U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

U.S. Department of Agriculture
Office of the Chief Information Officer
Fiscal Year 2008 Federal Information Security Management Act Report

Report No. 50501-13-FM
September 2008

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 30, 2008

The Honorable Jim Nussle
Director
Office of Management and Budget
Eisenhower Executive Office Building
1650 Pennsylvania Avenue NW.
Washington, D.C. 20503

Subject: U.S Department of Agriculture Office of the Chief Information Officer
Fiscal Year 2008 Federal Information Security Management Act Report
(Audit Report No. 50501-13-FM)

Dear Mr. Nussle:

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 numerous actions to improve the security over their IT resources; however, additional actions are still needed toward establishing an effective security program.

Sincerely,

/s/

Phyllis K. Fong
Inspector General

Executive Summary

U.S. Department of Agriculture Office of the Chief Information Officer Fiscal Year 2008 Federal Information Security Management Act Report (Audit Report No. 50501-13-FM)

Results in Brief

The efforts of the U.S. Department of Agriculture's (USDA) Office of the Chief Information Officer (OCIO) and the Office of Inspector General (OIG) over the past several years have continued to heighten program managers' awareness of the need to plan and implement effective information technology (IT) security. OCIO continued to improve its oversight role this year. The most important achievement for the Department was the implementation of the Cyber Security Assessment and Management (CSAM) system. The CSAM tool is a comprehensive Federal Information Security Management Act (FISMA) monitoring system developed by the Department of Justice. CSAM facilitates the Department's ability to identify common threats and vulnerabilities, supports a security control baseline to achieve FISMA compliance, and provides comprehensive IT weakness tracking to include:

- Plans of action and milestones (POA&M) relative to security;[1]
- Security categorizations and identification of financial systems;[2]
- Identification of core and common controls;
- Information concerning the application of National Institute of Standards and Technology (NIST) security controls to meet FISMA;
- Results of security control monitoring; and
- Analyses of compliance information.

When fully implemented, CSAM should help in the Department's effort to alleviate the IT material control weakness. However, until this system is fully populated and the Department's policies and procedures are in place and are fully operational, IT will continue to be a material weakness.

[1] A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for keysteps in meeting the task, and scheduled completion dates for the milestones. FISMA requires agencies to prepare POA&Ms for security weaknesses at the program and system levels.

[2] Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization.

The USDA is a complex organization with 29 separate agencies. We understand that a robust IT security program takes time to mature. The Department has continued to improve its security program; however, more needs to be accomplished. We continue to believe, as we reported in previous years, that the best approach to correcting the IT control weaknesses within the Department is to create a plan, with the cooperation of the agencies, that systematically addresses each issue.

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

The following summarizes the weaknesses discussed in exhibit A of this report, in which we respond to the Office of Management and Budget (OMB) questions as required by OMB Memorandum No. M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* dated July 14, 2008.

- For the last 2 years, we found that the information system inventory counts were accurate. However, agencies did not populate the inventory with system interfaces as required by FISMA.[3]

- The POA&M process requires agencies to assess the severity of weaknesses and prioritize required corrective action. There are currently over 2,600 POA&Ms in the CSAM; of those we found 683 POA&Ms with a priority of "None" and 500 with a severity level of "Not Applicable." In addition, 101 were inappropriately recorded as "Exclude From OMB" and 50 were cancelled and recreated in order to extend due dates for corrective action.

- OCIO improved its concurrency review process in assessing the quality of the certification and accreditation (C&A), documentation during fiscal year 2008.[4] We found that agencies' C&A packages generally did not meet NIST requirements.[5] The

[3] FISMA Section 3505(c) requires the head of each agency to develop and maintain an inventory of major information systems. Per FISMA, the identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. NIST Special Publication (SP) 800-53 control CA-3, requires that the organization must carefully consider the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks.

[4] The USDA concurrency review is a quality control process by OCIO to review the C&A documentation prior to approving an Authority to Operate for the agency IT systems.

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

packages submitted to OCIO did not always include complete documentation of all the required C&A elements. [6]

- The Department and its agencies made substantial improvements in the privacy impact assessment (PIA) process. This process requires agencies to perform analyses of how personal information is protected in their IT systems. We found that PIAs were documented for each system. Agencies appointed Privacy Officers and OCIO facilitates a monthly meeting to discuss privacy issues. In addition, privacy training was given to approximately 92 percent of USDA personnel during the fiscal year. However, we found that 8 of the 12 System of Records Notices (SORN) we reviewed were inaccurate or out-of-date. [7]

- OMB Memorandum No. M-07-16[8] requires that agencies reduce the volume of personally identifiable information (PII) within their systems, when possible. It also requires that agencies encrypt all mobile devices (e.g., laptops). The Department has a plan for protecting PII, but had not yet fully implemented it. For example, of the approximate 54,000 laptops within the Department, we found that 4.23 percent had been fully encrypted.

