U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

FISCAL YEAR 2005 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Report No. 50501-5-FM

October 2005

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

October 6, 2005

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

SUBJECT: Fiscal Year 2005 Federal Information Security Management Act Report (Audit Report No. 50501-5-FM)

Dear Director Bolten:

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. The Department 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 within USDA.

Sincerely,

/s/

Phyllis K. Fong
Inspector General

Executive Summary

Fiscal Year 2005 Federal Information Security Management Act Report

Results in Brief

The efforts of the Department's 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. Although the 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 management's historic lack of commitment to implementing an effective security program within their respective agencies. While progress has been made there is still much to be accomplished. Due to the significance of these weaknesses the Department cannot be assured that its systems and data are adequately secured. As a result, IT management and security remain a material weakness within the Department.

The following summarizes the weaknesses discussed in exhibit A of this report, in which OIG responds to the Office of Management and Budget's (OMB) questions as required by OMB Memorandum M-05-15, "Fiscal Year 2005 Reporting Instructions for the Federal Information Security."

- The Department does not have a reliable inventory of applications and general support systems from which to manage Department-wide IT security. Furthermore, the Department has not properly identified interfacing systems and networks to ensure service level agreements (SLA) require system security protection on all components interfacing with the Department's network resources. [1]

- Agencies have not followed NIST guidance when preparing security plans, risk assessments, and disaster recovery plans. Agencies relied on the contractors to complete certification and accreditation documentation.[2] Despite the fact that supporting documentation was either missing or contained inaccurate or incomplete data that did not comply with Federal requirements, agency officials inappropriately accredited their systems based in part on the recommendation of the certifying officials.

[1]OMB Circular No. A-130 Section 8 requires agreements between service recipients and service providers. Appendix III further details the agreements for system interconnection and information sharing. National Institute of Standards and Technology (NIST) Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems," provides in the Executive Summary that it contains guides and samples for developing an Interconnection Security Agreement and a memorandum of understanding which are forms of SLAs.

[2]Audit Report No. 50501-4-FM, Official Draft, "Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts," dated September 9, 2005.

- Agencies had not reported to OCIO the risk impact levels based on Federal Information Processing Standards (FIPS) 199 for 65 of the 160 systems we reviewed. These system risk impact levels are based on confidentiality, integrity, and availability of the data residing on the system. Further, our audits have shown that agencies did not ensure that the risk impact levels were consistent with FIPS requirements and that the risk ratings assigned remained consistent throughout all of the certification and accreditation documents.

- Agencies reported a greater number of deficiencies from audits and self assessments than they had in prior years; however, additional controls are needed to ensure the accuracy and timeliness of Plan of Actions and Milestones (POA&M) database results. At the time of our review, agencies were still completing risk assessments so not all weaknesses identified by those risk assessments had been reported in the POA&Ms. We also found that the agencies we reviewed did not have controls in place to ensure that POA&M data reported to the Department's Chief Information Officer was complete and accurate and identified (1) the tasks to be accomplished, (2) the resources required to accomplish the elements of the plan, or (3) any milestones in meeting the tasks.

- During the period of October 1, 2004, through July 23, 2005, the Department followed its policies and procedures for identifying, reporting, and resolving security incidents, and successfully closed 144 of the 202 fiscal year 2005 security incidents. Ninety-five percent of the security incidents involved malicious code, unauthorized access, and/or improper usage of network resources. However, testing disclosed that recent implementation of new technology on the U.S. Department of Agriculture telecommunications "backbone" severely degraded the Department's ability to identify, report, and resolve security incidents.

- Agencies had not timely completed patch management and infrastructure support services scans on network resources. Our analysis shows that security vulnerability patches were available for almost 6 years to as recent as 6 months that could have resolved agency system vulnerabilities. Despite the requirement that agencies and staff offices submit scanning and patch management assurances, only 5 of the 26 agencies and staff offices submitted vulnerability scan reports to OCIO. No agencies submitted patch management assurances.

- A complete and accurate listing of Internet Protocol (IP) addresses does not exist, even though OIG made a recommendation in fiscal year 2001 to create a consolidated listing. [3] In fiscal year 2006, OCIO again plans to

[3] Audit Report No. 50099-32-FM, "Government Information Security Reform Act – Fiscal Year 2001," August 2001, page 28.

develop a system in order to adequately track IP addresses, patch management, and scanning of network resources.

