



U.S. Department of Agriculture

Office of Inspector General



Audit Report

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2009 Federal Information Security Management Act

**Audit Report 50501-15-FM
November 2009**



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



DATE: November 17, 2009

The Honorable Peter Orszag
Director
Office of Management and Budget
Eisenhower Executive Office Building
1650 Pennsylvania Avenue N.W.
Washington, D.C. 20503

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer,
Fiscal Year 2009 Federal Information Security Management Act Report
(Audit Report 50501-15-FM)

This report presents the results of our audits of the U.S. 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,

/s/

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
Exhibit A: Office of Management and Budget (OMB) Reporting Requirements and U.S. Department of Agriculture (USDA) Office of Inspector General (OIG) Position	13
Abbreviations	29

**U.S. Department of Agriculture, Office of the Chief Information Officer,
Fiscal Year 2009 Federal Information Security Management Act
(Audit Report 50501-15-FM)**

Executive Summary

Although improvements have been made in the Department's information technology (IT) security in the last decade, many longstanding weaknesses remain. Since 2001, the Office of Inspector General (OIG) has reported material weaknesses in the design and effectiveness of the Department's overall IT security program. The U.S. Department of Agriculture (USDA) is a large and complex organization, which includes 29 separate agencies and staff offices, each with its own IT infrastructure. In order to mitigate the continuing material weaknesses, the Department should rethink its policy of attempting to simultaneously achieve numerous goals in short timeframes. Instead, 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.

For the Department's security program to be effective, agency inclusion and cooperation is essential. The Department needs to coordinate with each of its component agencies and offices to identify and prioritize the most significant security risks. It then needs to develop and implement a prioritized plan to systematically mitigate the risks using realistic goals and milestones. Once the plan is developed, the Department should continuously communicate with agencies to maintain their commitment to and progress towards implementing the needed corrective actions. Departmentwide security improvements require cooperative Department and agency commitment and action. Until this occurs, critical data are exposed to an increased risk of inappropriate disclosure, modification, or deletion because of USDA's current security program.

The most important accomplishment for the Department in the past year was the implementation of the Cyber Security Assessment and Management (CSAM) system. CSAM is a comprehensive system developed by the Department of Justice, which can facilitate achieving Federal Information Security Management Act (FISMA)¹ compliance. CSAM provides a vehicle for the Department, agencies, system owners, and security staffs to (1) manage their system inventory, interfaces, and related system security threats and risks; (2) enter system security data into a single repository to ensure all system security factors are adequately addressed; (3) prepare annual system security documents, such as security plans, risk analyses, and internal security control assessments; and (4) generate custom and pre-defined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. It also aids the Department and agencies in their testing of security controls, documenting weaknesses, and tracking the mitigation of those weaknesses.

This report constitutes OIG's independent evaluation of the Department's IT security program and practices, as required by FISMA.

The following summarizes the key matters discussed in exhibit A of this report. Exhibit A contains OIG's responses to the Office of Management and Budget's (OMB) required questions.

¹ FISMA of 2002, Title III, *Information Security*, dated December 17, 2002.

The questions were defined in OMB Memorandum M-09-29, *Fiscal Year 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009.

• To address OMB’s questions, we reviewed the data entered by the Department and agencies into the CSAM system. We found that although the Department had an accurate inventory of systems, the CSAM system data pointed to problems in other areas. Specifically, our review of the CSAM system data for the Department’s 287 FISMA reportable systems showed:

- Current certification and accreditations² (C&A) were not completed for 53 systems;
- required³ security controls were not reviewed and tested for 250 systems;
- contingency plans for 73 systems were not tested during the year;⁴
- interconnections with other systems were not accurately reported as required⁵ for 162 systems; and
- 12 systems were not accurately recorded in CSAM as contractor systems.⁶

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

• Our review of the plan of action and milestones (POA&M)⁷ process found the Department did not have effective policies and procedures for reporting IT security deficiencies in CSAM. For example, our review at one agency identified at least 35 instances where POA&Ms should have been created, but were not. In fact, the agency had not entered POA&Ms into CSAM for any IT

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

³ The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, dated December 2007, requires periodic testing and evaluations of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but not less than annually. The Department requires annual testing of 29 key controls; our number is based on 100 percent testing of those controls.

⁴ NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Systems*, dated December 2007, requires yearly testing of contingency plans.

⁵ FISMA requires agencies to identify information systems in an inventory, which includes identification (ID) of the interfaces between each system, and all other systems or networks, including those not operated by, or under the control of the agency.

⁶ A system hosted or operated by a contractor.

⁷ OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated October 17, 2001, required each agency to submit to OMB by October 31, 2001 (with brief quarterly updates thereafter), “a plan of action with milestones” to address all weaknesses identified by program reviews and evaluations. It defines a POA&M as a tool that identifies tasks needing to be accomplished to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. The goal of a POA&M should be to reduce the risk of the weakness identified. CSAM is used as the USDA POA&M repository, and to track and report to OMB progress to mitigate the weaknesses.

security weakness identified in fiscal year 2009. This occurred because the OCIO security manual did not include a policy that establishes a POA&M⁸ process for reporting IT security deficiencies and tracking the status of remediation efforts. Although there were no formal policies, the OCIO had a standard operating procedure (SOP)⁹ on the POA&M Management Process. Our review of the SOP determined that it was written prior to the implementation of CSAM and was no longer applicable.

Also, oversight of the POA&M process had not been a priority within the Department. As a result, sufficient resources had not been committed to provide Departmental and agency staffs' adequate training on POA&M management and oversight to ensure that all parties understood how to accomplish an effective POA&M program. A common theme found during our fiscal year 2009 reviews was that POA&Ms were considered to have negative consequences by agency security personnel. They believed that the use of POA&Ms was discouraged by agency upper management because they were viewed as a failure of the security staff to perform their responsibilities. Therefore, the security staffs were reluctant to record and track POA&Ms. As a result, the agency's IT resources were at a higher risk of compromise or malicious activity. OMB policy recognizes that the POA&M process is constructive. It ensures agencies are constantly reviewing their security posture and working towards finding and mitigating weaknesses.

- Based on the OIG reviews performed throughout fiscal year 2009, we continue to find that agencies are not following NIST and Departmental¹⁰ guidance when preparing C&A documentation. Agencies are required to submit their system C&A packages and all supporting documentation to the Department for an in-depth review (referred to as a concurrency review). During the concurrency review, the Department ensures that the documentation prepared to support system accreditation¹¹ is complete, accurate, reliable, and that it meets all NIST and other mandated documentation standards. We evaluated seven C&A concurrency reviews where the Department had concurred with the agencies' recommendations to accredit the system. We found that the agencies' security certification¹² documentation did not support accreditation. We found that agencies had not followed NIST guidance in all seven cases. Specifically, we found that three System Security Plans (SSP),¹³ four risk assessments (RA), and seven testing

⁸ 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.