- Departmental agencies were not always using the mandated NIST security configuration checklists when deploying hardware and software.[9] The checklists are tools that contain instructions and/or procedures for configuring an IT product to an operational environment to assist in implementing a baseline level of security. This occurred because agencies were not aware that completing the checklists was a mandated requirement.

- On March 27, 2007, OMB required the deployment of the Federal Desktop Core Configurations (FDCC). FDCC defines the minimum IT security requirements. For example, it includes procedures for managing password protection, installing patches, and performing vulnerability scans for systems that employ Windows XP and Windows Vista. The Department and its

[6] Agency owners of IT systems are required to submit documentation showing that their systems are secure. For example, in addition to other required documents, this documentation should include such items as security categorization documents, risk assessments, privacy act assessments, system security plans, security test and evaluation plans, and security assessment reports.

[7] A SORN is a notice provided to the public of the existence and character of a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of a system, and establishes what information about the system must be included.

[8] OMB Memorandum No. M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* dated May 22, 2007.

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

agencies were diligently testing settings and were in various stages of deployment. We noted that only approximately 4.63 percent of the Department's laptops/desktops were fully compliant with FDCC.

- The Department and its agencies were not following documented policies and procedures for identifying and reporting incidents internally to OCIO and OIG and/or externally to law enforcement authorities and the U.S. Computer Emergency Readiness Team (US-CERT). These incidents may involve lost and/or stolen computers, unauthorized access to an agency's network, etc. This occurred because the system used by OCIO to track and manage incidents was manually intensive and/or members of the incident response team had not received adequate formal training. As a result, USDA cannot be assured that all incidents were identified, and/or that incidents were being properly investigated and corrected.

  We found that 42 of 429 incidents were not reported to OIG. In addition, our review of 162 incidents over 15 days old disclosed that agencies had not created the required POA&Ms for 161 of these incidents. Depending upon the type of incident, this could result in an extended period of time before the incident is corrected and potential malicious activity prevented. We also found instances where documentation supporting the closure of the incident needed improvement.

- The Department and its agencies continue to make progress in the area of Security Awareness Training. Approximately 92 percent of all USDA employees received the required training during fiscal year 2008.[10] However, not all contractors appeared to be receiving the required training.

- We found that USDA was not adequately monitoring and prohibiting the downloading of peer to peer (P2P) software.[11] This occurred because OCIO believed P2P activity did not pose a significant threat compared to other types of incidents and, therefore, did not concentrate on this activity. As a result, USDA networks were vulnerable to damage that could be caused by malicious software, viruses, and worms imbedded within P2P files.

[10] Federal Information Security Management Act of 2002; OMB Circular No. A-130, *Security of Federal Automated Information Resources*, dated February 8, 1996; Department Manual (DM) 3545-001, *Computer Security Training and Awareness*, dated February 17, 2005; and OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006.

[11] P2P is a method of file sharing over a network in which individual computers are linked via the Internet or a private network to share programs/files, often illegally. Users download files directly from other users' computers rather than from a central server.

For example, we found that P2P reports were not distributed to agencies for almost 5 months of fiscal year 2008. Departmental policy requires that an incident be reported when P2P activity exceeds 75 hits per week from/to a single computer. We found 116 instances where P2P activity totaling more than 75 occurrences in 1 week was not declared an incident. In addition, agencies were not always reviewing the P2P reported activity.

- NIST and OMB require that a risk assessment be performed prior to an agency connecting to an e-Authentication (e-Auth) system (a central authentication point for electronic Government systems) to determine the level of authentication needed.[12] A separate risk assessment is required to provide assurance that business transactions have the required level of verification for authentication. Authentication risks with potentially higher consequences require higher levels of assurance. For example, a low level of assurance would only require a user ID and password. A high level of assurance would require "in-person" methods approved by OCIO. USDA was not able to provide a complete and/or accurate listing of systems that used e-Auth. In most instances, the agencies in our sample told us they were unaware of any requirement to do an e-Auth risk assessment prior to connecting to the system. Starting in fiscal year 2009, OCIO stated that the e-Auth risk assessment will be included in the overall risk assessment.