- As of August 30, 2005, only 54 percent of USDA employees and contractors had sufficient security awareness training, this percentage includes employees with significant IT security responsibility. Additionally, agencies still do not adequately track training of their contractors.

- Agencies reported to OCIO that over 500 of their approximately 109,000 employees had significant IT security responsibility. For employees with significant IT security, OCIO Cyber Security reported that role based training is deficient and needs to be adequately addressed.

- Agency's Federal Information Security Management Act compliance self assessments data as of August 31, 2005, showed that only 5 of the 26 agency and staff offices employed configuration management principles for their IT systems. Additionally, the Department-wide security configuration policy needs to be updated to include security policies for Windows 2003 Server, Cisco Router Internetwork Operating System, and Oracle software.

Due to the significance of these issues, 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 will not make additional recommendations related to those conditions 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
DM	Departmental Manual
FCIC	Federal Crop Insurance Corporation
FIPS	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FNS	Food Nutrition Service
FSA	Farm Service Agency
FS	Forest Service
GAO	Government Accountability Office (formerly the General Accounting Office)
GISRA	Government Information Security Reform Act
ISSPM	Information System Security Program Manager
IG	Inspector General
IP	Internet Protocol
IT	Information Technology
ITS	Information Technology Services, a division of the OCIO
MOU	Memorandum of Understanding
NASS	National Agricultural Statistics Service
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
RD	Rural Development
RMA	Risk Management Agency
SLA	Service Level Agreement
SP	Special Publication
TSO	Telecommunications 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 laid out 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.

The Act 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 establish new annual reviews, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

The legislation assigned specific responsibilities to OMB, agency heads, Chief Information Officers (CIO), and Inspectors General (IG). OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. This includes the authority to approve agency information security programs. OMB is also required to submit an annual report to Congress summarizing 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, the Act 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 Department-wide security program; and
- evaluating the agency and OCIO's Plan of Actions and Milestones consolidation and reporting process.

Scope and Methodology

The scope of our review was Department-wide and agency audits relating to IT completed during fiscal year 2005 through September 2005. We conducted this audit in accordance with Government Auditing Standards.

Fieldwork for this audit was performed at the Department OCIO from June to August 2005, and included a review of USDA's e-Authentication solution certification and accreditation documentation. 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 2005 audit work covered 10 agencies and staff offices: Animal and Plant Health Inspection Service (APHIS), Food 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 (OCFO), OCIO (includes Information Technology Services (ITS), National Information Technology Center (NITC), Telecommunication Services Operations (TSO)), Rural Development (RD), and Risk Management Agency (RMA) (includes Federal Crop Insurance Corporation (FCIC)). These agencies and staff offices operate approximately 302 of the estimated 460 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 in prior OIG and GAO audit reports; and

- gathered the necessary information to address the specific reporting requirements outlined in Office of Management and Budget's (OMB) Memorandum No. M-05-15, dated June 13, 2005.

[5]The Department identified 460 systems on its certification and accreditation spreadsheet dated August 1, 2005. OCIO's data are agency-supplied and have not been verified or audited. Based on independent auditor verification at three agencies, OIG identified at least another 38 systems not included in the 460. Hence, we question the accuracy and reliability of the total number of systems reported.

Section C: Inspector General Questions

1. **As required in the Federal Information Security Management Act (FISMA), the Inspector General (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 Publication (FIPS) 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 annual requirements for conducting 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, "Recommended Security Controls for Federal Information 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.**

   The U.S. Department of Agriculture (USDA) has approximately 26 agency and staff offices and over 460 systems. [6] We conducted reviews at 10 agencies that operated an estimated 302 systems. We reviewed 160 of the 302 systems.[7] Three of the systems selected for review were contractor operated systems. We used FIPS 199 risk impact levels for these systems as reported by OCIO. However, during our review of the Department's C&A 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 C&A documents.[8] We found that agencies had not reported to OCIO the risk levels based on FIPS 199 for 65 of the 160 systems reviewed. 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.

