U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Fiscal Year 2006 Federal Information Security Management Act Report

Report No. 50501-7-FM
September 2006

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 29, 2006

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

Subject: Fiscal Year 2006 Federal Information Security Management
Act Report (Audit Report No. 50501-7-FM)

Dear Director Portman:

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

Fiscal Year 2006 Federal Information Security Management Act Report (Audit Report No. 50501-7-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) in the past few years have heightened program management's awareness of the need to plan and implement effective information technology (IT) security. The National Information Technology Center, located in Kansas City, MO sustained its unqualified opinion on its general control structure. The Office of the Chief Financial Officer's National Finance Center, located in New Orleans, LA received its first unqualified opinion on its design of its general control structure. While its opinion on the effectiveness of its controls remained qualified, this was primarily attributed to the devastation caused by Hurricane Katrina. Although other agencies accelerated their efforts to comply with Federal information security requirements during the fiscal year, we continued to find significant weaknesses that can be attributed to a lack of management oversight and monitoring at both the Department and its agencies. While progress has been made, there is still much to be accomplished. An effective IT security program needs time to mature. Due to the significance of these weaknesses, the Department cannot be assured that its systems and data are adequately secured.

OCIO noted[1] that it is formulating a process for initiating, reviewing, and updating the Department's policies to provide guidance for improving compliance with Office of Management and Budget (OMB) requirements, National Institute of Standards and Technology (NIST) guidance, and Departmental Regulations (DR). OCIO reported that it is performing a gap analysis to prioritize required policy work and developing a program to review and update existing policies. In addition, OCIO has implemented a security review program to evaluate the accuracy of information provided by the agencies to improve the effectiveness of their security programs. However, until these controls are in place, operating, and effectively established, IT management and security remain a material internal control weakness for the Department.

This report constitutes the independent evaluation required of OIG of the Department's IT security program and practices by the Federal Information Security Management Act (FISMA).

The following summarizes the weaknesses discussed in exhibit A of this report, in which we respond to OMB's questions as required by OMB

[1] Chapters 4 and 5 of the OCIO FISMA report detail where improvements are underway and/or planned for correcting the material weaknesses within the Department.

Memorandum No. M-06-20, "Fiscal Year 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."

- During fiscal year 2006, OCIO implemented an annual Departmentwide IT system inventory requirement. However, we were unable to reach a conclusion on the accuracy/completeness of the inventory because OCIO relied on the agencies to report system inventory without validating the information reported. OCIO was unable to verify the accuracy and/or reliability of those agency-provided inventories. Our review of the inventory disclosed that the total number of systems declined from 460 in fiscal year 2005 to 260 in fiscal year 2006. The vast majority of this decline was due to a consolidation of systems at one agency. The agency went from 189 systems to 15, and most of the consolidation was done based on geographical location, rather than system characteristics.

- The consolidation of systems, discussed above, resulted in the inadequate oversight of the Department's Privacy Act implementation. We noted that it was difficult to determine which systems had the documentation required to comply with the law. We reviewed 13 privacy impact assessments and found that 6 did not answer one or more of the questions adequately and another was not in the required format. We also found that two of the Statement of Record Notices, required by law, were not published in the Federal Register.

- Agencies had not followed NIST guidance when preparing security plans, risk assessments, and disaster recovery plans. During fiscal year 2006, the Department acknowledged that certification and accreditation (C&A) documentation submitted prior to October 1, 2005, was inadequate and instituted a concurrency review process where second party approval was required prior to recommending agency accreditation. We found this process needed enhancements. We concluded that the three concurrency reviews we examined should not have resulted in approval for agency accreditation. For example, two of the reviews were performed on C&A documentation associated with the legacy systems that were being replaced.

- The Department reported the level of C&A compliance in its quarterly reports to OMB. However, we noted that eight systems had only obtained a conditional approval to operate. OMB policy states that an information system should not be accredited during a period of limited authorization to operate.[2]

[2] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 28, 2000.

- Department oversight over contingency planning and testing information needed improvement. We reviewed the Department's system for storing contingency and disaster recovery plans and found some systems were not included and others were missing critical information. We examined a sample of five test plans and found that they lacked specific success criteria, detailed schedules, scenarios and notification procedures, and/or internal or external connectivity.

- The Department implemented a new system to track plan of actions and milestones (POA&M) during fiscal year 2006. While this was a marked improvement over the legacy reporting system, numerous problems were encountered during implementation. Specifically we found that known IT weaknesses were not reported, not all weaknesses were tracked, conflicting information was reported, and agencies did not ensure that corrective actions were taken before closing out the weaknesses. In addition, the information contained in the system was not being used to report to OMB. One agency reported no weaknesses in the quarterly OMB submission, even though the system included 35 open weaknesses and its yearly internal self assessment reported 349 weaknesses.

- We noted that improvements were needed in the Department's reporting of system risk categories. For example, we found that two general support systems were rated as moderate risk even though those systems processed data from 18 high risk applications. In another example, a system that stored information on biological agents and toxins was rated as moderate risk.