- Departmental guidance requires that agencies perform vulnerability scans on their IT systems. If vulnerabilities are identified, management should analyze the vulnerability to determine if it is willing to accept the risk or corrective action is needed. If it is determined that corrective action is needed, but not accomplished within 30 days, a POA&M should be established.[13] The POA&M process assists agencies with monitoring the timeliness of corrective actions. We found 265 vulnerabilities that existed for over 30 days without recorded POA&Ms. We also found devices on an agency's network that the agency was not aware of and, as a result, that were not scanned. Vulnerabilities on an agency's network could result in systems that are at an unnecessarily high risk of exploitation.

[12] NIST SP 800-63, *Electronic Authentication Guideline*, dated April 2006; and OMB Memorandum No. 04-04, *E-Authentication Guidance for Federal Agencies,* dated December 2003.
[13] DM 3530-001, *Vulnerability Scan Procedures*, dated July 20, 2005.

- We found that 134 of the 144 disaster recovery plans we reviewed were not documented in accordance with Federal and Departartmental guidance.[14] This documentation is required to provide IT security personnel with their detailed roles and responsibilities in the event of a disaster. Without adequate documentation, we could not determine whether the plans had been tested. In addition, the lack of documentation may prevent an effective continuity of operation plan from being implemented and impact the agency's ability to meet its mission.

- Agencies were not always adequately patching software for known vulnerabilities. We found over 2,100 missing patches. Routinely applying patches is an effective method of mitigating risk and/or correcting identified vulnerabilities.

Recommendations In Brief

Recommendations have been reported at the agency level. Therefore, we did not make any recommendations in this report.

[14] NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* dated June 2002; and DM 3570-001, *Disaster Recovery and Business Resumption Plans*, dated February 17, 2005.

Abbreviations Used in This Report

ASSERT	Automated Security Self-Evaluation and Remediation Tracking
C&A	certification and accreditation
CCC	Commodity Credit Corporation
CIO	Chief Information Officer
CS	OCIO-Cyber Security
CSAM	Cyber Security Assessment and Management
DA	Departmental Administration
DM	Departmental Manual
e-Auth	e-Authentication
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FNS	Food and Nutrition Service
FS	Forest Service
FSA	Farm Service Agency
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
IG	Inspectors General
IT	Information Technology
ITS	Information Technology Services
NASS	National Agricultural Statistics Service
NFC	National Finance Center
NITC	National Information Technology Center
NIST	National Institute of Standards and Technology
NRCS	Natural Resources Conservation Service
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OIG	Office of Inspector General
P2P	peer-to-peer
PIA	Privacy Impact Assessment
PII	personally identifiable information
POA&M	plan of action and milestones
SORN	System of Record Notices
SP	Special Publication
SSP	system security plan
US-CERT	United States Computer Emergencies Readiness Team
USDA	U.S. Department of Agriculture
WCTS	Washington Communications and Technology Services

Table of Contents

Background and Objectives

Background

Improving the overall management and security of information technology (IT) resources is a top priority in the U.S. Department of Agriculture (USDA). As technology has enhanced the ability to share information instantaneously among computers and networks, it has also made organizations more vulnerable to unlawful and destructive penetration and disruption. Insiders with malicious intent, recreational and institutional hackers, and attacks by intelligence organizations of other countries are just a few of the threats that pose a risk 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, the Federal Information Security Management Act (FISMA). FISMA permanently reauthorized the framework established in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal Government's information and information systems, such as the development of minimum standards for agency systems. The National Institute of Standards and Technology (NIST) has been tasked to work with agencies in the development of 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, and is consistent with existing information security guidance issued by the Office of Management and Budget (OMB) and NIST. Most importantly, however, the provisions consolidate these separate requirements and guidance into an overall framework for managing information security. It establishes new annual reviews, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

FISMA assigns specific responsibilities to OMB, agency heads, Chief Information Officers (CIO), and Inspectors General (IG). OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. This includes the authority to approve agency information security programs. OMB is also required to submit an annual report to Congress summarizing the results of agencies' evaluations of its information security programs.

Each agency must establish an agency-wide risk-based information security program to be overseen by the agency CIO to ensure that information security is practiced throughout the lifecycle of each agency system. Specifically, this program must include:

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

- development and implementation of risk-based, cost effective policies and procedures to provide security protections for information collected or maintained by or for the agency;

- training on security responsibilities for information security personnel and on security awareness for agency personnel;

- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;

- a process for identifying and remediating any significant deficiencies;

- procedures for detecting, reporting, and responding to security incidents; and

- an annual program review by agency program 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 IG or an independent evaluator, and the results of these evaluations are to be reported to OMB.