   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 the Security Act, Office of

[6]The Department identified 460 systems on its certification and accreditation (C&A) spreadsheet dated August 1, 2005. Office of the Chief Information Officer's (OCIO) data are agency-supplied and have not been verified or audited. Based on independent auditor verification at three agencies, the Office of Inspector General (OIG) identified at least another 38 systems not included in the 460. Hence, we question the accuracy and reliability of the total number of systems reported.

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

[8]Audit Report No. 50501-4-FM, Official Draft, "Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts," dated September 9, 2005.

Management and Budget (OMB), and NIST guidelines. Agencies primarily use OIG audits to identify weaknesses in their management and oversight of contractors.

Agencies also rely on our reviews of the Department's centralized data centers to ensure that the Security Act, OMB, and NIST guidelines are followed by those centers.

Thirteen of the 26 agencies and staff offices did not meet FISMA requirements to provide security self assessments to the OCIO. Only 2 of the 26 agencies and staff offices met FISMA requirements to use NIST SP 800-26 to assess all of their systems and their overall security program. The remaining 11 agencies used NIST SP 800-26 to review either major applications or their overall security program, but did not assess both as required by FISMA.

Based on the OIG reviews performed throughout fiscal year 2005, we continue to find that not all agencies have followed NIST guidance when preparing security plans, risk assessments, and disaster recovery plans. As reported last year, and again this year during our audit of the Department's C&A efforts, the Department does not have a reliable inventory of applications and general support systems from which to manage Department-wide information technology (IT) security. The Department relies on agencies to provide a comprehensive system inventory; however, with limited resources, OCIO is unable to verify the accuracy or reliability of those agency-provided inventories. OIG was not involved in the development and verification of agency IT system inventory. While we agree that OCIO's current list of major applications provides a 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.

2. For each part of this question, identify actual performance in fiscal year 2005 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 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.					
		1.a. Fiscal year 2005 Agency Systems		1.b. Fiscal year 2005 Contractor Systems[9]		1.c. Fiscal year 2005 Total Number of Systems		2.a Number of systems certified and accredited[10]		2.b. Number of systems for which security controls have been tested and evaluated in the last year		2.c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
		Total #[11]	# Rev.[12]	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
1. APHIS	High	9	0			9	0	7	78%	7	78%	0	0%
	Moderate	10	1			10	1	6	60%	6	60%	0	0%
	Low	12	0			12	0	9	75%	9	75%	0	0%
	Not Categorized	5	0			5	0	4	80%	4	80%	0	0%
	Sub-total	36	1			36	1	26	72%	26	72%	0	0%
2. FNS	High	11	2	1	1	11	2	8	73%	8	73%	1	9%
	Moderate	1	0			1	0	1	100%	1	100%	0	0%
	Low	0	0			0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0			0	0	0	0%	0	0%	0	0%
	Sub-total	12	2			12	2	9	75%	9	75%	1	8%
3. FS	High	4	4	2	2	4	4	4	100%	4	100%	0	0%
	Moderate	6	6			6	6	6	100%	6	100%	0	0%
	Low	5	5			5	5	5	100%	5	100%	0	0%
	Not Categorized	62	62			62	62	62	100%	62	100%	0	0%
	Sub-total	77	77			77	77	77	100%	77	100%	0	0%
4. FSA (includes CCC)	High	48	48			48	48	18	38%	20	42%	17	35%
	Moderate	11	11			11	11	0	0%	0	0%	0	0%
	Low	5	5			5	5	0	0%	0	0%	0	0%
	Not Categorized	0	0			0	0	0	0%	0	0%	0	0%
	Sub-total	64	64			64	64	18	28%	20	31%	17	27%

[9] Contractor systems identified in question 1b are included in question 1a totals.

[10] Based on numbers reported to OCIO; however, OIG's review of C&As determined that the C&A process was ineffectively implemented and the departmental oversight of the C&A process could be significantly improved. We determined that agencies did not accurately report the number of systems accredited. OIG did not verify the numbers reported by OCIO. Audit Report No. 50501-4-FM, Official Draft, "Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts," dated September 9, 2005.

[11] Based on independent auditor verification and may not be consistent with the number of systems reported by OCIO.