⁹ *POA&M Management Process, Standard Operating Procedure*, dated February 27, 2008.

¹⁰ NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004; Departmental Manual (DM) 3555-001, *Certification and Accreditation Methodology*, dated October 18, 2005.

¹¹ Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

¹² Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, 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.

¹³ The SSP is a required C&A document that provides an overview of the security requirements of the system and describes the controls in place (or planned) for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. (NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, dated February 2006).

documents¹⁴ did not meet NIST requirements; and two agencies had not selected the required controls to test. When reviewing CSAM, we found there were 34 systems with an expired authority to operate or interim authority to operate (IATO).¹⁵ We have reported problems in the C&A process since 2001 and attribute these continuing problems to a lack of commitment by agencies to a quality C&A process, as well as a lack of Departmental oversight. Agencies do not know if required system controls have been implemented correctly because the controls may not have been documented and tested. Systems, and the information in those systems, may be at risk if security controls have not been implemented correctly.

- We found two agencies were not performing continuous monitoring of security controls in accordance with NIST¹⁶ guidance. Neither agency had documented the critical system controls that needed to be monitored, the frequency of that monitoring, or the actions to be taken based on the results of the monitoring. In addition, one agency did not effectively perform annual system self assessments or document the results in CSAM as required. The lack of continuous monitoring was attributed to insufficient resources and agency staffs not realizing the importance of the process. Without a formal continuous monitoring plan, agencies cannot be certain that they are accomplishing the objectives of their security program.

- The Department needed to take additional actions to minimize the risk of unauthorized release of “privacy data” as required by OMB guidance.¹⁷ Due to the complexity and age of the legacy systems within USDA, the Department had not fully implemented its plan to reduce the use of social security numbers (SSN) as identifiers in application databases. OMB requires that the Department track all sensitive data extracts (i.e., extracts containing SSNs) to ensure the data are erased within 90 days or once they are no longer being used. The Department was not aware of this requirement and had not implemented a policy or plan to address this task. Also, because of technical issues associated with getting encryption software to run on USDA workstations, the overall size of the Department and the diversity of programs, full disk encryption had only been implemented on 53 percent of the Department’s laptops. As a result, the potential exists for sensitive information to reside on unencrypted computers/devices.¹⁸

¹⁴ A Security Testing and Evaluation (ST&E) is one phase of the C&A where an independent party evaluates and conducts testing of the controls established in and around a system. The purpose is to determine whether controls as stated in the system documentation are adequate and operating as prescribed.

¹⁵ Authority to Operate (ATO) or Interim Authority to Operate (IATO) is the last step in the C&A process. If C&A is adequate and meets NIST requirements an ATO is given for a period of 3 years. If after assessing the results of the security certification the agency deems that the risk to agency operations is unacceptable, but there is an overarching necessity to place the system into operation or continue its operation, an IATO may be issued for up to 6 months in order for the agency to fix the vulnerabilities in the IT system.

¹⁶ NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, dated December 2007, requires agencies to “monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.”

¹⁷ OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006; OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006; OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

¹⁸ The next step of the Department’s encryption effort will include external storage media. OCIO stated this will begin in the next few months.

- We reviewed the Department’s Privacy Impact Assessment (PIA) implementation as required by the e-Government Act of 2002.¹⁹ The Department is required to publish all PIAs on a publicly accessible website. We found that 13 of the required 122 PIAs were missing from the Department’s website.
- NIST²⁰ states “although the solutions to IT security are complex, one simple yet effective tool is the security configuration checklist.” Both NIST and the Department²¹ have issued policies requiring the use of checklists when deploying certain software. We found that agencies were not using the required checklists when deploying the software covered by the NIST requirements. Specifically, we scanned systems at two agencies using a commercially available software tool that compares implemented server settings with those required by NIST and Departmental checklists. One agency stated it used a checklist but did not know if it was NIST compliant (we determined that it was not compliant). The other agency stated the security configuration checklist settings caused operational problems. As a result, it implemented only 69 percent of the settings. The agency had not documented the reasons for not implementing the remaining 31 percent of the settings. The use of security configuration checklists to deploy software and hardware ensures consistency across the agency and ease of maintenance. When USDA agencies do not use and follow the checklists, helpdesk support, inventory management capabilities, and operating costs are all negatively affected due of the lack of standardization.
- OMB²² required agencies with Windows Vista or Windows XP operating systems, and/or plans to upgrade to these operating systems, to adopt standard security configurations on workstations by February 1, 2008. The standard security configurations were developed by NIST, the Department of Defense, and the Department of Homeland Security and are commonly referred to as the Federal Desktop Core Configuration (FDCC). Because of the complexity of the Department and its many diverse systems, it did not meet the OMB mandated deadline. The Department issued a memo on February 15, 2008, requiring agencies to be FDCC compliant by July 31, 2008. As of September 30, 2009, the Department reported only 8 percent of machines had deployed 100 percent of the FDCC standard security configuration settings. However, for those machines without full deployment of the FDCC standard security configuration settings, the Department reported an average of about 90 percent of the settings were deployed. We have not validated this percentage or the actual settings deployed. As a result, we do not know the extent to which their workstations are properly secured and in compliance with the FDCC.

¹⁹ e-Government Act of 2002, PL 107–347, dated December 17, 2002, requires agencies to conduct PIA for new IT investments and online information collections. A PIA is a review of how information about individuals is handled within the agency when the agency uses IT to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information.

²⁰ NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*, dated May 2005.

²¹ OCIO issued a memorandum, *Required Use of Security Configuration Guides*, dated March 10, 2009.

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

• The Department had made progress in the required²³ reporting of security incidents²⁴ to law enforcement and the US-Computer Emergency Readiness Team (US-CERT).²⁵ However, we found that due to the volume of incidents throughout the year, the Department did not always follow its own security review procedures. We reviewed 49 incidents (5 privacy-related) and found only 18 of the 49 (37 percent) incidents were handled in accordance with Departmental procedures, which require that agencies submit documentation to the OCIO and carryout pre-defined steps. The procedures also require that the agency undertake and document a thorough investigation of the initial cause of the incident. In addition, the procedures require agencies to submit a detailed final report to the OCIO outlining the steps taken to mitigate the cause of the incident. Despite these procedures, we found that:

- 19 incidents did not have all required documentation;
- 16 incidents were reported as closed, before the required reviews were completed;
- 12 incidents were not adequately investigated;
- 12 incidents had incomplete final reports; and
- 5 privacy-related incidents were improperly handled.