Objectives

The audit objective was to form a basis for conclusion regarding the status of USDA's overall IT security program by:

- Evaluating the effectiveness of the Office of the Chief Information Officer's (OCIO) oversight role of agency CIOs and FISMA compliance;

- determining whether agencies have maintained 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 plan of action and milestones consolidation and reporting process;

- analyzing USDA's Privacy Act[15] documentation to ensure USDA has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information; and

- reviewing the adequacy of e-Authentication risk assessments.

[15] The Privacy Act of 1974, 5 U.S.C. § 552a.

Scope and Methodology

The scope of our review was Departmentwide and included agency audits relating to IT completed during fiscal year 2008. We conducted this audit in accordance with *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 that 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 May to September 2008. In addition, the results of IT control testing and compliance with laws and regulations performed by contract auditors at three additional agencies are included in this report. Further, the results of our most recent general control and application control reviews were considered and incorporated into this report. In total, our fiscal year 2008 audit work covered eight agencies and/or staff offices: Departmental Administration (DA), Food and Nutrition Service (FNS), Forest Service (FS), Farm Service Agency (FSA), National Agricultural Statistics Service (NASS), Natural Resources Conservation Service (NRCS), Office of the Chief Financial Officer, and OCIO. These agencies and staff offices operate approximately 114 of the OCIO estimated 249 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 Office of Inspector General (OIG) contractors. Contractor audit work consisted primarily of audit procedures found in the U.S. Government Accountability Office (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 No. M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 14, 2008; and

- Performed detailed testing specific to FISMA requirements at selected agencies as detailed in this report.[16]

[16] DA, OCIO-Washington Communications and Technology Services, and NASS.

Section C: Inspector General (IG) Questions

1. **In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and Federal Information Processing Standards Publication (FIPS) 199 impact level (high, moderate, low, or not categorized).**

   As required in the Federal Information Security Management Act (FISMA), the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

   Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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

   (See table on next page.)

2. For the Total Number of 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 (C&A), security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

Bureau Name (OIG Reviewed)[17]	FIPS 199 System Impact Level	Question 1.						Question 2. – Agency Reported					
		1.a. Fiscal year 2008 Agency Systems		1.b. Fiscal year 2008 Contractor Systems		1.c. Fiscal year 2008 Total Number of Systems (Agency and Contractor systems)		2.a[18] Number of systems certified and accredited As of 9/12/08		2.b[19] Number of systems for which security controls have been tested and reviewed in the past year. As of 9/12/08		2.c[20] Number of systems for which contingency plans have been tested in accordance with policy As of 9/12/08	
		Total #	# Rev.	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
1. DA	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	5	5	0	0	5	5	N/A	N/A	N/A	N/A	N/A	N/A
	Low	2	2	0	0	2	2	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	7	7	0	0	7	7	N/A	N/A	N/A	N/A	N/A	N/A
2. FNS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	7	3	3	3	10	6	N/A	N/A	N/A	N/A	N/A	N/A
	Low	1	0	0	0	1	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	8	3	3	3	11	6	N/A	N/A	N/A	N/A	N/A	N/A
3. FS	High	1	0	0	0	1	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	18	7	2	2	20	9	N/A	N/A	N/A	N/A	N/A	N/A
	Low	5	0	0	0	5	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	24	7	2	2	26	9	N/A	N/A	N/A	N/A	N/A	N/A
4. FSA	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	21	2	0	0	21	2	N/A	N/A	N/A	N/A	N/A	N/A
	Low	2	0	0	0	2	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	23	2	0	0	23	2	N/A	N/A	N/A	N/A	N/A	N/A

[17] Departmental Administration (DA), Food and Nutrition Service (FNS), Forest Service (FS), Farm Service Agency (FSA) (includes Commodity Credit Corporation (CCC)) National Agricultural Statistics Service (NASS), Natural Resources Conservation Service (NRCS), Office of the Chief Financial Officer-National Finance Center (OCFO-NFC), and Office of the Chief Information Officer (OCIO) (includes Information Technology Services (ITS), National Information Technology Center (NITC), and Washington Communications and Technology Services (WCTS)).

[18] These numbers are from the Cyber Security Assessment and Management (CSAM) system which is not fully populated. In addition, these include fiscal year 2006 and 2007 C&As which OIG has already stated are inadequate, see Question 5. Therefore, we do not attest to numbers in this column.

[19] Office of Inspector General (OIG) cannot determine an accurate number of systems that have self assessments completed. CSAM is in the implementation phase and self assessments will not be populated until September 19, 2008, which is after our audit timeframes.

[20] We cannot attest to numbers in this column. Agencies have not completed inputting all documentation into CSAM and have not identified all systems tested.