[12] Reviews conducted from October 1, 2004, through August 31, 2005.

Bureau Name (OIG Reviewed)	FIPS Risk Impact Level	Question 1.						Question.2.					
		1.a. Fiscal year 2005 Agency Systems		1.b. Fiscal year 2005 Contractor Systems		1.c. Fiscal year 2005 Total Number of Systems		2.a Number of systems certified and accredited[13]		2.b. Number of systems for which security controls have been tested and evaluated in the last year		2.c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
		Total #[14]	# Rev.[15]	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
5. NASS	High	6	1			6	1	6	100%	6	100%	0	0%
	Moderate	0	0			0	0	0	0%	0	0%	0	0%
	Low	0	0			0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0			0	0	0	0%	0	0%	0	0%
	Sub-total	6	1			6	1	6	100%	6	100%	0	0%
6. NRCS	High	0	0			0	0	0	0%	0	0%	0	0%
	Moderate	4	1			4	1	4	100%	4	100%	0	0%
	Low	0	0			0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0			0	0	0	0%	0	0%	0	0%
	Sub-total	4	1			4	1	4	100%	4	100%	0	0%
7. OCFO	High	26	2			26	2	26	100%	26	100%	0	0%
	Moderate	1	0			1	0	0	0%	0	0%	0	0%
	Low	3	0			3	0	3	100%	3	100%	0	0%
	Not Categorized	1	0			1	0	1	100%	1	100%	0	0%
	Sub-total	31	2			31	2	30	97%	30	97%	0	0%
8. OCIO (includes ITS, NITC, and TSO)	High	12	1			12	1	10	83%	10	83%	1	8%
	Moderate	11	1			11	1	11	100%	11	100%	2	18%
	Low	2	0			2	0	2	100%	2	100%	0	0%
	Not Categorized	8	2			8	2	0	0%	0	0%	0	0%
	Sub-total	33	4			33	4	23	70%	23	70%	3	9%
9.RD	High	6	4			6	4	6	100%	6	100%	0	0%
	Moderate	2	0			2	0	2	100%	2	100%	0	0%
	Low	12	0			12	0	12	100%	12	100%	0	0%
	Not Categorized	0	0			0	0	0	0%	0	0%	0	0%
	Sub-total	20	4			20	4	20	100%	20	100%	0	0%

[13]Based on numbers reported to OCIO; however, OIG's review of C&As determined that the C&A process was ineffectively implemented and the departmental oversight of the C&A process could be significantly improved. We determined that agencies did not accurately report the number of systems accredited. OIG did not verify the numbers reported by OCIO. Audit Report No. 50501-4-FM, Official Draft, "Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts," dated September 9, 2005.

[14]Based on independent auditor verification and may not be consistent with the number of systems reported by OCIO.

[15]Reviews conducted from October 1, 2004, through August 31, 2005.

Bureau Name (OIG Reviewed)	FIPS Risk Impact Level	Question 1.						Question.2.					
		1.a. Fiscal year 2005 Agency Systems		1.b. Fiscal year 2005 Contractor Systems		1.c. Fiscal year 2005 Total Number of Systems		2.a Number of systems certified and accredited[16]		2.b. Number of systems for which security controls have been tested and evaluated in the last year		2.c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
		Total #[17]	# Rev.[18]	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
10.RMA (includes FCIC)	High	7	3			7	3	7	100%	7	100%	0	0%
	Moderate	0	0			0	0	0	0%	0	0%	0	0%
	Low	0	0			0	0	0	0%	0	0%	0	0%
	Not Categorized	12	1			12	1	10	83%	10	83%	0	0%
	Sub-total	19	4			19	4	17	90%	17	90%	0	0%
USDA Totals	High	**129**	**65**	**3**	**3**	**129**	**65**	**92**	71%	**94**	73%	**19**	15%
	Moderate	**46**	**20**			**46**	**20**	**30**	65%	**30**	65%	**2**	4%
	Low	**39**	**10**			**39**	**10**	**31**	79%	**31**	79%	**0**	0%
	Not Categorized	**88**	**65**			**88**	**65**	**77**	88%	**77**	88%	**0**	0%
	Total	**302**	**160**	**3**	**3**	**302**	**160**	**230**	76%	**232**	77%	**21**	7%