OCIO officials stated that errors occurred in the handling of the incidents due to the volume of the reported incidents. We found that OCIO staff and contractor personnel were unclear as to what procedures to follow when security incidents were reported. For example, OCIO and its contractor staff did not always ensure that agencies included the checklists contained in the procedure's appendix with its incident submissions. When we inquired as to why the checklists were not included, the OCIO personnel stated that since checklists were an appendix to the procedures they were not required. The appendix's checklists are required when an agency reports an incident.

OMB²⁶ has mandated that an incident be reported within 1 hour when it may involve privacy information. The Department included OMB's mandated timeframe in its procedures for handling privacy incidents. The OCIO officials stated that staff did not always follow procedures when handling privacy incidents because of the unrealistic timeframe mandated by OMB, even though it had included the timeframe in its own procedures. This failure to follow policies and procedures may affect the Department's ability to rapidly detect incidents and the loss of privacy information. The rapid detection and reporting of incidents is essential for minimizing data loss and destruction, mitigating any exploited weaknesses, and restoring computing services.

²³Agriculture Security Operations Center Computer Incident Response Team-Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents, dated June 9, 2009.

²⁴DM 3505-000, *USDA Cyber Security Incident Handling Procedures*, dated March 20, 2006, states an incident is a violation or imminent threat of violation of computer security policies, acceptable use or standard computer security practices. It is also any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, or disruption or denial of service.

²⁵US-CERT provides response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local Government, industry and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). The NCSD was established by DHS to serve as the Federal Government's cornerstone for cyber security coordination and preparedness.

²⁶OMB Memorandum 07-16 requires reporting to US-CERT within 1 hour of discovery/detection.

- The Department has made significant improvements to ensure that all employees receive security awareness training; however, there was no consistent method for tracking security training for USDA contractors. The Department has a database to maintain a record of all contractors within the Department; however, use of the database was not required and only two agencies were using it. Therefore, it was difficult for the Department and the agencies to identify contractors, their access controls, and whether they had received the required²⁷ training.
- Federal law, NIST, and the Department²⁸ require all users with significant security responsibilities to receive specialized role-based training, in addition to security awareness training. We were unable to determine whether all employees that should have received the additional role-based training actually received it. Agencies interpreted the definition of “significant IT security responsibilities” differently because the Department’s security training policy did not clearly define what “significant IT security responsibilities” encompassed. For example, one agency determined that only the staff working in its security office had significant security responsibilities and needed the training. Another agency interpreted the definition of significant security responsibilities to apply to all staff with elevated privileges²⁹ to the agency’s systems. As a result, employees who were actually assigned significant IT security responsibilities did not receive the additional training, as required by law, NIST, and the Department.
- For a number of years, we have recommended that the Department adopt a verifiable scanning and reporting process. OIG has been scanning USDA networks for vulnerabilities for over 9 years and continues to identify a significant number of weaknesses. To achieve a better understanding of the security posture of the Department, we scanned the networks of two agencies using industry standard, commercially available software.³⁰ The scanning software is constantly updated with current information, allowing it to identify both old and new vulnerabilities in servers, workstations, network devices, and websites. Our scans and reviews identified a number of issues.
- A review of each agency’s servers, workstations, and network devices was conducted to determine if vulnerabilities were being mitigated in a timely manner. To make this determination, we compared an agency’s scan results for multiple months. We concluded that the vulnerability was not mitigated in a timely manner if it continued to exist on multiple monthly scans and a POA&M had not been created. We found over 20,000 vulnerabilities on agencies’ servers, workstations, and networks that had not been mitigated in a timely manner.
 - We requested from each agency an inventory of the devices attached to its networks and a list of the devices that it was scanning. The two lists were then compared. We found that some devices were not being scanned.

²⁷ FISMA of 2002, Title III *Information Security*, dated December 17, 2002 and NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, dated December 2007.

²⁸ NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998, FISMA, and DM 3545-001, *Computer Security Training and Awareness*, dated February 17, 2005.

²⁹ Elevated privileges are those above a normal system user. These would include staff that had administrative privileges to servers, databases and networks.

³⁰ The commercially available software scans workstations, servers, network devices and websites to look for known vulnerabilities that have not been mitigated. Some of the items scanned for include: missing patches, poor website coding practices and insecure software settings.

- Each agency's network devices were evaluated to determine if they were configured in accordance with NIST³¹ standards. We found 299 critical settings³² that were not in conformance.
- The code used to construct agency controlled websites was evaluated to determine if it was written so that the website was secure. The software identified 322 instances where the implemented code was not secure.
- Servers and workstations were analyzed to determine if required software patches were applied in a timely manner. The software identified 1,705 required patches that had not been installed on servers and 36,184 required patches that had not been installed on workstations.

Agencies stated that timing issues, a lack of resources, and their unfamiliarity with scanning requirements contributed to these issues. As a result, USDA networks and information technology resources are vulnerable to illegal and malicious activity, and exploitation by internal and external sources.

Recommendation Summary

1. Develop and implement an effective plan to mitigate the material IT weakness 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 and implement effective policies and procedures to fully utilize CSAM for Departmental oversight.
3. Develop and implement an effective monthly FISMA scorecard to be used for agency reporting and Departmental oversight. Ensure that the scorecard includes verifiable items such as, but not limited to: vulnerability scanning, patching, anti-virus reports, and training.
4. Develop and implement an effective process to ensure system interfaces are accounted for in CSAM.
5. Develop and implement an effective process to ensure POA&Ms are entered, tracked, and closed properly. The process should include the required link to budgetary resources.
6. Develop and implement an effective C&A process based on NIST guidance. Ensure that all systems have the proper authority to operate.

³¹ NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, dated December 2007.

³² Critical security settings are those software configuration settings which may allow a device or software on a device to be compromised because they are not set in the most secure manner possible.

7. Issue Departmental guidelines implementing continuous monitoring in accordance with NIST guidance.
8. Implement all requirements of the OMB Privacy memos.
9. Implement effective policies and procedures to ensure agencies use required NIST and Departmental configuration checklists and have documented the reasons for those settings not implemented.
10. Complete the FDCC deployment and ensure all FDCC deviations are documented by the agencies.
11. Ensure all OCIO personnel and contractors adhere to Departmental policies and procedures concerning incident reporting, including the OMB mandated timeframes for reporting incidents.
12. Develop training policies and procedures for personnel with significant security responsibilities; to include a Departmental definition of what constitutes significant security responsibilities.
13. Ensure that encryption of all mobile computers/devices is completed timely, to include removable storage devices/media.
14. Develop and implement policies and procedures requiring all agencies to populate and regularly update the Non-Employee Identity System with contractor information.

Background & Objectives

Background

Improving the overall management and security of IT resources needs to be a top priority for USDA. As technology has enhanced the ability to share information instantaneously among computers and networks, it has also made 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 but a few of the threats that pose risks to the Department's critical systems and data.