Bureau Name (OIG Reviewed)[21]	FIPS 199 System Impact Level	Question 1.						Question 2. – Agency Reported					
		1.a. Fiscal year 2008 Agency Systems		1.b. Fiscal year 2008 Contractor Systems		1.c. Fiscal year 2008 Total Number of Systems (Agency and Contractor systems)		2.a[22] Number of systems certified and accredited As of 9/12/08		2.b[23] Number of systems for which security controls have been tested and reviewed in the past year. As of 9/12/08		2.c[24] Number of systems for which contingency plans have been tested in accordance with policy As of 9/12/08	
		Total #	# Rev.	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
5. NASS	High	1	1	0	0	1	1	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	5	5	0	0	5	5	N/A	N/A	N/A	N/A	N/A	N/A
	Low	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	6	6	0	0	6	6	N/A	N/A	N/A	N/A	N/A	N/A
6. NRCS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	3	3	0	0	3	3	N/A	N/A	N/A	N/A	N/A	N/A
	Low	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	3	3	0	0	3	3	N/A	N/A	N/A	N/A	N/A	N/A
7. OCFO-NFC	High	10	9	0	0	10	9	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	3	3	0	0	3	3	N/A	N/A	N/A	N/A	N/A	N/A
	Low	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	13	12	0	0	13	12	N/A	N/A	N/A	N/A	N/A	N/A
8. OCIO	High	5	3	0	0	5	3	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	14	2	0	0	14	2	N/A	N/A	N/A	N/A	N/A	N/A
	Low	6	0	0	0	6	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	25	5	0	0	25	5	N/A	N/A	N/A	N/A	N/A	N/A
USDA Totals	**High**	**17**	**13**	**0**	**0**	**17**	**13**	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	**76**	**30**	**5**	**5**	**81**	**35**	N/A	N/A	N/A	N/A	N/A	N/A
	Low	**16**	**2**	**0**	**0**	**16**	**2**	N/A	N/A	N/A	N/A	N/A	N/A
	Total	**109**	**45**	**5**	**5**	**114**	**50**	N/A	N/A	N/A	N/A	N/A	N/A

[21] DA, FNS, FS, FSA (includes CCC), NASS, NRCS, OCFO-NFC, and OCIO (includes ITS, NITC, WCTS).

[22] These numbers are from the CSAM system which is not fully populated. In addition, these include fiscal year 2006 and 2007 C&As which OIG has already stated are inadequate, see Question 5. Therefore, we do not attest to numbers in this column.

[23] OIG cannot determine an accurate number of systems that have self assessments completed. CSAM is in the implementation phase and self assessments will not be populated until September 19, 2008, which is after our audit timeframes.

[24] We cannot attest to numbers in this column. Agencies have not completed inputting all documentation into CSAM and have not identified all systems tested.

3.a. 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, the Office of Management and Budget (OMB) policy and the National Institute of Standards and Technology (NIST) guidelines, national security policy, and agency policy.

Self-reporting NIST Special Publication 800-53 requirements by a contractor or other organization is not sufficient; however, self-reporting by another Federal agency may be sufficient.

(OIG's response is underlined below.)

Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

OCIO relies on agencies to perform 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, and NIST. U.S. Department of Agriculture (USDA) employs contractors in many aspects of its system operations. Contractors are used for network administration, system development, and as system administrators. We found documented evidence that oversight of contractor systems was being accomplished.

3.b. The agency has developed a complete inventory of major information systems (including major national security systems) used or operated by an agency or a contractor or other organization on behalf of the agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

(OIG's response is underlined below.)

Response Categories:

- **The inventory is approximately 0-50 percent complete**
- **The inventory is approximately 51-70 percent complete**
- **The inventory is approximately 71-80 percent complete**
- **The inventory is approximately 81-95 percent complete**
- **The inventory is approximately 96-100 percent complete**

The efforts of the USDA's OCIO and OIG in the past several years have continued to heighten program managers' awareness of the need to plan and implement effective information technology (IT) security. OCIO continued to improve its oversight role this year. The most important achievement for the Department was the implementation of the Cyber Security Assessment and Management (CSAM) system. The CSAM tool is a comprehensive Federal Information Security Management Act (FISMA) monitoring system developed by the Department of Justice. CSAM facilitates the Department's ability to identify common threats and vulnerabilities, supports a security control baseline to achieve FISMA compliance, and provides comprehensive IT weakness tracking to include:

- Plans of action and milestones (POA&M) relative to security;[25]
- Security categorizations and identification of financial systems;
- Identification of core and common controls;
- Information concerning the application of NIST security controls to meet FISMA;
- Results of security control monitoring; and
- Analyses of compliance information.