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 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% of the time**
- **<u>Sometimes, for example, approximately 51-70% of the time</u>**
- **Frequently, for example, approximately 71-80% of the time**
- **Mostly, for example, approximately 81-95% of the time**
- **Almost Always, for example, approximately 96-100% of the time**

[16]Based on numbers reported to OCIO; however, OIG's review of C&As determined that the C&A process was ineffectively implemented and the departmental oversight of the C&A process could be significantly improved. We determined that agencies did not accurately report the number of systems accredited. OIG did not verify the numbers reported by OCIO. Audit Report No. 50501-4-FM, Official Draft, "Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts," dated September 9, 2005.
[17]Based on independent auditor verification and may not be consistent with the number of systems reported by OCIO.
[18]Reviews conducted from October 1, 2004, through August 31, 2005.

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 has been limited to access controls, security clearances, security awareness training, and oversight by the agencies of contractor activities. Based on our reviews, we have no evidence that the agencies have adequately employed methods to ensure that contractor provided services meet the requirements of the Security Act, OMB, and NIST guidelines.

(b) 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% complete**
- **Approximately 51-70% complete**
- **Approximately 71-80% complete**
- **Approximately 81-95% complete**
- **Approximately 96-100% complete**

Based on our reviews, we have documented evidence that the Department does not have a reliable inventory of applications and general support systems from which to manage Department-wide IT security and has not properly identified interfacing systems and networks to ensure Service Level Agreements (SLA) require system security protection on all components interfacing with the Department's network resources. [19] The Department relies on agencies to provide a comprehensive list; however, OCIO is 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 IT system inventories and their interfacing systems and networks. While we agree that OCIO's current list of major applications provides a 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.

During our reviews, we determined formal agreements between systems that interconnected did not exist. We found one agency had not executed a SLA with OCIO for

[19] Audit Report No. 50501-4-FM, Official Draft, "Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts," dated September 9, 2005.

the e-Authentication security interconnections even though OMB and NIST require agreements between service recipients and service providers.[20] At another agency, the system security plan stated that SLAs with interconnecting systems were pending. In both instances, the systems were fully accredited.

(c) OIG generally agrees with the Chief Information Officer (CIO) on the number of agency owned systems. (OIG's response is underlined.) 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) 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. (OIG's response is underlined.) Yes or No.

As stated in our response to question 3.a. above, the number of systems within the Department (both Department or contractor run) 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.

Our reviews have found that OCIO updates its system inventory as needed; however, we question the accuracy of the system inventory because, as mentioned in response to question 3.a., OCIO relies on the agencies to report system inventory. Further, OCIO is unable to verify the accuracy or reliability of those agency-provided inventories due to limited resources.

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

During our review of the e-Authentication C&A documentation, we determined that limited system e-Authentication risk assessments have been completed. We determined that e-Authentication does not have a configuration management plan as required by Departmental Manual (DM) 3520-001. Currently there are 127 USDA applications encompassing 17 agencies that rely on e-Authentication for single sign-on capabilities, with an additional 60 USDA applications and 4

[20]OMB Circular No. A-130, Section 8, requires agreements between service recipients and service providers. Appendix III further details the agreements for system interconnection and information sharing. NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," provides in the Executive Summary that it contains guides and samples for developing an Interconnection Security Agreement and a MOU which are forms of SLAs.

Federal Government applications in the process of integrating to e-Authentication. During our review of USDA's e-Authentication C&A documentation, we determined that the risk assessment was geared to only two FSA applications while the security plan included another 22 applications belonging to FSA, RD, and NRCS. Additionally, the risk assessment did not consider all applicable laws and regulations related to system security such as NIST, OMB Circular No. A-130, The Computer Security Act, or the Government Information Security Reform Act (superseded by the Federal Information Security Management Act of 2002). Without taking these laws and regulations into consideration, OCIO may not identify all the weaknesses within e-Authentication.

OCIO did not have a MOU or SLA with any interconnecting systems and e-Authentication. Without controls over interconnecting systems, OCIO cannot be assured that e-Authentication is being appropriately protected. This could result in a compromise of all connected systems and data they store, process, or transmit.

4. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide Plan of Actions and Milestones (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.

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

d. The 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% of the time**
- **Sometimes, for example, approximately 51-70% of the time**
- **Frequently, for example, approximately 71-80% of the time**
- **Mostly, for example, approximately 81-95% of the time**
- **Almost Always, for example, approximately 96-100% 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% of the time**
- **Sometimes, for example, approximately 51-70% of the time**
- **Frequently, for example, approximately 71-80% of the time**
- **Mostly, for example, approximately 81-95% of the time**
- **Almost Always, for example, approximately 96-100% 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% of the time**
- **Sometimes, for example, approximately 51-70% of the time**
- **Frequently, for example, approximately 71-80% of the time**
- **Mostly, for example, approximately 81-95% of the time**
- **Almost Always, for example, approximately 96-100% of the time**

Our review of OCIO's POA&M process determined that agencies were generally incorporating all known IT security weaknesses into the POA&M database. We found that OCIO established a deliverable schedule for agencies to follow to ensure the timely updates of the POA&M database. Further, we found that agencies reported a greater number of deficiencies from audits and self assessments than they had in prior years; however, additional controls are needed to ensure the accuracy and timeliness of POA&M database results. At the time of our review, agencies were still completing risk assessments so not all weaknesses identified by those risk assessments had been reported in the POA&Ms. We also found that the agencies we reviewed did not have controls in place to ensure that POA&M data reported to the Department's CIO were complete and accurate. For instance, we noted several POA&Ms that were identified as "complete" because the agency lacked the time and resources and/or funding to complete such actions, which included development of a system development life cycle process, conducting a business impact analysis, and updating and testing contingency plans. Our review showed that the POA&M did not identify (1) the tasks to be accomplished; (2) the resources required to accomplish the elements of the plan; or (3) any milestones in meeting the tasks.

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,
- system security test plans,
- MOU or SLA 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," (May, 2004) for C&A work initiated after May, 2004. This includes use of the FIPS 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. Assess the overall quality of the Department's C&A process. (OIG's response is underlined below.) Response Categories:**

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

    Despite repeated audit disclosures and pledges of corrective action, the Department and its agencies did not address OMB requirements that major applications and general support systems be certified and accredited until OMB made a specific call in its passback language for compliance by the end of fiscal year 2004. At that time the Department implemented an ambitious process and schedules to meet the stringent timeframes. Discussions with agency personnel disclosed that they relied on the contractors completing the documentation to adequately meet the requirements. Given the timeframes allotted and the absence of prior accreditations, the agencies could not have produced complete, accurate, and trustworthy information given the depth and breadth of documentation required to adequately support each accreditation. [21]

[21] Audit Report No. 50501-4-FM, Official Draft, "Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts," dated September 9, 2005.

6. Configuration Management.

a. Is there an agency-wide security configuration policy? (OIG's response is underlined.) Yes or No.

The Department-wide security configuration policy needs 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 (IOS), and Oracle software. We determined that OCIO provided the agencies security assessment guidelines for Windows XP Professional, Windows NT, Windows 2000 Professional, Windows 2000 Server, Solaris, HP-UX, and Linux operating systems.[22] In addition, the Department has 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.

Furthermore, we found that only 15 of 26 agencies provided OCIO their FISMA compliance self assessments data by August 31, 2005. One of the questions on the compliance self assessment asks whether the agency employs IT configuration management principles. We found that only 5 of the 26 agencies and staff offices employed configuration management principles for all of their IT systems.

	Product	Rarely, or on approximately 0-50% of the systems running this software	Sometimes, or on approximately 51-70% of the systems running this software	Frequently, or on approximately 71-80% of the systems running this software	Mostly, or on approximately 81-95% of the systems running this software	Almost Always, or on approximately 96-100% of the systems running this software
1	Window XP Professional	X				
2	Windows NT	X				
3	Windows 2000 Professional	X				
4	Windows 2000 Server	X				
5	Windows 2003 Server	X				
6	Solaris	X				
7	HP-UX	X				
8	Linux	X				
9	Cisco Router IOS	X				
10	Oracle	X				
11	Other (see narrative above)	X				

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

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.