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

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

FISMA assigned specific responsibilities to OMB, agency heads, Chief Information Officers (CIO), and Inspector Generals (IG). OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. The responsibilities include the authority to approve agencies information security programs. OMB also requires the submittal of an annual report to Congress summarizing the results of agencies' evaluations of their information security programs.

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

- Periodic RAs that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- development and implementation of risk-based, cost-effective policies and procedures to provide security protections for the agency's information;
- training that covers security responsibilities for information security personnel and security awareness for agency personnel;

- periodic management testing and evaluation of the effectiveness of security policies, procedures, controls, and techniques;
- processes for identifying and remediating significant security deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- annual program reviews by agency officials.

In addition to the responsibilities listed above, FISMA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and 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 OCIO's oversight of agencies' CIOs, and compliance with FISMA;
- determining whether agencies maintain an adequate system of internal controls over IT assets in accordance with FISMA and other applicable laws and regulations;
- evaluating OCIO's progress in establishing a Departmentwide security program, which includes effective certifications and accreditations;
- evaluating the agencies' and OCIO's POA&M consolidation and reporting process; and
- analyzing USDA's Privacy Act documentation to ensure USDA has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.

Scope and Methodology

The scope of our review was Departmentwide and included agency IT audits completed during fiscal year 2009. We conducted this audit in accordance with *Government Auditing Standards*. Those standards required we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Fieldwork for this audit was performed at OCIO from June to October 2009. In addition, the results of IT control testing and compliance with laws and regulations performed by contract auditors at four additional agencies are included in this report. In total, our fiscal year 2009 audit work covered 10 agencies and staff offices: Economic Research Service (ERS), Food and Nutrition Service, Forest Service, Farm Service Agency (FSA), Food Safety and Inspection Service, Natural Resources Conservation Service (NRCS), Office of the Chief Financial Officer (OCFO), OCIO, Rural Development, and Risk Management Agency. These agencies and staff offices operate approximately 181 of the OCIO's estimated 287 general support and major application systems within the Department.

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

- Consolidated the results and issues from our prior IT security audit work and the work of contractors administered by USDA's OIG. Contractor audit work consisted primarily of audit procedures found in the U.S. Government Accountability Office's (GAO) Financial Information System Control Audit Manual;
- evaluated the Department's progress in implementing recommendations to correct material weaknesses identified in prior OIG and GAO audit reports;
- gathered the necessary information to address the specific reporting requirements outlined in OMB Memorandum M-09-29, Fiscal Year 2009 *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009; and,
- performed detailed testing specific to FISMA requirements at selected agencies as detailed in this report.

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

(OMB Questions are in bold, OIG responses are underlined)

Question 1:

FISMA Systems Inventory

Identify the number of Agency and contractor systems by component and FIPS 199 impact level (low, moderate, high) reviewed.

Question 2:

Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing
For the Total Number of Reviewed Systems Identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed the past year, and a contingency plan tested in accordance with policy.

Note: Totals listed below are not Department totals, but represent only those 10 agencies reviewed by OIG or OIG contractors during fiscal year 2009.

As of 10/6/2009		Question 1						Question 2		
Bureau Name	FIPS 199 System Impact Level	1.a FY 2009 Agency Systems		1.b FY 2009 Contractor Systems		1.c Total Number of Systems (Agency and Contractor systems)		2.a Number of systems certified and accredited	2.b Number of systems for which security controls have been tested and reviewed in the past year	2.c Number of systems for which contingency plans have been tested in accordance with policy
		# Total	# Rev.	# Total	# Rev.	# Total	# Rev.			
Economic Research Service	High	0	0	0	0	0	0	0	0	0
	Moderate	1	1	0	0	1	1	1	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	1	1	0	0	1	1	1	0	0
Food and Nutrition Service	High	0	0	0	0	0	0	0	0	0
	Moderate	7	2	3	0	10	2	7	0	3
	Low	1	0	0	0	1	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	8	2	3	0	11	2	7	0	3

Forest Service	High	1	0	0	0	1	0	1	0	1
	Moderate	16	3	5	2	21	5	20	0	20
	Low	4	0	0	0	4	0	4	0	4
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	21	3	5	2	26	5	25	0	25
Farm Service Agency - Commodity Credit Corporation	High	0	0	0	0	0	0	0	0	0
	Moderate	48	10	0	0	48	10	41	32	48
	Low	22	0	0	0	22	0	21	0	22
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	70	10	0	0	70	10	62	32	70
Food Safety and Inspection Service	High	0	0	0	0	0	0	0	0	0
	Moderate	12	1	0	0	12	1	12	0	5
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	12	1	0	0	12	1	12	0	5
Natural Resources Conservation Service	High	0	0	0	0	0	0	0	0	0
	Moderate	3	3	0	0	3	3	3	0	3
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	3	3	0	0	3	3	3	0	3
Office of Chief Financial Officer	High	11	10	0	0	11	10	10	1	10
	Moderate	13	2	0	0	13	2	11	0	12
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	24	12	0	0	24	12	21	1	22
Office of Chief Information Officer - Information Technology Management	High	0	0	0	0	0	0	0	0	0
	Moderate	2	1	2	0	4	1	4	0	0
	Low	1	0	0	0	1	0	1	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	3	1	2	0	5	1	5	0	0
Office of Chief Information Officer - National Information Technology Center	High	4	3	0		4	3	3	0	1
	Moderate	5	0	0	0	5	0	4	0	4
	Low	5	0	0	0	5	0	4	1	4
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	14	3	0	0	14	3	11	1	9

Rural Development	High	0	0	0	0	0	0	0	0	0
	Moderate	10	1	0	0	10	1	10	1	10
	Low	2	0	0	0	2	0	2	0	2
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	12	1	0	0	12	1	12	1	12
Risk Management Agency	High	0	0	0	0	0	0	0	0	0
	Moderate	3	3	0	0	3	3	3	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub-Total	3	3	0	0	3	3	3	0	0
TOTALS:	HIGH	16	13	0	0	16	13	14	1	12
	MOD	120	27	10	2	130	29	116	33	105
	LOW	35	0	0	0	35	0	32	1	32
	NOT CAT	0	0	0	0	0	0	0	0	0
GRAND TOTALS:		171	40	10	2	181	42	162	35	149

Totals for the entire Department are:

- Total USDA reportable systems – 287 (Question 1);
- Number of systems Certified and Accredited – 234 (Question 2a);
- Number of systems for which security controls had been tested and reviewed in the past year³³ – 37 (Question 2b); and
- Number of systems for which contingency plans had been tested during the past year in accordance with policy (Question 2c) - 214.

Question 3:

Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and Agency policy.

Agencies are responsible for ensuring the security of information systems used by a contractor of their Agency or other organization on behalf of their Agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another

³³ The Department requires annual testing of 29 key controls; our number was based on 100 percent testing of those controls.