When fully implemented, CSAM will help in the Department's effort to alleviate material IT control weakness. However, until this tool is fully populated and the Department has policies and procedures in place and are fully operational, IT will continue to be a material weakness.

For the last 2 years, we found that the information system inventory counts were accurate. However, agencies did not populate the inventory with system interfaces as required by FISMA.[26]

We considered the system inventory to be accurate; however, proper annotation of all interfaces is an integral part of any inventory. Therefore, we are assigning inventory with an overall 81 to 95 percent completion percentage.

[25] A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. FISMA requires agencies to prepare POA&Ms for security weaknesses at the program and system levels.

[26] FISMA Section 3505(c) requires the head of each agency to develop and maintain an inventory of major information systems. Per FISMA, the identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. NIST Special Publication (SP) 800-53 control CA-3, requires that the organization must carefully consider the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks.

3.c. The IG generally agrees with the Chief Information Officer (CIO) on the number of agency-owned systems. Yes or No.

3.d. 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 or No.

3.e. The agency inventory is maintained and updated at least annually. Yes or No.

3.f. If agency IG does not evaluate the agency's inventory as 96-100 percent complete, please list by system name, Component/Bureau, and the Unique Project Identifier (if known); and indicate if the system is an agency or contractor system.

Component/Bureau	System Name	Exhibit 53 UPI (must be 23-digits)	Agency or Contractor system?
Number of known systems missing from inventory:			

As noted above, the inventory count and system listing is correct; however, system interfaces are not defined. There are no missing systems for question 3.f., just missing interfaces.

4. Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide POA&M process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided. (OIG's response is underlined.)

The Department must rely on the individual agencies to create POA&Ms for security weaknesses found, properly prioritize them, and follow through with corrective actions. The Department has concentrated this year on getting CSAM implemented and populated. The system is not yet fully populated and policies and procedures for Departmental oversight have yet to be determined or implemented.

The POA&M process continues to need improvement. Agencies are required to assess the severity of weaknesses and prioritize required corrective action. There are currently over 2,600 POA&Ms in the CSAM; we found 683 POA&Ms with a priority of "None" and 500 with a severity level of "Not Applicable." In addition, 101 were inappropriately recorded as "Exclude From OMB" and 50 were cancelled and recreated in order to extend due dates for corrective action.

We also found 265 vulnerabilities over 30 days old in which the agencies had not created POA&Ms as required by Departmental guidance.[27]

4.a. The POA&M is an agency-wide process, incorporating all known IT security weaknesses 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. (OIG's response is underlined below.) Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

As noted above, we found 265 vulnerabilities over 30 days old in which the agencies had not created POA&Ms as required by Departmental guidance.

4.b. When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s). (OIG's response is underlined below.) Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

As noted in our response to Question 4, it is the overall management of POA&Ms (prioritizing, determining the severity, timely recording, and completing corrective action) that needs improvement within the Department.

4.c. Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly). (OIG's response is underlined below.) Response Categories:

[27] Departmental Manual 3530-001, *Vulnerability Scan Procedures,* Appendix A, dated July 20, 2005.

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

As noted in our response to Question 4, it is the overall management of POA&Ms (prioritizing, determining the severity, timely recording, and completing corrective action) that needs improvement within the Department.

4.d. Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis. (OIG's response is underlined below.) Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

As noted in our response to Question 4, this year the Department has concentrated on implementing a new system that will provide improved oversight in the future. However, the policies and procedures for this oversight have not been developed and implemented because CSAM is a new tool that the Department is still in the process of implementing.

4.e. IG findings are incorporated into the POA&M process. (OIG's response is underlined below.)

Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

4.f. POA&M process prioritizes information technology (IT) security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources. (OIG's response is underlined below.)

Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

As noted in our response to Question 4, we found of the 848 open POA&Ms, 683 were recorded with a priority of "None," and 500 were recorded with a severity level of "Not Applicable."

5. IG Assessment of the Certification and Accreditation (C&A) Process

Agencies shall follow NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004 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*, dated February 2004 to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

The OCIO has worked diligently to raise the level of quality of the C&A documentation. The concurrency review process it has implemented is an important and necessary quality assurance step.[28] The process had been accurately annotating where the C&A documentation has not met required standards. But, agencies are responsible for the quality of the C&A documentation and following NIST guidance.[29] OCIO has given seminars on C&A best practices and lessons learned to agencies in an attempt to upgrade the quality of that submitted documentation. Unfortunately, it has not worked and agency submitted documentation continues to be lacking. This lack of quality submitted documentation has cost the OCIO much time and resources to review and comment on what it has received. It has slowed down the C&A process and created a backlog. This has impacted concurrency review process timeframes and quality. We found that agencies' C&A packages submitted generally did not meet NIST requirements.