- Annual risk assessments within the Department did not include an assessment of actual controls within the systems. One agency reported that change management was fully implemented, yet our audit disclosed that its policies and procedures were ineffective. In another assessment the agency listed 93 controls as not applicable, because the hosting agency was responsible for them. Our audit disclosed that some of the controls did belong to the agency and should have been assessed. During our fiscal year 2006 review, we determined that the OCIO had changed the level where a functional area is rated deficient and therefore needs a POA&M. Through fiscal year 2005, deficiency was defined as a functional area rated at level 3 (procedures and controls are implemented) or less. For fiscal year 2006, that level had changed to 2 (documented procedures and controls) or less. This change required agencies to report and remediate fewer weaknesses. OCIO was unable to provide an explanation to support this change in reporting weaknesses from agency self-assessments.

- The Department implemented a security review program to periodically evaluate the accuracy of information provided by the agencies and provide effective oversight of agency security programs. However, we found that this program needed improvements. We noted that in the 8 reviews performed during fiscal year 2006, there were 123 weaknesses identified by OCIO. Of those, only 52 were addressed in the agency POA&Ms. This occurred because the Department did not always follow-up on the findings to ensure the agencies were accurately mitigating weaknesses. In addition, the reviews could be enhanced by including checklists to help ensure consistency.

- We found that USDA's Information Security Status (scorecard) did not always contain accurate information. We found that agencies were not properly reporting the status of their programs in the monthly or quarterly updates to OMB. As noted in this report, we found inaccurate reporting by the agencies in every category except security awareness training.

- We completed four stand-alone IT security audits that fed into our FISMA consolidation. We also ensured that the IT security audit coverage for our fiscal year 2006 financial statement audits was completed in time to be consolidated into our FISMA report. We noted that configuration management within the Department was not always effective. Although most agencies had policies and procedures, we found that they were not always followed. We found that controls were not always implemented to help ensure that system software changes were properly authorized, documented, tested, and monitored.

- We noted that the Department's vulnerability scanning and patch management program needed improved oversight. We found that the number of devices that needed scanning varied significantly on a monthly basis. In addition, at one agency, we found that 6,270 devices needed scanning and 10,505 devices needed patches.[3] We also noted unmitigated vulnerabilities that were not reported as weaknesses on agency POA&Ms. The OCIO did not review agency scan and patch certificates for accuracy or viability.

- We noted that incident reporting within the Department needed improvement. We found that incidents were not always tracked, reported to appropriate authorities, and/or closed timely. For example, our review of incidents reported through July 15, 2006, disclosed that (1) incidents were not always closed within 30 days, (2) incidents were missing from the tracking spreadsheet, (3) incidents were not always reported to appropriate authorities, and (4) false positives documentation was deleted and not further tracked, even though some were ultimately found to be actual incidents. In addition, we found that an incident tracking database

[3] Scanning should be performed on all devices on the network, while patching is done only as new vulnerabilities are found and vendors mitigate them. The number of devices patched should not significantly outnumber the total number of devices scanned.

had not been implemented, even though we had initially recommended that this weakness be remediated during fiscal year 2002 and the Department agreed to do so.

- We noted that the Department needed an internet protocol (IP) address inventory system. We have reported since fiscal year 2001 that the Department needed an IP address tracking system and the Department agreed to do so.

Due to the significance of these issues, information technology (IT) security remains a material internal control weakness for the Department.

Recommendation In Brief

This report presents the results of our audit work in assessing the security over the Department's IT resources. The recommendations we made to correct the deficiencies identified in this evaluation have been documented in other agency reports and we are not making additional recommendations in this report.[4]

[4] See exhibit B for a listing of those reports.

Abbreviations Used in This Report

APHIS	Animal and Plant Health Inspection Service
C&A	certification and accreditation
CCC	Commodity Credit Corporation
CIO	Chief Information Officer
DA	Departmental Administration
DM	Departmental Manual
FCIC	Federal Crop Insurance Corporation
FIPS	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FNCS	Food, Nutrition, and Consumer Services
FSA	Farm Service Agency
FS	Forest Service
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
IG	Inspector General
IP	internet protocol
IT	Information Technology
ITS	Information Technology Services
NFC	National Finance Center
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
OMB	Office of Management and Budget
OIG	Office of Inspector General
POA&M	plan of actions and milestones
RMA	Risk Management Agency
RD	Rural Development
SP	Special Publication
TSO	Telecommunication Services Operations
US-CERT	United States Computer Emergencies Readiness Team
USDA	U.S. Department of Agriculture
UTN	Universal Telecommunications Network

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 and establishing 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 their information security programs.

Each agency must establish an agency-wide risk-based information security program to be overseen by the agency CIO and 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 appropriate laws and regulations;
- evaluating OCIO's progress in establishing a Departmentwide security program; and

- evaluating the agencies' and OCIO's plan of actions and milestones consolidation and reporting process.

Scope and Methodology

The scope of our review was Departmentwide and agency audits relating to information technology (IT) completed during fiscal year 2006. We conducted this audit in accordance with *Government Auditing Standards*.