Federal Agency, for example, a Federal service provider may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

3a. Does the Agency have policies for oversight of contractors? Yes/No

OIG requested the Department's policy for contractor oversight but it was not provided. OCIO responded that contractor oversight was specified in each individual contract.

3b. Does the Agency have a materially correct inventory of major information systems (including national security systems) operated by or under the control of such Agency. Yes/No

The Cyber Security Assessment and Management (CSAM) system is the official repository for the Department's system inventory. Our review disclosed a total of 287 FISMA reportable systems, which corresponded to the Department's inventory count.

3c. Does the Agency maintain an inventory of interfaces between the Agency systems and all other systems, such as those not operated by or under the control of the Agency? Yes/No

FISMA³⁴ requires agencies to maintain an inventory of information systems, which includes an identification of the interfaces between each system, and all other systems or networks, including those not operated by, or under the control of the agency.

We found the Department was not maintaining an accurate inventory of interfaces in CSAM. We reviewed each of the interfaces listed in each System Security Plan (SSP)³⁵ for the 287 FISMA reportable systems. We then compared that list of interfaces to those documented in CSAM and found that 162 out of the 287 systems were not accurately reporting interfaces with other systems. In most instances, the SSP documented more interfaces than were recorded in CSAM. Agencies are responsible for accurately documenting interface data in CSAM and failed to accurately account for all interconnections. Since interfaces allow the exchange of data between two systems, it is important that security controls in each interconnected system accurately reflect the risk of inadvertent disclosure of information. Without proper documentation and testing of those interfaces, the confidentiality, integrity, and availability of the exchanged data could have been compromised without discovery.

3d. Does the Agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the Agency? Yes/No

Interface agreements are required to be in place and operational on the SSP template provided to each agency.

³⁴ FISMA of 2002, Title III *Information Security*, dated December 17, 2002.

³⁵ 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 (National Institute of Standards and Technology (NIST), Special Publication (SP) 800-18, *Guide for Developing Security Plans for Federal Information Systems*, dated February 2006).

3e. The Agency inventory is maintained and updated at least annually. Yes/No

We found the Department conducted semi-annual inventory reconciliations.

3f. The IG generally agrees with the CIO on the number of Agency-owned systems. Yes/No

Our review of the CSAM inventory found 19 contractor systems. However, during our review of the SSPs, we discovered 31 systems were actually hosted or operated by a contractor. The number of systems owned by the Department should be decreased by the 12 contractor systems that are misreported in CSAM as agency owned systems. This does not change the total number of 287 FISMA reportable systems identified in CSAM.

3g. The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency. Yes/No

The number of contractor systems listed in CSAM is inaccurate. We found 12 additional contractor systems being reported as agency owned systems (see 3f).

Question 4:

Evaluation of Agency Plan of Action and Milestone (POA&M) Process

Assess whether the Agency has developed, implemented, and is managing an Agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.

4a. Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts? Yes/No

The OCIO security manual does not include policy for establishing a POA&M³⁶ process for reporting IT security deficiencies and for tracking the status of remediation efforts. Although there are no formal policies, the OCIO has prepared a standard operating procedure (SOP)³⁷ concerning the POA&M Management Process. Our review of the SOP determined that it was written prior to the implementation of CSAM and is no longer applicable. Also, we found that OMB's requirement³⁸ to link budgetary resources to POA&Ms has not been met. We found 1,263 out of 4,502 POA&Ms in CSAM did not have the required budgetary links. As a result of

³⁶ A POA&M is a tool that identifies tasks that need to be accomplished to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. It details resources required to accomplish the elements of the plan, milestones 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.

³⁷ *POA&M Management Process, Standard Operating Procedure*, dated February 27, 2008.

³⁸ OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated October 17, 2001, states that, "to promote greater attention to security as a fundamental management priority, OMB continues to take steps to integrate security into the capital planning and budget process," and requires each POA&M to be linked to its budgetary and capital planning by including the unique project identifier on all POA&Ms.

this lack of guidance, agencies were unclear about when to enter POA&Ms, what information should be included, and in some cases were not entering them at all (see 4c).

4a(1). Has the Agency fully implemented the policy? Yes/No

There is not a current Departmental policy for the POA&M process (See 4a).

4b. Is the Agency currently managing and operating a POA&M process? Yes/No

CSAM provided the Department an extremely useful tool for managing and operating POA&Ms. However, the Department and agencies are not effectively utilizing the tool (see 4c).

4c. Is the Agency's POA&M process an Agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the Agency or by a contractor of the Agency or other organization on behalf of the Agency? Yes/No

Our review of the POA&M³⁹ process found the Department does not have effective policies and procedures for reporting IT security deficiencies in CSAM. For example, our review at one agency identified at least 35 instances where POA&Ms should have been created, but were not. In fact, the agency has not entered POA&Ms into CSAM for any IT security weakness identified during fiscal year 2009. In another agency, we found 543 weaknesses that were not documented and tracked as POA&Ms. This occurred because the OCIO security manual does not include a policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts. Although there are no formal policies, the OCIO has prepared a Standard Operating Procedure⁴⁰ on the POA&M management process. Our review of the SOP determined that it was written prior to the implementation of CSAM and is no longer applicable.

Also, oversight of the POA&M process has not been a priority within the Department. As a result, sufficient resources have not been committed to provide Departmental and agency staffs' adequate training on POA&M management and oversight to ensure that all parties understand how to accomplish an effective POA&M program. A common theme found during our FY 2009 reviews was that POA&Ms were considered to have negative consequences by agency security personnel. They believed that the use of POA&Ms was discouraged by agency upper management because they were viewed as a failure of the security staffs to perform their responsibilities. Therefore, the security staffs were reluctant to record and track POA&Ms. As a result, the agency's IT resources are at a higher risk of compromise or malicious activity. OMB policy recognizes that the POA&M process is constructive. It ensures agencies are constantly reviewing their security posture and working towards finding and mitigating weaknesses.

³⁹ OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated October 17, 2001, required each agency to submit to OMB by October 31, 2001 (with brief quarterly updates thereafter), "a plan of action with milestones" to address all weaknesses identified by program reviews and evaluations. It defines a POA&M as a tool that identifies tasks needing to be accomplished to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. The goal of a POA&M should be to reduce the risk of the weakness identified. CSAM is used as the USDA POA&M repository, and to track and report to OMB progress toward mitigating the weaknesses.

⁴⁰ *POA&M Management Process, Standard Operating Procedure*, dated February 27, 2008.

4d. Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources? Yes/No

We determined that 100 percent of the POA&Ms entered into CSAM had a priority.

4e. When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)? Yes/No

Agencies are not creating all of the necessary POA&Ms, thus, the current POA&M process is not ensuring that all weaknesses were being entered (see 4c).