5.a. The IG rates the overall quality of the agency's C&A process as:

Response Categories:

[28] The USDA concurrency review is a quality control process by OCIO to review the C&A documentation prior to approving an agency's Authority to Operate its IT systems.
[29] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* dated May 2004.

- **Excellent**
- **Good**
- **Satisfactory**
- **Poor**
- **Failing**

5.b. The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)

Security Plan	X
System impact level	X
System test and evaluation	X
Security control testing	X
Incident handling	X
Security awareness training	X
Configurations/patching	X
Other:	X

6-7. IG Assessment of Agency's Privacy Program and Privacy Impact Assessment (PIA) Process

6. Provide a qualitative assessment of the agency's PIA process, as discussed in Section D Question 5, including adherence to existing policy, guidance, and standards.

Assess the overall quality of the Department's PIA policies.

Response Categories:

- **Excellent**
- **Good**
- **Satisfactory**
- **Poor**
- **Failing**

The Department and OCIO made substantial improvements in the PIA process. This process requires agencies to perform analyses of how personal information is protected in their IT systems. We found that PIAs were documented for each system. Agencies appointed Privacy Officers and OCIO facilitates a monthly meeting to discuss privacy issues. In addition, privacy training was given to approximately 92 percent of USDA personnel during the fiscal year. However, we found that 8 of the 12 System of Records Notices (SORN) we reviewed were inaccurate or out-of-date. [30]

[30] A SORN is a statement providing to the public notice of the existence and character of a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

7. Provide a qualitative assessment of the agency's progress to date in implementing the provisions of OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

Response Categories:

- **Excellent**
- **Good**
- **Satisfactory**
- **Poor**
- **Failing**

OMB Memorandum M-07-16 is a complex document with many different requirements. There are four attachments that discuss topics on how to safeguard PII data. The four attachments and how the Department is handling each is discussed below.

Attachment 1-Safeguarding Against the Breach of PII

- Privacy Act Requirements - requires that agencies reduce the volume of PII within their systems, when possible. It also requires that agencies encrypt all mobile devices. This is discussed in Question 6 of this document.

- Security Requirements – requires that agencies implement controls over encryption, remote access, time-out, log-out functionalities, and adequate C&A documentation. This is discussed in Question 5 of this document.

OMB Memorandum No. M-07-16[31] requires that agencies reduce the volume of PII within their systems, when possible. It also requires that agencies encrypt all mobile devices (e.g., laptops). The Department has a plan for protecting PII, but had not yet fully implemented it. For example, of the approximate 54,000 laptops within the Department, we found that 4.23 percent had been fully encrypted.

Attachment 2-Incident Reporting and Handling Requirements

- This requirement discusses how PII incidents are being handled by the Department. This is answered in Question 9 of this document.

Attachment 3-External Breach Notification

- This requires that agencies develop a breach notification policy and plan. This is answered in Question 9 of this document.

[31] OMB Memorandum No. M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* dated May 22, 2007.

Attachment 4-Rules and Consequences

- This requirement addresses how managers, supervisors and employees are to be informed and trained regarding their respective responsibilities relative to safeguarding PII information and the consequences for violation of these responsibilities. This is answered in Question 10 of this document.

8. Configuration Management

8.a. Is there an agency-wide security configuration policy? Yes or No.

Departmentwide configuration policies and procedures are readily available for all systems on the OCIO website.

8.b. Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the NIST's website at http://checklists.nist.gov.

Departmental agencies were not always using the mandated NIST security configuration checklists when deploying hardware and software.[32] The checklists are tools that contain instructions and/or procedures for configuring an IT product to an operational environment to assist in implementing a baseline level of security. This occurred because agencies were not always aware that completing the checklist was a mandated requirement.

Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

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

8.c. Indicate which aspects of Federal Desktop Core Configurations (FDCC) have been implemented as of this report:

On March 27, 2007, OMB required the deployment of the Federal Desktop Core Configurations (FDCC). FDCC defines the minimum IT security requirements. For example, it includes procedures for managing password protection, installing patches, and performing vulnerability scans for systems that employ Windows XP and Windows Vista. The Department and its agencies were diligently testing settings and were in various stages of deployment. We noted that approximately 4.63 percent of the Department's laptops/desktops were fully compliant with FDCC.

In addition, the implementation of the required Federal Acquisition Regulation language pertaining to the FDCC has not been incorporated into USDA procurement documents.

8.c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. (OIG's response is underlined.) Yes or <u>No</u>.

