stratum 2; universe counts are also provided in the table.

Table 1: Incidents universe and sample counts by category

Stratum	Incident Type	Universe	Sample
1	USCERT CAT2 - Denial of Service (DoS) Count	1	1
1	USDA CAT7 - Spam Count	1	1
2	USCERT CAT1 - Unauthorized Access Count	22	1
2	USCERT CAT3 - Malicious Code Count	612	28
2	USCERT CAT4 - Improper Usage Count	69	3
2	USCERT CAT5 - Scans/Probes/Attempted Access Count	90	5
2	USCERT CAT6 - Investigation Count	236	10
2	USDA CAT8 (USCERT CAT1) - Loss, Theft, Missing Count	271	8
2	USDA CAT9 - Block List Count	171	9
	Total:	1473	66

Results:

Results are projected to the audit universe of 1,473 incidents. Achieved precision, relative to the universe of 1,473 incidents, is reflected by the confidence interval for a 95 percent confidence level. All projections are made using the normal approximation to the binomial as reflected in standard equations for a stratified sample.⁹⁸

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

⁹⁸ Scheaffer, Mendenhall, Ott, Elementary Survey Sampling, Fourth Edition (Chapter 5), Duxbury Press, c1990.

Table 2: Incident Response and Reporting Projections

Criterion tested	Estimate of number of exceptions	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved precision ⁹⁹	Actual number of exceptions observed in sample
			Lower	Upper			
<i>Not all checklists completed as required by SOP</i>	139	52.831	33	244	.380	7%	7
<i>Incidents were not reported to US-CERT as required</i>	115	48.642	18	212	.423	7%	5
<i>Incidents were not resolved in a timely manner</i>	138	52.831	32	243	.383	7%	6
<i>Incidents were not resolved to minimize further damage</i>	322	74.929	172	471	.233	10%	14

Based on our sample results:

- We estimate that 139 incidents (about 9.4 percent of the audit universe) had incomplete checklists. We are 95 percent confident that between 33 (2.2 percent) and 244 (16.7 percent) incidents in the audit universe are non-compliant with this criterion.
- We estimate that 115 incidents (about 7.8 percent of the audit universe) were not reported to US-CERT as required. We are 95 percent confident that between 18 (1.2 percent) and 212 (14.4 percent) incidents in the audit universe are non-compliant with this criterion.
- We estimate that 138 incidents (about 9.3 percent of the audit universe) were not resolved in a timely manner. We are 95 percent confident that between 32 (2.2 percent) and 243 (16.5 percent) incidents in the audit universe are non-compliant with this criterion.
- We estimate that 322 incidents (21.9 percent) were not resolved to minimize further damage. We are 95 percent confident that between 172 (11.7 percent) and 471 (32 percent) incidents in the audit universe are non-compliant with this criterion

2. POA&Ms

Open POA&Ms

Universe:

The universe of open POA&Ms consisted of 2,094 POA&Ms.

Sample Design:

We based our sample size on a 50 percent error rate and desired absolute precision of +/-10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 93 POA&Ms for review. We noted that this sample size would also be adequate for a 1

⁹⁹ Achieved precision equals one-half the difference between the lower bound and the upper bound of the confidence interval. For example, $(244 - 33) / 2 = 105.5$. Expressed as a fraction of the universe, this is $105.5 / 1473 = 7.16$ percent.

percent error rate and a tolerable upper limit of 5 percent at the 95 percent confidence level. We selected a simple random sample of 93 POA&Ms for review.

Results:

Results for all criteria are projected to the audit universe of 2,094 POA&Ms. Achieved precision relative to the audit universe is reported for each criterion. The corresponding lower and upper bounds of the 95 percent confidence interval are also included. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.¹⁰⁰

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

Table 3: Open POA&M Projections

Criterion tested	Estimate of number of exceptions	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved Precision	Actual number of exceptions observed in sample
			Lower	Upper			
<i>Source of weakness not tracked</i>	721	100.672	519	922	0.140	10%	32
<i>Not appropriately prioritized</i>	901	104.901	691	1,110	0.116	10%	40
<i>Not updated in a timely manner</i>	338	77.925	182	494	0.231	7%	15
<i>Milestone dates not adhered to</i>	1,464	97.192	1,269	1,658	0.066	9%	65

Based on our sample results:

- We estimate that for 721 (about 34 percent of the universe) open POA&Ms in our universe, the identified source of weakness was not tracked. We are 95% confident that between 519 (25 percent) and 922 (44 percent) incidents in the audit universe are non-compliant with this criterion.
- We estimate that 901 (about 43 percent of the universe) open POA&Ms in our universe were not appropriately prioritized. We are 95% confident that between 691 (33 percent) and 1,110 (53 percent) incidents in the audit universe are non-compliant with this criterion.
- We estimate that 338 (about 16 percent of the universe) open POA&Ms in our universe were not updated in a timely manner. We are 95 percent confident that between 182 (9 percent) and 494 (24 percent) incidents in the audit universe are non-compliant with this criterion.

¹⁰⁰ Op. cit., Scheaffer et al. Chapter 4.

- We estimate that for 1,464 (about 70 percent of the universe) open POA&Ms in our universe, milestone dates were not adhered to. We are 95 percent confident that between 1,269 (61 percent) and 1,658 (79 percent) incidents in the audit universe are non-compliant with this criterion.

Closed POA&Ms

Universe:

The universe of closed POA&Ms consisted of 1,023 closed POA&Ms.

Sample Design:

Based on observations from prior year non-statistical samples, we based our sample size on a “moderate error rate” scenario: a 30 percent error rate and +/-10 percent precision at the 95 percent confidence level. With these assumptions, we calculated a sample size of 76 closed POA&Ms for review. We noted that this sample size would also be reasonable for a 1 percent error rate and a tolerable upper limit of 5 to 6 percent at the 95 percent confidence level.