Fieldwork for this audit was performed at the Department OCIO from July to September 2006. 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 2006 audit work covered 10 agencies and staff offices: Animal and Plant Health Inspection Service (APHIS), Food, Nutrition, and Consumer Services (FNCS), Forest Service (FS), Farm Service Agency (FSA) (includes Commodity Credit Corporation (CCC)), Natural Resources Conservation Service (NRCS), Office of the Chief Financial Officer (OCFO), OCIO (includes Information Technology Services (ITS) and National Information Technology Center (NITC) Telecommunication Services Operations (TSO)), Rural Development (RD), Risk Management Agency (RMA) (includes Federal Crop Insurance Corporation (FCIC)), and Departmental Administration (DA). These agencies and staff offices operate approximately 172 of the OCIO estimated 260 general support and major application systems within the Department.[5]

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

- Consolidated the results and issues from our prior IT security audit work. Our audit work consisted primarily of audit procedures found in the U.S. Government Accountability Office (GAO) Financial Information System Control Audit Manual;

- evaluated OCIO's progress in implementing recommendations to correct material weaknesses identified in prior Office of Inspector General and GAO audit reports; and

- gathered the necessary information to address the specific reporting requirements outlined in Office of Management and Budget's Memorandum No. M-06-20, dated July 17, 2006.

[5] The Department identified 260 systems in its plan of actions and milestones system as of July 2006. The data were input by the agencies and had not been verified or audited. Based on independent auditor review of this data and inappropriate consolidation of systems, we question the accuracy and reliability of the total number of systems reported.

Section C: Inspector General (IG) Questions

1. **As required in Federal Information Security Management Act (FISMA), the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By Federal Information Processing Standards (FIPS) Publication 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).**

   To meet the requirement for conducting a National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26 review, agencies can (1) continue to use NIST SP 800-26, or (2) conduct a self-assessment against the controls found in NIST SP 800-53.

   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.

   The U.S. Department of Agriculture (USDA) has approximately 26 agency and staff offices that OCIO estimate operate about 260 information systems.[6] We conducted reviews at 10 agencies that operated an estimated 172 systems. We reviewed 45 of the 172 systems.[7] One of the systems selected for review was a contractor operated system. We used FIPS Publication 199[8] risk impact levels for these systems as reported by OCIO. During our review of the Department's system categorization efforts, we determined that system risk ratings based on confidentiality, integrity, and availability of the data residing on the system were inconsistent with FIPS requirements and agencies did not ensure that the risk ratings they assigned remained consistent throughout all of the system documentation. Without a proper risk level assignment, agencies cannot design adequate risk-based security programs to ensure appropriate security controls are in place to protect confidentiality, integrity, and availability of their information systems.

[6] The Department identified 260 systems in the Automated Security Self-Evaluation and Remediation Tracking (ASSERT) tool as of July 2006. Office of the Chief Information Officer's (OCIO) data are agency-supplied and have not been verified or audited. In fiscal year 2005, OCIO reported 460 systems. Based on independent auditor verification we found one agency inventory count that went from 189 systems in fiscal year 2005 to 15 in fiscal year 2006. Nine of the 15 systems reported in fiscal year 2006 were consolidated based on geographic region. In addition, an adequate reconciliation was not completed for systems reported from fiscal year 2005 to systems reported in fiscal year 2006. A comparison of the 2 years revealed 26 systems missing from the reconciliation records.

[7] The depth and breadth of our reviews varied by audit.

[8] FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," dated December 2003.

To the extent that agencies use the Department's centralized data centers, our reviews help ensure that those centers take the necessary actions to meet the requirements of FISMA, OMB, and NIST guidelines. Agencies primarily use Office of Inspector General (OIG) audits to identify weaknesses in their management and oversight of contractors.

USDA used the ASSERT tool to perform self-assessments based on NIST SP 800-26.[9] Our review of agency self-assessments showed that controls were assessed at incorrect levels and some controls were not reported at all. In addition, because self-assessments were not complete by the time we finished our audit work and because they were not scheduled to be reviewed and signed-off by agency personnel until September 29, 2006, we were unable to ensure the self-assessments were accurately reporting the status of controls within agency systems. Additionally, during our fiscal year 2006 review, OCIO had changed the level where a functional area is rated deficient and therefore needs a plan of action and milestone (POA&M). Through fiscal year 2005, deficiency was defined as a functional area rated at level 3 (procedures and controls are implemented) or less. For fiscal year 2006, that level had changed to 2 (documented procedures and controls) or less. This change requires agencies to report and remediate fewer weaknesses. OCIO was unable to provide an explanation to support this change in reporting weaknesses from agency self-assessments.

Based on the OIG reviews performed throughout fiscal year 2006, we continued to find that not all agencies have followed NIST guidance when preparing security plans, risk assessments, and disaster recovery plans.

[9] NIST SP 800-26, "Security Self-Assessment Guide for Information Technology Systems," dated November 2001.

2. For each part of this question, identify actual performance in fiscal year 2006 by risk impact level and bureau, in the format provided. From the representative subset of systems evaluated, identify the number of systems which have completed the following; have a current certification and accreditation (C&A), a contingency plan tested within the past year, and security controls tested within the past year.