4f. For Systems Reviewed:

4f(1). Are deficiencies tracked and remediated in a timely manner? Yes/No

Agencies are bundling unrelated deficiencies into a single POA&M and are not creating the necessary POA&Ms for some identified weaknesses; therefore, the Department cannot be assured that deficiencies are tracked and remediated in a timely manner (see 4c).

4f(2). Are the remediation plans effective for correcting the security weakness? Yes/No

We found that agencies combined unrelated weaknesses into a single POA&M, which lowered the number of outstanding POA&Ms. For example, we found one agency combined eight unrelated weaknesses into one POA&M without any of the details required by NIST.⁴¹ This practice distorted the remediation tracking process which made it impossible to understand the internal control problem, determine whether it was an issue that affected other parts of the environment, and conclude if it was being mitigated.

Also, as noted in 4c above, agencies are not creating all necessary POA&Ms.

4f(3). Are the estimated dates for remediation reasonable and adhered to? Yes/No

Agencies are not creating all necessary POA&Ms and are bundling multiple deficiencies into others. Therefore, the resources required to accomplish the remediation are not defined, the tasks needing to be accomplished are not identified, and the milestones and scheduled dates are not documented (see 4c).

⁴¹ NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Section 2.6, dated May 2004, states that “the POA&Ms document identifies: (i) the tasks needing to be accomplished; (ii) the resources required to accomplish the elements of the plan; (iii) any milestones in meeting the tasks; and (iv) scheduled completion dates for the milestones.”

4g. Do program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)? Yes/No

When POA&Ms are properly entered, the OCIO can easily track their progress by using predefined queries in CSAM. Unfortunately, as noted in 4c, agencies are not entering POA&Ms.

4h. Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis? Yes/No

According to OCIO, the only review/validation of POA&M activities covered about 10 percent of the POA&Ms closed during fiscal year 2009. As noted in previous questions, the POA&M process in the Department is not working effectively.

Question 5:

IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the Agency's certification and accreditation (C&A) process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" for C&A work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

5a. Has the Agency developed and documented an adequate policy for establishing a C&A process that follows the NIST framework? Yes/No

The Department has issued adequate guidance⁴² for agencies to use during the C&A process. The guidance followed the NIST C&A framework.

5b. Is the Agency currently managing and operating a C&A process in compliance with its policies? Yes/No

Based on the OIG reviews performed throughout FY 2009, we found that agencies are not following NIST and Departmental⁴³ guidance when preparing C&A documentation. Agencies are required to submit their system C&A packages and all supporting documentation to the Department for an in-depth review (referred to as a concurrency review). During the concurrency review, the Department ensures that the documentation prepared to support system accreditation⁴⁴ is complete, accurate, reliable, and that it meets all NIST and other mandated

⁴² DM 3555-001 Chapter 11, Part 1, *Certification and Accreditation Methodology*, dated October 18, 2005.

⁴³ NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004, DM 3555-001, *Certification and Accreditation Methodology*, dated October 18, 2005.

⁴⁴ Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

documentation standards. We evaluated seven C&A concurrency reviews where the Department had concurred with the agencies' recommendations to accredit the system. We found that the agencies' security certification⁴⁵ documentation did not support accreditation. We determined that agencies had not followed NIST guidance in all seven cases. Specifically, we found that three SSPs,⁴⁶ four risk assessments (RA), and seven testing documents⁴⁷ did not meet NIST requirements; and two agencies did not select the required controls to test. In addition, when reviewing CSAM, we found there were 34 systems with an expired Authority to Operate (ATO) or Interim Authority to Operate (IATO).⁴⁸ We have reported problems in the C&A process since 2001, and attribute these continuing problems to a lack of commitment by agencies to a quality C&A process, as well as a lack of Departmental oversight. Agencies do not know if required system controls have been implemented correctly because the controls may not have been documented and tested. Systems, and the information in those systems, may be at risk if security controls have not been implemented correctly.

5c. For systems reviewed, does the C&A process adequately provide:

5c(1). Appropriate risk categories Yes/No

All seven C&A submissions in our sample had appropriate risk categories (see 5b).

5c(2). Adequate risk assessments Yes/No

Four of the seven RAs we reviewed during our C&A testing did not meet NIST requirements (see 5b).

5c(3). Selection of appropriate controls Yes/No

Appropriate controls had not been selected as required by NIST for two of the seven reviewed C&As (see 5b).

5c(4). Adequate testing of controls Yes/No

System controls had not been adequately tested for four of the seven C&As reviewed (see 5b).

⁴⁵ 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.

⁴⁶ The SSP is a required C&A document that provides an overview of the security requirements of the system and describes the controls in place (or planned) for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. (NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, dated February 2006).

⁴⁷ A Security Testing and Evaluation (ST&E) is one phase of the C&A where an independent party evaluates and conducts testing of the controls established in and around a system. The purpose is to determine whether controls as stated in the system documentation are adequate and operating as prescribed.

⁴⁸ An ATO or IATO is the last step in the C&A process. If C&A is adequate and meets NIST requirements an ATO is given for a period of 3 years. If, after assessing the results of the security certification, the agency deems that the risk to agency operations is unacceptable but there is an overarching need to place the system into operation or continue its operation, an IATO may be issued for up to 6 months in order for the agency to fix the vulnerabilities.

5c(5). Regular monitoring of system risks and the adequacy of controls Yes/No

We found two agencies were not performing continuous monitoring of security controls in accordance with NIST⁴⁹ guidance. Neither agency had documented the critical system controls that needed to be monitored, the frequency of that monitoring, or the actions to be taken based on the results of the monitoring. In addition, one agency did not effectively perform annual system self-assessments or document the results in CSAM as required. The lack of continuous monitoring was attributed to insufficient resources and agency staffs that did not realize the importance of continuous monitoring.

5d. For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented? Yes/No

The documentation for all seven C&As in our sample do not follow NIST requirements (see 5b).

Question 6:

IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

Provide a qualitative assessment of the Agency's process, as discussed in the Senior Agency Official for Privacy (SAOP) section, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.

6a. Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information? Yes/No

The Department has several manuals and regulations that adequately cover the OMB guidance.⁵⁰

6b. Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies? Yes/No

The Department needs to take additional actions to minimize the risk of unauthorized release of "privacy data" as required by OMB guidance.⁵¹ Due to the complexity and age of the legacy systems within USDA, the Department has not fully implemented its plan to reduce the use of social security numbers (SSN) as identifiers in application databases. OMB requires that the Department track all sensitive data extracts (i.e., extracts containing SSNs) to ensure the data are

⁴⁹ NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, dated December 2007, requires agencies to "monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis."