8.c.2. New Federal Acquisition Regulation 2007-004 language, which modified "Part 39 – Acquisition of Information Technology," is included in all contracts related to common security settings. (OIG's response is underlined.) Yes or <u>No</u>.

8.c.3. All Windows XP and VISTA computing systems have implemented the FDCC security settings. (OIG's response is underlined.) Yes or <u>No</u>.

9. Incident Reporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.

USDA was not following documented policies and procedures for identifying and reporting incidents internally to OCIO and OIG and/or externally to law enforcement authorities and the U.S. Computer Emergency Readiness Team (US-CERT). These incidents may involve lost and/or stolen computers, unauthorized access to an agency's network, etc. This occurred because the system used by OCIO to track and manage incidents was manually intensive and/or members of the incident response team had not received adequate formal training. As a result, USDA cannot be assured that all incidents were identified, and/or that incidents were being properly investigated and corrected.

We found that 42 of 429 incidents were not reported to OIG. In addition, our review of 162 incidents over 15 days old disclosed that agencies had not created the required POA&Ms for 161 of these incidents. Depending upon the type of incident, this could result in an extended

period of time before the incident is corrected and potential malicious activity prevented. We also found instances where documentation supporting the closure of the incident needed improvement. For example, we found incidents that had been closed without any documentation supporting the closure.

9.a. The agency follows documented policies and procedures for identifying and reporting incidents internally. (OIG's response is underlined.) Yes or No.

9.b. The agency follows documented policies and procedures for external reporting to US-CERT. (http://www.us-cert/gov) (OIG's response is underlined.) Yes or No.

9.c. The agency follows documented policies and procedures for external reporting to law enforcement authorities. (OIG's response is underlined.) Yes or No.

10. Security Awareness Training

Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?

We found that the Department and its agencies continue to make progress in ensuring that all USDA employees are provided the Security Awareness and Privacy Act training. Approximately 92 percent of all USDA employees received the required training during fiscal year 2008. However, not all contractors appeared to be receiving the required training.

Response Categories:

- **Rarely, for example, approximately 0-50 percent of the time**
- **Sometimes, for example, approximately 51-70 percent of the time**
- **Frequently, for example, approximately 71-80 percent of the time**
- **Mostly, for example, approximately 81-95 percent of the time**
- **Almost Always, for example, approximately 96-100 percent of the time**

11. Collaborative Web Technologies and Peer-to-Peer File Sharing

We found that USDA was not adequately monitoring and prohibiting the downloading of peer to peer (P2P) software.[33] This occurred because OCIO believed P2P activity did not pose a significant threat compared to other types of incidents; and therefore, did not concentrate on this activity. As a result, USDA networks were vulnerable to damage that could be caused by malicious software, viruses, and worms imbedded within P2P files.

[33] P2P is a method of file sharing over a network in which individual computers are linked via the Internet or a private network to share programs/files, *often* illegally. Users download files directly from other users' computers rather than from a central server.

For example, we found that P2P reports were not distributed to agencies for almost 5 months of fiscal year 2008. Departmental policy requires that an incident be reported when P2P activity exceeds 75 hits per week to a single computer. We found 116 instances where P2P activity totaling more than 75 occurrences in 1 week was not declared an incident. In addition, agencies were not always reviewing the P2P reported activity.

Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? OIG's response is underlined.) Yes or No.

12. e-Authentication (e-Auth) Risk Assessments

12.a. Has the agency identified all e-Auth applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST SP 800-63, *Electronic Authentication Guidelines*? (OIG's response is underlined.) Yes or No.

12.b. If the response is "No," then please identify the systems in which the agency has not implemented the e-Auth guidance and indicate if the agency has a planned date of remediation.

NIST and OMB require that a risk assessment be performed prior to an agency connecting to an e-Authentication (e-Auth) system (a central authentication point for electronic Government systems) to determine the level of authentication needed.[34] A separate risk assessment is required to provide assurance that business transactions have the required level of verification for authentication. Authentication risks with potentially higher consequences require higher levels of assurance. For example, a low level of assurance would only require a user ID and password. A high level of assurance would require "in-person" methods approved by OCIO. USDA was not able to provide a complete and/or accurate listing of systems that used e-Auth. In most instances, the agencies in our sample told us they were unaware of any requirement to do an e-Auth risk assessment prior to connecting to the system. Starting in fiscal year 2009, OCIO stated that the e-Auth risk assessment will be included in the overall risk assessment.

[34] NIST SP 800-63, *Electronic Authentication Guideline*, dated April 2006; and OMB Memorandum No. 04-04, *E-Authentication Guidance for Federal Agencies,* dated December 2003.