Bureau Name (OIG Reviewed)	FIPS Risk Impact Level	Question 1.						Question 2. – Agency Reported					
		1.a. Fiscal year 2006 Agency Systems		1.b. Fiscal year 2006 Contractor Systems		1.c. Fiscal year 2006 Total Number of Systems		2.a[10] Number of systems certified and accredited As of 7/31/06		2.b.[11] Number of systems for which security controls have been tested and evaluated in the last year. As of 7/31/06		2.c.[12] Number of systems for which contingency plans have been tested in accordance with policy and guidance As of 7/31/06	
		Total #	# Rev.	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
1. APHIS	High	8	1	0	0	8	1	6	75%	7	88%	4	50%
	Moderate	9	0	0	0	9	0	7	78%	6	67%	2	22%
	Low	3	0	0	0	3	0	0	0%	0	0%	0	0%
	Not Categorized	24	0	0	0	24	0	0	0%	0	0%	0	0%
	Sub-total	44	1	0	0	44	1	13	30%	13	30%	6	14%
2. DA	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	7	1	0	0	7	1	0	0%	0	0%	0	0%
	Sub-total	7	1	0	0	7	1	0	0%	0	0%	0	0%
3. RMA	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
(Includes FCIC)	Moderate	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	7	6	0	0	7	6	0	0%	0	0%	0	0%
	Sub-total	7	6	0	0	7	6	0	0%	0	0%	0	0%
4. FSA (includes CCC)	High	18	6	0	0	18	6	18	100%	17	94%	17	94%
	Moderate	2	0	0	0	2	0	2	100%	2	100%	2	100%
	Low	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	21	6	0	0	21	6	21	100%	20	95%	20	95%

[10] OIG cannot determine an accurate number of systems that have an adequate C&A. The OCIO had stated that C&As prior to October 1, 2005 were not adequate and would be corrected during the next review cycle. Our audits during fiscal year 2006 determined that C&As are still inadequate and therefore we cannot attest to the accuracy of any number in this column.

[11] OIG cannot determine an accurate number of systems that have self-assessments completed. We found that the agencies were not correctly reporting weaknesses and the system is not updated (it is not even required to be updated until September 29, 2006).

[12] The Department uses the Living Disaster Recovery Planning System (LDRPS) as a central repository to store information on contingency plans and disaster recovery plans. Our review of that system found that not all plans were stored in LDRPS and that information was inconsistent and did not meet NIST guidance. Therefore, we cannot attest to the accuracy of any number in this column.

Bureau Name (OIG Reviewed)	FIPS Risk Impact Level	Question 1.						Question 2. – Agency Reported					
		1.a. Fiscal Year 2006 Agency Systems		1.b. Fiscal Year 2006 Contractor Systems		1.c. Fiscal Year 2006 Total Number of Systems		2.a[13] Number of systems certified and accredited As of 7/31/06		2.b.[14] Number of systems for which security controls have been tested and evaluated in the last year. As of 7/31/06		2.c.[15] Number of systems for which contingency plans have been tested in accordance with policy and guidance As of 7/31/06	
		Total #	# Rev.	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
5. FS	High	6	0	0	0	6	0	0	0%	0	0%	0	0%
	Moderate	8	5	0	0	8	5	0	0%	0	0%	0	0%
	Low	2	0	0	0	2	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	16	5	0	0	16	5	0	0%	0	0%	0	0%
6. FNS	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	7	1	3	1	10	2	9	90%	10	100%	10	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	1	0	0	0	1	0	0	0%	0	0%	0	0%
	Sub-total	8	1	3	1	11	2	9	82%	10	91%	10	91%
7. RD	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	11	1	0	0	11	1	11	100%	11	100%	11	100%
	Low	3	0	0	0	3	0	0	0%	0	0%	0	0%
	Not Categorized	9	0	0	0	9	0	0	0%	0	0%	0	0%
	Sub-total	23	1	0	0	23	1	11	48%	11	48%	11	48%
8.OCFO - NFC	High	5	5	0	0	5	5	4	80%	4	80%	4	80%
	Moderate	6	4	0	0	6	4	6	100%	6	100%	6	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	3	0	0	0	3	0	0	0%	0	0%	0	0%
	Sub-total	14	9	0	0	14	9	10	71%	10	71%	10	71%
9. OCIO (includes ITS, NITC, and TSO)	High	8	5	0	0	8	5	5	63%	5	63%	5	63%
	Moderate	11	7	0	0	11	7	11	100%	10	91%	11	100%
	Low	6	1	0	0	6	1	6	100%	6	100%	6	100%
	Not Categorized	1	0	0	0	1	0	0	0%	0	0%	0	0%
	Sub-total	26	13	0	0	26	13	22	85%	21	81%	22	85%

[13] OIG cannot determine an accurate number of systems that have an adequate C&A. The OCIO had stated that C&As prior to October 1, 2005 were not adequate and would be corrected during the next review cycle. Our audits during fiscal year 2006 determined that C&As are still inadequate and therefore we cannot attest to the accuracy of any number in this column.

[14] OIG cannot determine an accurate number of systems that have self-assessments completed. We found that the agencies were not correctly reporting weaknesses and the system is not updated (it is not even required to be updated until September 29, 2006).