⁵⁰ Departmental Regulation 3505-003, *Access Control Policy*, dated August 11, 2009; DM 3515-001, *Collection of Web Page Cookies & Privacy Requirements*, dated August 19, 2004; DM 3515-002, *Privacy Impact Assessment*, dated February 17, 2005; DM 3545-001, *Computer Security Training and Awareness*, dated February 17, 2005; DM 3550-002, *Sensitive but Unclassified (SBU) Information Protection*, dated February 17, 2005.

⁵¹ OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006, OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

erased within 90 days or once they are no longer being used. The Department was not aware of this requirement and had not implemented a policy or plan to address this task. Also, because of technical issues associated with getting encryption software to run on USDA workstations and the overall size of the Department and the diversity of programs, full disk encryption has only been implemented on 53 percent of the Department's laptops. As a result, the potential exists for sensitive information to reside on unencrypted computers/devices.⁵²

6c. Has the Agency developed and documented an adequate policy for PIA's? Yes/No

The Department has issued policy and procedures⁵³ that adequately addresses privacy impact assessments.

6d. Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate PIA? Yes/No

We reviewed the Department's PIA implementation as required by the e-Government Act of 2002.⁵⁴ The Department is required to publish all PIAs on a publicly accessible website. We found that 13 of the required 122 PIAs were missing from the Department's website.

**Question 7:
Configuration Management**

7a. Is there an Agency-wide security configuration policy? Yes/No

NIST⁵⁵ states "although the solutions to IT security are complex, one simple yet effective tool is the security configuration checklist." Both NIST and the Department⁵⁶ have issued policies requiring its use when deploying certain software. We found that agencies are not using the required checklists when deploying the software covered by NIST requirements. Specifically, we scanned systems at two agencies using a commercially available software tool that compares implemented server settings with those required by NIST and Departmental checklists. One agency stated it used a checklist, but did not know if it was NIST compliant (we determined that it was not). The other agency stated the security configuration checklist settings caused operational problems. As a result, it implemented only 69 percent of the settings. The agency had not documented the reasons for not implementing the remaining 31 percent of the settings. The use of security configuration checklists to deploy software and hardware ensures consistency across the agency and ease of maintenance. When USDA agencies do not use and follow the checklists, helpdesk support, inventory management capabilities, and operating costs are impacted due of the lack of standardization.

⁵² The next step of the Department's encryption effort will include external storage media. OCIO stated this will begin in the next few months.

⁵³ DM 3515-002, *Privacy Impact Assessment*, dated February 17, 2005.

⁵⁴ e-Government Act of 2002, Public Law 107-347, dated December 17, 2002, requires agencies to conduct PIA for new IT investments and online information collections. A PIA is a review of how information about individuals is handled within the agency when the agency uses IT to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information.

⁵⁵ NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*, dated May 2005.

⁵⁶ OCIO issued a memorandum, *Required Use of Security Configuration Guides*, dated March 10, 2009.

7a(1). For each Operating System (OS)/platform/system for which your Agency has a configuration policy, please indicate the status of implementation for that policy.

Although the Department has an agency-wide configuration policy, OIG only tested compliance with the Microsoft Windows Server 2003 OS (see question 7a). We are therefore marking all of the below configuration policies⁵⁷ as “adopted agency-wide policy and have started implementation.”

- Microsoft Windows Server 2003
- Microsoft Windows XP
- Cisco IOS
- Redhat Enterprise Linux 4
- Sun Solaris 10
- Microsoft Windows 2000
- IBM AIX 4
- Oracle Database 10g
- Microsoft Exchange 2007 for Windows Server 2003
- Research in Motion Blackberry
- Apple Mac OS X

In addition, OMB⁵⁸ requires agencies with Windows Vista or Windows XP operating systems, (or plans to upgrade to these operating systems), to adopt standard security configurations on workstations by February 1, 2008. The standard security configurations have been developed by NIST, the Department of Defense, and the Department of Homeland Security and are commonly referred to as the Federal Desktop Core Configuration (FDCC). Because of the complexity of the Department and its many diverse systems, it did not meet the OMB mandated deadline. The Department issued a memorandum on February 15, 2008, which required agencies to be FDCC compliant by July 31, 2008. As of September 30, 2009, the Department reported only 8 percent of machines had deployed 100 percent of the FDCC standard security configuration settings. However, for those machines without full deployment of the FDCC standard security configuration settings, the Department reported an average of about 90 percent of the settings were deployed. We have not validated this percentage or the actual settings deployed. As a result, we do not know the extent to which their workstations are properly secured and in compliance with the FDCC.

7b. Indicate the status of the implementation of Federal Desktop Core Configurations (FDCC) at your Agency :

7b(1). Agency has documented deviations from FDCC standard configuration. Yes/No

We received a listing of documented FDCC standard configuration deviations provided by the Department. The listing did not include all agencies and was inconsistent with what we found at

⁵⁷ This is a list of operating systems for various hardware devices by vendor which is taken from the Cyberscope (OMB FISMA Website) drop down menus that correspond to the equivalent published USDA configuration guides. USDA has some guides that did not have a corresponding Cyberscope drop down menu.

⁵⁸ OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, dated March 22, 2007.

the two agencies reviewed. For example, we found 20 security settings were not implemented in the two agencies, while the Department had 14 deviations documented for these agencies.

7b(2). New Federal Acquisition 2008-004 language, which modified “Part 39-Acquisition of Information Technology,” is included in all contracts related to common security settings. Yes/No.

Our review at two agencies found the required language included in procurement contracts. However, the Department reports that the acquisition language was not found in all contracts.

**Question 8:
Incident Reporting**

8a. How often does the Agency comply with documented policies and procedures for identifying and reporting incidents internally? Answer will be a percentage range

The Department has made progress in the required⁵⁹ reporting of security incidents⁶⁰ to law enforcement and the US-Computer Emergency Readiness Team (US-CERT).⁶¹ However, we found that due to the volume of incidents throughout the year, the Department did not always follow its own security review procedures. We reviewed 49 incidents (5 privacy-related) and found only 18 of the 49 incidents (37 percent) were handled in accordance with Departmental procedures, which require that agencies submit documentation to the OCIO and carry out pre-defined steps. The procedures also require that agencies undertake and document a thorough investigation of the initial cause of the incident. In addition, the procedures require agencies to

submit detailed final reports to the OCIO outlining the steps taken to mitigate the cause of the incident. We present the details of our findings below:

- 19 incidents did not have all required documentation;
- 16 incidents were reported as closed before the required reviews were completed;
- 12 incidents were not adequately investigated;
- 12 incidents had incomplete final reports; and
- 5 privacy-related incidents were improperly handled.

OCIO officials stated that errors occurred in handling of the incidents due to the volume of the reported incidents. We found that OCIO staff and contractor personnel were unclear as to what procedures to follow when security incidents were reported. For example, OCIO and its contractor staff did not always ensure that agencies included the checklists contained in the

⁵⁹ *Agriculture Security Operations Center Computer Incident Response Team-Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents*, dated June 9, 2009.