We selected a simple random sample of 76 POA&Ms for review and identified a possible stop-or-go decision once the first 43 POA&Ms were reviewed.

Results:

Results are projected to the universe of 1,023 closed POA&Ms. Achieved precision relative to the universe is reported for each criterion. The corresponding lower and upper bounds of the 95 percent confidence interval are also included. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.¹⁰¹

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

Table 4: Closed POA&M Projections

Criterion tested	Estimate of number of exceptions	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved Precision	Actual number of exceptions observed in sample
			Lower	Upper			
<i>Closed POA&Ms did not have remediation actions to sufficiently address the identified weaknesses</i>	190	60.122	69	312	.316	12%	8

¹⁰¹ Ibid.

Based on our sample results, we estimate that for 190 (about 19 percent of the universe) closed POA&Ms in the universe, remediation actions did not sufficiently address weaknesses. We are 95 percent confident that between 69 (7 percent) and 312 (30 percent) incidents in the universe are non-compliant with this criterion.

3. System / Contingency Planning

Universe:

Our universe consisted of all FISMA reportable systems for the three agencies reviewed as of August 2, 2011. Each system is to have a contingency plan that contains very specific recovery information for the agency in the event of a disaster.

Sample Design:

We selected a simple random sample of 25 contingency plans for review. For a 95 percent confidence level, this sample size was adequate for a range of potential outcomes: from a 0 percent exception rate with a 5 percent upper limit to a 30 percent error rate with +/-10 percent precision. Our simple random sample included at least one contingency plan from each agency, so we did not use stratification.

Results:

The audit team reviewed the first 17 system contingency plans selected in the sample. Results are projected to the audit universe of 37 systems. Achieved precision relative to the universe is reported for each criterion. The corresponding lower and upper bounds of the 95 percent confidence interval are also included. The achieved confidence intervals were wider than targeted in the design because the review was terminated once the first 17 system contingency plans were reviewed. For two criteria, the lower bound was lower than the number of exceptions observed in the sample. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.¹⁰²

Projections are shown in Table 5. Narrative interpretation of the results can be found below the table.

¹⁰² Ibid.

Table 5: System / Contingency Planning Projections

Criterion tested	Estimate of number of exceptions	Standard Error	95% Confidence Interval		Coefficient of Variation	Achieved Precision	Actual number of exceptions observed in sample
			Lower	Upper			
<i>The system contingency plans are missing or incomplete.</i>	22	3.347	15	29	.154	19%	10
<i>The system backups are not performed in a timely manner.</i>	7	2.593	1	12	.397	15%	3
<i>The system backups are not appropriately tested.</i>	11	3.099	4	17	.285	18%	5

Based on our sample results:

- We estimate that 22 (about 59 percent of the universe) systems in our universe had missing or incomplete contingency plans. We are 95 percent confident that between 15 (40 percent) and 29 systems (78 percent) are non-compliant with this criterion.
- We estimate that for 7 (about 18 percent of the universe) systems in our universe, backups were not performed in a timely manner. We are 95 percent confident that up to 12 (33 percent) systems are non-compliant with this criterion.
- We estimate that for 11 systems (about 29 percent of the universe) in our universe, backups were not appropriately tested. We are 95 percent confident that up to 17 (47 percent) systems are non-compliant with this criterion.

4. Authority to Operate (ATO) Recertification

Universe:

Our universe consisted of 55 FISMA reportable systems requiring ATO recertification in FY11. These were systems which had not been retired and for which the certification expired in FY11. Attributes to be tested pertained to System Security Plans, Risk Assessments, and Security Assessment Reports.

Sample Design:

We selected a simple random sample of 25 systems for review, which would satisfy various possible combinations of error rates, confidence level, and precision. We also provided for a stop-or-go decision, in which a “stop” decision for a particular criterion could be based on the first 10 to 15 plans selected, if the review was resulting in all selections having an exception.

Results:

Because the review was producing an extremely high error rate, we made projections after 12 reportable systems were reviewed for the first criterion and after the first 10 reportable systems were reviewed for the remaining two criteria. For the latter two criteria, the smaller sample

resulted in a slight loss of precision overall, but the lower limit on the projection is still very high. All results below are projected to the universe of 55 reportable system certifications.

Table 6: ATO Recertification Projections

Criterion Tested	Sample Size	Estimate of number of exceptions	Lower Error Limit at 95% CL [number / fraction]	Actual number of exceptions observed in sample
<i>Were System Security Plans (SSP) adequate?</i>	12	55	44 / 80.3%	12
<i>Did Systems SARs reviewed meet the minimum security requirements required by NIST?</i>	10	55	42 / 76.4%	10
<i>Were risk assessments conducted in accordance with government policies?</i>	10	55	42 / 76.4%	10

Based on our sample results:

- We estimate that all 55 SSPs are inadequate. We are 95 percent confident that at least 80.3 percent of the SSPs in the universe are inadequate.
- We estimate that all 55 SARs fail to meet the minimum NIST security requirements. We are 95 percent confident that at least 76.3 percent of systems in our universe failed to meet the minimum NIST requirements.
- We estimate that none of the 55 risk assessments were conducted in accordance with government policies. We are 95 percent confident that at least 76.3 percent of the risk assessments in our universe were not conducted in accordance with government policies.

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

How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse

In Washington, DC 202-690-1622

Outside DC 800-424-9121

TDD (Call Collect) 202-690-1202

Bribes or Gratuities

202-720-7257 (Monday–Friday, 9:00 a.m.– 3 p.m. ET)



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