[15] The Department uses the Living Disaster Recovery Planning System (LDRPS) as a central repository to store information on contingency plans and disaster recovery plans. Our review of that system found that not all plans were stored in LDRPS and that information was inconsistent and did not meet NIST guidance. Therefore, we cannot attest to the accuracy of any number in this column.

Exhibit A – OMB Reporting Requirements and USDA OIG Position

		Question 1.						**Question 2. – Agency Reported**					
Bureau Name (OIG Reviewed)	**FIPS Risk Impact Level**	**1.a. Fiscal Year 2006 Agency Systems**		**1.b. Fiscal Year 2006 Contractor Systems**		**1.c. Fiscal Year 2006 Total Number of Systems**		**2.a[16] Number of systems certified and accredited As of 7/31/06**		**2.b.[17] Number of systems for which security controls have been tested and evaluated in the last year. As of 7/31/06**		**2.c.[18] Number of systems for which contingency plans have been tested in accordance with policy and guidance As of 7/31/06**	
		Total #	**# Rev.**	**Total #**	**# Rev**	**Total #**	**# Rev**	**Total #**	**Percent of Total**	**Total #**	**Percent of Total**	**Total #**	**Percent of Total**
10. NRCS	High	1	0	0	0	1	0	0	0%	0	0%	0	0%
	Moderate	2	1	0	0	2	1	0	0%	0	0%	0	0%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	3	1	0	0	3	1	0	0%	0	0%	0	0%
USDA Totals	High	**46**	**17**	**0**	**0**	**46**	**17**	**33**	**72%**	**33**	**72%**	**30**	**65%**
	Moderate	**56**	**19**	**3**	**1**	**59**	**20**	**46**	**78%**	**45**	**76%**	**42**	**71%**
	Low	**15**	**1**	**0**	**0**	**15**	**1**	**7**	**47%**	**7**	**47%**	**7**	**47%**
	Not Categorized	**52**	**7**	**0**	**0**	**52**	**7**	**0**	**0%**	**0**	**0%**	**0**	**0%**
	Total	**169**	**44**	**3**	**1**	**172**	**45**	**86**	**50%**	**85**	**49%**	**79**	**46%**

[16] OIG cannot determine an accurate number of systems that have an adequate C&A. The OCIO had stated that C&As prior to October 1, 2005 were not adequate and would be corrected during the next review cycle. Our audits during fiscal year 2006 determined that C&As are still inadequate and therefore we cannot attest to the accuracy of any number in this column.

[17] OIG cannot determine an accurate number of systems that have self-assessments completed. We found that the agencies were not correctly reporting weaknesses and the system is not updated (it is not even required to be updated until September 29, 2006).

[18] The Department uses the Living Disaster Recovery Planning System (LDRPS) as a central repository to store information on contingency plans and disaster recovery plans. Our review of that system found that not all plans were stored in LDRPS and that information was inconsistent and did not meet NIST guidance. Therefore, we cannot attest to the accuracy of any number in this column.

3. **In the format below, evaluate the agency's oversight of contractor systems and agency system inventory.**

   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, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST SP 800-26 and/or NIST SP 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:[19]**

   - **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. USDA employs contractors in many aspects of its system operations. Contractors are used for network administration, system development, and as system administrators. In conducting our agency reviews, testing of contractor operations had been limited to access controls, security clearances, security awareness training, and oversight by the agencies of contractor activities. Based on our reviews at 10 agencies, we found only limited evidence that the agencies had adequately employed methods to ensure that contractor provided services met the requirements of FISMA, OMB, and NIST guidelines. For example, we found inadequate oversight of both the contract and contractors in one audit of a major implementation of the nation-wide Universal Telecommunication Network (UTN).[20] We found that the agency had not conducted required failover testing, security control testing, and C&A of the UTN network before implementation. The agency did not have controls in place to ensure adequate contractor testing of the network prior to implementation.

[19] Based on consolidation of systems and an unreliable reconciliation we could not determine an accurate systems inventory. We cannot give a percentage with any degree of accuracy.

[20] Audit Report No. 88501-6-FM, "Management and Security over the USDA Universal Telecommunication Network," dated August 2006.

b.1 The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such 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:

- **Approximately 0-50 percent complete**
- **Approximately 51-70 percent complete**
- **Approximately 71-80 percent complete**
- **Approximately 81-95 percent complete**
- **Approximately 96-100 percent complete**

We could not report a percentage with any degree of accuracy. Based on our reviews, we have documented evidence that the Department did not have a reliable inventory of applications and general support systems from which to manage Departmentwide IT security. The Department relied on agencies to provide a comprehensive list; however, OCIO was unable to verify the accuracy or reliability of those agency-provided inventories due to limited resources. OIG was not involved in the development and verification of agencies' information technology (IT) system inventories and their interfacing systems and networks. Our review of the Department's inventory system showed the total number of systems declined from 460 in fiscal year 2005 to only 260[21] in fiscal year 2006. The vast majority of this decline was a consolidation of systems in one agency. That agency went from 189 systems to 15. Most of the consolidation was done by geographical areas of the country. The Department also did not attempt to reconcile fiscal year 2005 inventory numbers to fiscal year 2006. During our review we found 26 systems were missing between the 2 years and the OCIO had to request additional information from the agencies to determine the cause. While we agree that OCIO's current list of major applications provides a good starting point, OCIO needs to be fully aware of all applications and general support systems that reside on the Department's network to ensure that agencies are in compliance with OMB and FISMA requirements, and to effectively manage the Department's security program.