⁶⁰ DM 3505-000, *USDA Cyber Security Incident Handling Procedures*, dated March 20, 2006, states an incident is a violation or imminent threat of violation of computer security policies, acceptable use or standard computer security practices. It is also any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, or disruption or denial of service.

⁶¹ US-CERT provides response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local Government, industry, and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCS) at the Department of Homeland Security (DHS). The NCS was established by DHS to serve as the Federal Government’s cornerstone for cybersecurity coordination and preparedness.

procedure's appendix with their incident submissions. When we inquired as to why the checklists were not included, OCIO personnel stated that since checklists were an appendix to the procedures they were not required. The appendix's checklists were required when an agency submits an incident.

OMB⁶² has mandated that an incident be reported within 1 hour when it may involve privacy information. The Department included OMB's mandated timeframe in its procedures for handling privacy incidents. OCIO officials stated that staff did not always follow procedures when handling privacy incidents because of the unrealistic timeframe mandated by OMB, even though it had included the timeframe in its procedures. This failure to follow policies and procedures may affect the Department's ability to rapidly detect incidents and the loss of privacy information. The rapid detection and reporting of incidents is essential for minimizing data loss and destruction, mitigating any exploited weaknesses, and restoring computing services.

8b. How often does the Agency comply with documented policies and procedures for timely reporting of incidents to US-CERT? Answer will be a percentage range.

We found 41 of the 49 reviewed incidents (84 percent) were timely reported to US-CERT in accordance with Departmental policy.

8c. How often does the Agency follow documented policies and procedures for reporting to law enforcement? Answer will be a percentage range.

We found all 49 (100 percent) of the reviewed incidents were reported to OIG in accordance with Departmental policies and procedures.

⁶² OMB Memorandum 07-16 requires reporting to US-CERT within 1 hour of discovery/detection.

**Question 9:
Security Awareness Training**

Provide an assessment of whether the Agency has provided IT security awareness training to all users with log-in privileges, including contractors. Also provide an assessment of whether the Agency has provided appropriate training to employees with significant IT security responsibilities.

9a. Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log-in privileges, and providing them with suitable IT security awareness training? Yes/No

The Department has made significant improvements to ensure that all employees receive security awareness training; however, there is no consistent method for tracking security training for USDA contractors. The Department has a database to maintain a record of all contractors within the Department; however, use of the database is not required and only two agencies are using it. Therefore, it is difficult for the Department and the agencies to identify contractors, their access controls, and whether they have received the required training.⁶³

9b. Report the following for your Agency:

9b(1). Total number of people with log-in privileges to Agency systems.

The Department did not provide the total number of people with log-in privileges to USDA systems in a timely manner. On October 8, 2009, OCIO sent out a data call to all USDA agencies requesting that they provide this information. Because the last agency responded on November 6, 2009, we have not had an opportunity to determine the accuracy of the information.

9b(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program."

The Department has a total of 110,828⁶⁴ employees and an unknown number of contractors. As of July 2009, 120,956 employees and contractors had taken the Department's security awareness training.

9b(3). Total number of employees with significant information security responsibilities.

The Department did not provide a list of employees with significant information security responsibilities in a timely manner. On October 8, 2009, OCIO sent out a data call to all USDA agencies requesting that they provide this information. The last agency responded on November 6, 2009. Therefore, we have not had an opportunity to review the accuracy of the information.

⁶³ FISMA of 2002, Title III *Information Security*, dated December 17, 2002 and NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, dated December 2007.

⁶⁴ As of August 24, 2009.

9b(4). Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, “Information Technology Security Training Requirements: A Role- and Performance-Based Model”

Federal law, NIST, and the Department⁶⁵ require all users with significant security responsibilities to receive specialized role-based training in addition to security awareness training. We were unable to determine whether all employees that should have received the additional role-based training actually received it. Agencies interpreted the definition of “significant IT security responsibilities” differently because the Department’s security training policy did not clearly define what “significant IT security responsibilities” encompassed. For example, one agency determined that only the staff working in its security office needed the training. Another agency interpreted the definition of significant security responsibilities to apply to all staff with elevated privileges⁶⁶ to the agency’s systems. As a result, employees who were actually assigned significant IT security responsibilities did not receive the required additional training.

**Question 10:
Peer-to-Peer File Sharing**

10. Does the Agency explain policies regarding the use peer-to-peer file sharing in IT security awareness training, ethics training, or any other Agency-wide training? Yes/No

During fiscal year 2009, the Department issued a policy⁶⁷ stating that the use of commercial peer-to-peer (P2P)⁶⁸ software was prohibited on all USDA equipment and networks without explicit authorization from the OCIO. The policy further stated that agency personnel, contractors, and partners should not download and install commercial P2P software.

We determined the P2P file sharing policy was not in the Department’s IT security awareness training. This occurred because the Department used the Information Systems Security Line of Business course. This course was designed to meet the NIST requirement for basic awareness training across the Government, and did not include individual Department/agency policies or procedures. Therefore, the Department can not verify that every employee and contractor has been trained on the P2P policy.

⁶⁵ NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998; FISMA, and DM 3545-001, *Computer Security Training and Awareness*, dated February 17, 2005.

⁶⁶ Elevated privileges are those above a normal system user, such as staff that have administrative privileges to servers, databases and networks.

⁶⁷ OCIO Memorandum, “*Use of Peer-to-Peer Software Policy*,” dated March 17, 2009.

⁶⁸ P2P is software often used to obtain freeware, shareware, and bootleg software. The use of this software creates vulnerabilities, which can be exploited to allow malicious code and other illegal material into the USDA network.

Abbreviations

ATO	Authority to Operate
C&A	certification and accreditation
CIO	Chief Information Officer
CSAM	Cyber Security Assessment and Management
DHS	Department of Homeland Security
DM	Departmental Manual
ERS	Economic Research Service
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
FNS	Food Nutrition Service
GAO	U.S. Government Accountability Office
GISRA	Government Information Security Reform Act
IATO	Interim Authority to Operate
IG	Inspector General
IT	information technology
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
NRCS	Natural Resources Conservation Service
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
P2P	Peer to Peer
PIA	Privacy Impact Analysis
POA&M	Plan of Action and Milestones
PL	Public Law
RA	risk assessment
SOP	Standard Operating Procedure
SP	Special Publication
SSN	Social Security Number
SSP	System Security Plan
US-CERT	US-Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture

Informational copies of this report have been distributed to:

XXXXXXXXXXXXXXXXXXXX (#)

XXXXXXXXXXXXXXXXXXXX (#)

XXXXXXXXXXXXXXXXXXXX (#)