From October 1, 2004, through July 23, 2005, OCIO followed its documented policies and procedures for identifying, reporting, and resolving incidents.[23] As of July 27, 2005, we determined that 144 of the 202 (71 percent) fiscal year 2005 security incidents had been successfully closed. Based on OIG prior audit recommendations, OCIO is in the process of revising its incident tracking process to enhance the tracking and monitoring of security incidents within the Department, and it is scheduled to be complete by September 30, 2005.[24] The new process should aid in quick identification of agencies that have not adequately addressed security incidents and allow for frequent follow up from OCIO Cyber Security staffs to agencies that are not timely in resolving security incidents.

The Department's recent implementation of new technology on the USDA "backbone" called Universal Telecommunications Network (UTN), has degraded the ability of OCIO to identify, report, and resolve security incidents. On July 23, 2005, USDA converted to the UTN and USDA, for a significant period of time, no longer had adequate intrusion detection sensors in place for the entire network. UTN was not designed to capture the number of intrusion attempts and specific information about the security incident to help resolve it; hence, with the implementation of UTN, the internal monitoring and reporting process was degraded. One feature of the UTN was to block certain types of potential intrusions before they hit the Department's backbone. However, because OCIO officials managing the UTN implementation were unaware of the reporting requirement of FISMA, they did not ensure the contractor had the ability to report on blocked attempts, which should also be reported under FISMA.

Our audit work to date has identified several incidents that went undetected by the UTN contractor. At least two website defacements were reported by United States Computer Emergencies Readiness Team (US-CERT) before Department officials became aware of it. Another problem noted with the contractor's reporting is its inability to detect and/or block peer-to-peer connections. Prior to implementation of the UTN, OCIO identified and reported several instances of peer-to-peer software used to download copyright or pornographic materials. During this review, OIG performed various tests, including testing of the Internet content filters. OIG's testing activities were never detected, even though UTN officials explicitly stated that these were being monitored.

Additionally, security vulnerability patches were available for almost 6 years to as recent as 6 months that could have resolved identified system vulnerabilities at the agencies we reviewed.

[23] DM 3505-001, Chapter 1 – Part 1, "Incident Response Procedures," dated July 15, 2004.
[24] At the end of fieldwork, this tracking process had not been implemented.

Completion of timely patch management and scans would aid in identifying and possibly preventing security incidents. Currently, OCIO tracks patch management and Internet Security Systems scans via the receipt of assurances from the agencies and this information is put into separate spreadsheets. Despite the requirement that agencies and staff offices submit scanning and patch management assurance statements to OCIO monthly, only five agencies submitted vulnerability scan reports to OCIO. However, no agency submitted patch management assurances.

Even though OIG made a recommendation in fiscal year 2001, we continue to find that OCIO has not developed a system to adequately track Internet Protocol (IP) addresses. [25] On August 31, 2005, OCIO Cyber Security officials stated that a waiver was signed to contract for the development of a database to track IP addresses, patches, and scanning. Currently, no up-to-date consolidated listings of IP addresses exist. Consequently, when security incidents occur OCIO may not get timely resolution because they are not able to contact the appropriate agency for action.

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

Despite the fact that the Department had not identified all incidents as discussed in our response to question 7a, we found that OCIO did report three known security incidents to law enforcement during fiscal year 2005. OCIO Cyber Security officials stated that another three incidents were reported to OCIO by the Federal Bureau of Investigations. However, the agencies do not follow USDA policies and procedures for reporting security incidents to law enforcement authorities.[26] The policy states that the Information System Security Program Manager (ISSPM) should complete an intrusion report and forward it onto Cyber Security for referral to OIG. Cyber Security staff stated that agencies do not provide this information to Cyber Security staff. Hence, OCIO Cyber Security could not give us a complete count of security incidents reported to law enforcement for the Department even though departmental guidance requires agency ISSPMs to report all incidents reported to law enforcement to OCIO. OCIO Cyber Security staffs are not aware of all incidents reported to law enforcement because several agencies have their own law enforcement unit or their own forensics units and these agencies do not inform OCIO Cyber Security of security incidents reported to law enforcement.