In another audit we found that an agency consolidated seven systems involving more than 50 business applications that supported their core mission.[22] These applications were in mixed stages of the system development life cycle and used different technologies, including mixed program specific applications alongside administrative applications (i.e., time and attendance).

[21] This is an estimate of the number of systems based on agencies reporting to OCIO. OCIO did not validate this number. Therefore, we could not attest to its accuracy.

[22] Audit Report No. 10501-5-FM, "NRCS Application Controls-Program Contracts System (ProTracts)," dated July 2006.

Furthermore, the consolidation of systems led to inadequate oversight of the Department's Privacy Act implementation. We found, because of the system consolidation going on within the Department, that it was difficult to determine which systems had the required documentation and had complied with the law. We reviewed 13 privacy impact assessments and found that 6 did not answer one or more of the questions adequately and another one was not in the required format. We also found that 2 of the Statement of Record Notices required by law, were not published in the Federal Register.

b2. If the agency IG does not evaluate the agency's inventory as 96-100 percent complete, please list the systems that are missing from the inventory.

As reflected in our response to 3.b.1, during our review we found 26 systems missing from the inventory. The OCIO was researching these systems to determine whether they were retired or it was an error. We cannot be assured that these were actually missing. We did not audit the entire inventory listing and could not determine if the listing was accurate or there were other systems missing.

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

As reflected in our response to question 3.b., we did not generally agree with the number of agency owned systems.

d. The OIG 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.

We do not generally agree. As stated in our response to question 3.a. above, the number of systems within the Department (both Department and contractor administered) can not be relied upon until OCIO validates the number of systems within the Department and establishes controls to maintain an accurate inventory.

e. The agency inventory is maintained and updated at least annually. (OIG's response is underlined.) Yes or No.

During fiscal year 2006, OCIO implemented an annual inventory requirement. However, we question the accuracy of the system inventory because, as mentioned in response to question 3.a., OCIO relied on the agencies to report system inventory. Further, OCIO was unable to verify the accuracy or reliability of those agency-provided inventories.

f. **The agency has completed system e-Authentication risk assessments. (OIG's response is underlined.) Yes or No.**

During fiscal year 2006, OCIO performed a security review of e-authentication and found the same issues we had reported in our fiscal year 2005 FISMA report. Specifically:

- New interfaces and updated system security architecture were not in the current documentation;
- the security plan had not been updated in 2 years, although changes to the system had been made; and
- documented processes did not exist for contractor account removal, incident responses, and responsible individuals had not been trained.

4. **Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide POA&M process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. (OIG's response is underlined.)**[23]

For items 4a.-4.f, the response categories are as follows:

- **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**

[23] OIG cannot determine an accurate number of systems that have self-assessments completed, which is the first part of the POA&M process. We found that the agencies were not correctly reporting weaknesses and the system was not updated (it is not required to be updated until September 29, 2006). Therefore, we cannot provide an accurate percentage.

The Department implemented a new system to track plan of actions and milestones (POA&M) during fiscal year 2006. While there was a marked improvement over the legacy reporting system, numerous problems were encountered during implementation. Specifically, we found that known IT weaknesses were not reported, not all weaknesses were tracked, conflicting information was reported, and agencies did not ensure that corrective actions were taken before closing out the weaknesses. In addition, the information contained in the system was not being used to report to OMB. One agency reported no weaknesses in the quarterly OMB submission, even though the system included 35 open weaknesses and its yearly internal self assessment reported 349 weaknesses.

Also, the Department was incorrectly reporting risk categories that are not in accordance with FIPS Publication 199.[24] For example, we found two general support systems rated as moderate, even though there were 18 high risk systems that store or transmit data over the network. In another example, a system which stores information on biological agents and toxins was rated moderate.

In addition, annual risk assessments within the Department were not reporting actual controls within the systems. One agency reported that change management was fully implemented, yet our audit disclosed that its policies and procedures were ineffective. In another assessment the agency listed 93 controls as not applicable because the hosting agency was responsible for them. Our audit disclosed that the controls did belong to the agency and should have been assessed. Finally, during our fiscal year 2006 review, we determined that the OCIO had changed the level where a functional area is rated deficient and therefore needs a POA&M. Through fiscal year 2005, deficiency was defined as a functional area rated at level 3 (procedures and controls are implemented) or less. For fiscal year 2006, that level had changed to 2 (documented procedures and controls) or less. This change required agencies to report and remediate fewer weaknesses. OCIO was unable to provide an explanation to support this change in reporting weaknesses from agency self-assessments.

Finally, the Department had implemented a security review program to periodically evaluate the accuracy of information provided by the agencies and provide effective oversight of agency security programs. However, we found this program needed improvement. We found that in the 8 reviews performed, there were 123 weaknesses identified by the OCIO. Of those, only 52 were identified in the agencies' POA&Ms. This occurred because the Department did not followup on findings to ensure the agencies were mitigating the weaknesses. In addition, the reviews did not use checklists for consistent reporting nor did they keep documented records of findings.