[25] Audit Report No. 50099-32-FM, "Government Information Security Reform Act – Fiscal Year 2001," August 2001 page 28.
[26] DM 3505-001, Chapter 1 – Part 1, Section 2e, "Incident Response Procedures," dated July 15, 2004.

c. The agency follows defined procedures for reporting to the US-CERT. http://www.us-cert.gov. (OIG's response is underlined.) Yes or <u>No</u>.

During fiscal year 2005, as of July 27, 2005, USDA's Cyber Security staff reported 202 network security incidents to US-CERT as required by its policy in the following categories:

Category	Name	Total Incidents
0	Network Defense Testing	1
1	Unauthorized Access	42
2	Denial of Service	5
3	Malicious Code	136
4	Improper Usage	14
5	Scans/Probes/Attempted Access	2
6	Investigation	2
Total		**202**

However, as stated above, on July 23, 2005, USDA converted to UTN and this conversion substantially degraded USDA's incident reporting, handling, response, and oversight process because USDA no longer has adequate intrusion detection sensors in place for the entire network. The UTN implementation prevents the intrusion detection system from "seeing the vast majority of USDA network traffic" and an overall network view is no longer available for network security staff to review, analyze, and report potential incidents to Cyber Security for action. OCIO officials informed us that this is an issue currently being addressed by its contractor. The contractor's intrusion detection system was not designed to report the number of intrusion attempts that were blocked.

The Department is required by FISMA to report security incidents to US-CERT so this information can be forwarded to Homeland Security. Therefore, the Department needs to have an intrusion detection process in place that monitors its network for intrusions; report these intrusions to US-CERT; and ensure that immediate corrective action is taken to prevent and detect similar incidents.

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 Categories:

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

Our review found that approximately 54 percent of USDA employees (includes employees with significant IT security responsibility) have sufficient security awareness training. The Department's primary vehicle for this training is the Department's AgLearn online system. OCIO requires agencies to complete security awareness training prior to FISMA reporting; however agencies do not always comply. Therefore, the Department can not ensure that every employee receives the proper training. On August 5, 2005, OCIO Cyber Security sent out a memorandum to agency senior management informing them that security awareness and training requirements were not being met, and, in fact, were far behind schedule with only 21 percent reporting in AgLearn as of July 20, 2005. As of August 15, 2005, AgLearn showed that 66,990 of 131,271 (51 percent) employees had completed security awareness training. Furthermore, the AgLearn statistics did not coincide with training numbers reported in the FISMA, so OCIO Cyber Security requested agency officials to validate the training numbers and send supporting documentation to Cyber Security by August 16, 2005. As of August 30, 2005, one agency had not sent validation of employee and contractor training numbers to OCIO. The information provided showed 109,505 employees of which 59,334 had received security awareness training (54.18 percent). In addition, agencies reported 532 of the 109,505 employees had significant IT security responsibility. Because of their responsibilities, these employees are to receive additional training consistent with their duties. OCIO Cyber Security reported that role based training for employees with significant IT security is deficient and needs to be adequately addressed.

Finally, our reviews have shown that agencies do 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. However, the vehicle for ensuring that this message gets to all users within the Department, is the AgLearn system. Based on our response to question number 8 above, we question how effectively this policy is being implemented.

Exhibit B – Audits Referenced to in the Report

Audit Report No.	Title	Estimated Issue Date
05401-14-FM	Federal Crop Insurance Corporation/Risk Management Agency's Financial Statements for Fiscal Year 2005	November 2005
06401-20-FM	Commodity Credit Corporation's Financial Statements for Fiscal Years 2005 and 2004	November 2005
08401-5-FM	Forest Services for Fiscal Year 2005 Financial Statements	November 2005
10501-5-FM	National Resources Conservation Service Applications Controls – Program Contracts System	November 2005
27401-1-FM	Food and Nutrition Service – Fiscal Year 2005 Financial Statements	November 2005
50501-3-FM	Management and Security Over IT Convergence/Common Computing Environment	October 2005
50501-4-FM	Review of USDA's Certification and Accreditation Efforts	October 2005
88501-2-FM	National Information Technology Center General Controls Review – Fiscal Year 2005	September 21, 2005 (actual issuance)