[24] FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," dated December 2003.

We found that reporting of the USDA's Information Security Status (scorecard) needed improvement. Agencies were not properly reporting the status of their programs in the monthly or quarterly updates to OMB. As noted in this report, we found inaccurate reporting by the agencies in every category except security awareness training.

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.) 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**

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**

c. Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress. (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**

d. 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**

e. OIG 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**

f. POA&M process prioritizes 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**

Based on our analysis of previous audit findings and the POA&Ms, we continued to find that agencies were experiencing logical access control weaknesses, because policies and procedures were not in place to (1) timely remove user accounts when no longer needed, (2) periodically reconcile user accounts to current employees and contractors, and (3) assign users only those permissions needed to perform their job responsibilities. In addition, agencies had inadequate controls over the following:

- Physical access to computer systems and critical network components,
- network resource scans,
- risk assessments,

- contingency plans,
- contingency plan testing,
- patch management,
- system documentation and change management,
- system development life cycle procedures,
- memorandums of understanding or service level agreements with interconnecting systems, and
- oversight of partnering organizations.

5. **OIG Assessment of the C&A process. OMB is requesting IGs to provide a qualitative assessment of the agency's C&A process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST 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 Publication 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Response Categories:[25]**

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

   Agencies have not followed NIST guidance when preparing security plans, risk assessments, and disaster recovery plans. Also, the Department had acknowledged that C&A documentation submitted prior to October 1, 2005 was inadequate and instituted a concurrency review where second party approval was required prior to accreditation. We found this process was inadequate in all three concurrency reviews we examined and that those systems should not have been accredited.

   Also, the Department did not always accurately report compliance with C&A requirements in the quarterly report to OMB. We found that eight systems were included in the quarterly count that had only obtained a conditional approval to operate. This is contrary to OMB policy, which states that an information system is not to be accredited during the period of limited authorization to operate.[26]

[25] OIG cannot determine an accurate number of systems that have an adequate C&A. The OCIO had stated that C&As prior to October 1, 2005 were not adequate and would be corrected during the next review cycle. Our audits during fiscal year 2006 determined that C&As were still inadequate, therefore we cannot attest to the accuracy of any number because we consider the process to be flawed. Therefore, we cannot provide an accurate percentage.

[26] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 28, 2000.

Finally, the Department's oversight of contingency planning and testing information was inadequate. We reviewed the Department's system for storing contingency and disaster recovery plans and found some were missing completely while others were missing critical information. We examined a sample of five test plans and found that they lacked specific success criteria, detailed schedules, scenarios and notification procedures and/or internal and external connectivity.

6. Configuration Management.

a. Is there an agencywide security configuration policy? (OIG's response is underlined.) Yes or <u>No</u>.

The Departmentwide security configuration policy needed to be updated. The Department does not have updated configuration guides available for all of the products listed in the table below.

We determined that the configuration policy needs to be revised to include security policies for Windows 2003 Server, Cisco Router Internetwork Operating System, and Oracle software. We determined that OCIO provided the agencies with security assessment guidelines for the Windows XP Professional, Windows NT, Windows 2000 Professional, Windows 2000 Server, Solaris, HP-UX, and Linux operating systems.[27] In addition, the Department had similar security assessment guidelines for mainframe, classified systems, personal electronic devices, telecommunications, Web farms, and AS400s. Security guidelines are also in force for wireless devices, laptops, physical security, privacy of systems, classified systems, and information systems security.

Despite the guidance we found that configuration management within the Department was ineffective. We completed four stand-alone IT security audits that fed into our FISMA consolidation. We also ensured that the IT security audit coverage for our fiscal year 2006 financial statement audits was completed in time to be consolidated into our FISMA report. We found that agencies' change management practices were ineffective. Although most had polices and procedures, we found that they were not being followed. We found that controls did not exist to ensure that system software changes were properly authorized, documented, tested, and monitored.

[27] DM 3540-002, "Risk Assessment and Security Checklists," Chapter 8, Part 2, August 19, 2004.

We noted that the Department's vulnerability scanning and patch management program needed improved oversight. We found that the number of devices that needed scanning significantly varied on a monthly basis. In addition, at one agency, we found that 6,270 devices needed scanning and 10,505 devices needed patches.[28] We also noted unmitigated vulnerabilities that were not reported as weaknesses on agency POA&Ms. The OCIO did not review the scan and patch certificates for accuracy or viability.

Also, agencies were required to submit POA&Ms for vulnerabilities unmitigated within 30 days. Our review of the POA&Ms dated July 28, 2006 showed only one agency had actually reported a weakness related to scanning vulnerabilities. Finally, OCIO was unable to provide documentation that all agencies had submitted certificates for the month of April 2006. Of the 26 agencies, OCIO was able to provide only 18 submitted scanning certificates.

b. Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software. (OIG's response is underlined.) Yes or <u>No</u>.

	Product	**Addressed in agencywide policy? Yes, No, or N/A.**	**Do any agency systems run this software? Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.**
1	Window XP Professional	**Yes**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
2	Windows NT	**Yes**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
3	Windows 2000 Professional	**Yes**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
4	Windows 2000 Server	**Yes**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
5	Windows 2003 Server	**No**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
6	Solaris	**No**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
7	HP-UX	**No**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
8	Linux	**No**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
9	Cisco Router IOS	**No**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
10	Oracle	**No**	**Yes**	**Rarely, or, on approximately 0-50 percent of the systems running this software**
11	Other (see narrative)	**N/A**	**N/A**	**Rarely, or, on approximately 0-50 percent of the systems running this software**

[28] Scanning should be performed on all devices on the network, while patching is done only as new vulnerabilities are found and vendors mitigate them. The number of devices patched should not significantly outnumber the total number of devices scanned.

Exhibit A – OMB Reporting Requirements and USDA OIG Position

7. **Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.**

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

   We noted that incident reporting within the Department needed improvement. We found that incidents were not always tracked, reported to appropriate authorities, and/or closed timely. For example, our review of incidents reported through July 15, 2006, disclosed that (1) incidents were not always closed within 30 days, (2) incidents were missing from the tracking spreadsheet, (3) incidents were not always reported to appropriate authorities, and (4) false positives documentation was deleted and not further tracked, even though some were found to be actual incidents. In addition, we found that an incident tracking database had not been implemented, even though we had initially recommended that this weakness be remediated during fiscal year 2002 and the Department agreed to do so.

   Finally, the Department needed an internet protocol (IP) address inventory system. We have reported since fiscal year 2001 that the Department needs an IP address tracking system, and yet it is still not in production. The Department had a contract to develop the database, but it was not yet operational.

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

   During our review we found that OCIO was not informing law enforcement of incidents for a significant portion of the year. OCIO informed us that it did not know that it was a requirement.

   c. **The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov. (OIG's response is underlined.) Yes or No**.

   We found that OCIO was not reporting all incidents to US-CERT. During our review we found that 18 incidents were not reported to US-CERT. We were informed that these were false positives. When we requested documentation on 6 of these proving that they were, in fact, false positives, OCIO was unable to provide any documents. When they requested additional information from the agencies, it was determined that 2 of these were not false positives and should have been forwarded to US-CERT. The OCIO agreed to research the remaining 12 to determine whether they should have been reported.

8. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? (OIG's response is underlined below.) Response Choices include:

- **Rarely, or, approximately 0-50 percent of employees have sufficient training**
- **Sometimes, or approximately 51-70 percent of employees have sufficient training**
- **Frequently, or approximately 71-80 percent of employees have sufficient training**
- **Mostly, or approximately 81-95 percent of employees have sufficient training**
- **Almost Always, or approximately 96-100 percent of employees have sufficient training**

Our review did confirm that the Department was adequately obtaining basic security and awareness training. We found over 98 percent of the Department's employees had the training. However, our audits have shown that agencies did not adequately track their contractors, and therefore, have difficulty in ensuring that they receive the required annual security training.

9. Does the agency explain policies regarding 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

USDA explains peer-to-peer file sharing policy in the IT security awareness training. Further, DM 3525-002, dated July 15, 2004, states that USDA has a long-established policy that does not condone or support employees' use of Government computers or networks for unauthorized purposes such as the use of peer-to-peer programs and other programs that perform these functions.

Our review confirmed that peer-to-peer file sharing was addressed in the Security Literacy and Basics course available on AgLearn and OCIO Cyber Security's security awareness training disk. The course teaches that peer-to-peer software are programs that link computers together across the internet for the purpose of sharing files, music, and videos and peer-to-peer software traditionally bypasses security controls and client/server networks that exist in business and Government offices. Because peer-to-peer software bypasses the USDA network security checks and balances, the installation of peer-to-peer software is prohibited at USDA. In addition, OCIO tracks and sends out periodic emails to agencies informing them of peer-to-peer activity on their networks. Although they issue listings of IP addresses with this activity, they do not block this traffic at the firewall.

Exhibit B – Audits Referenced to in the Report

Audit Report No.	Title	Estimated Issue Date
05401-15-FM	Audit of Fiscal Year 2006 Federal Crop Insurance Corporation's Financial Statements	November 2006
06401-21-FM	Audit of Commodity Credit Corporation's Fiscal Year 2006 Financial Statements	November 2006
08401-7-FM	Audit of Fiscal Year 2006 Forest Services Financial Statements	November 2006
10501-5-FM	National Resources Conservation Service Applications Controls – Program Contracts System	July 2006
11401-24-FM	Fiscal Year 2006 – National Finance Center General Controls	September 2006
50401-59-FM	Fiscal Year 2006 USDA Financial Statements	November 2006
85501-1-FM	Review of Dedicated Loan Origination and Servicing System's Application Controls – Fiscal Year 2006	October 2006
88501-6-FM	Management and Security Over the U.S. Department of Agriculture Universal Telecommunications Network	August 2006
88501-7-FM	Information Technology Services (ITS) General Controls Review – Fiscal Year 2006	October 2006
88501-9-FM	National Information Technology Center General Controls Review - Fiscal Year 2006	September 2006