U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Fiscal Year 2007 Federal Information Security Management Act Report

Report No. 50501-11-FM
September 2007

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 26, 2007

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

Subject: Fiscal Year 2007 Federal Information Security Management Act Report

Dear Director Nussle:

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

Sincerely,

/s/

Phyllis K. Fong
Inspector General

Executive Summary

Fiscal Year 2007 Federal Information Security Management Act Report (Audit Report No. 50501-11-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 several years have heightened program management's awareness of the need to plan and implement effective information technology (IT) security. OCIO has improved its oversight in several areas during this fiscal year. For example, the inventory of agency systems had significantly improved. In other areas, such as the certification and accreditation (C&A) process, improvements were noted, but additional work is still needed. The Department has advanced in the past several years, but much more work is needed to address the IT material control weaknesses that continue to impact this large and complex organization.

The continuing material IT control weaknesses within the Department are due to the lack of an effective overall Departmentwide plan. The Department needs to coordinate with all of its agencies, determine the overall risks, prioritize the risks, and develop and implement a time-phased plan to systematically mitigate risks. With agency cooperation and acceptance improvements could be made.

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

The following summarizes the key matters discussed in exhibit A of this report, which contains OIG's responses to questions required by Office of Management and Budget (OMB) Memorandum No. M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 25, 2007.

- Our review disclosed that agencies that had contractor systems attached to their networks could not provide documentation to validate that sufficient oversight and evaluation activities were in place to ensure information systems used or operated by a contractor of the agency, or other organization on behalf of the agency, met the requirements of FISMA, OMB, and National Institute of Standards and Technology (NIST) guidelines.

- While OCIO made significant improvements in its oversight of the Departmental inventory records, the process did not include tracking system interfaces or contractor systems. In addition, guidance regarding contractor systems had not been developed and provided to agencies. A review of 14 system security plans revealed that 6 systems interfaced with other systems; however, none of those interfaces appeared within the official Department inventory. System interfaces were not part of the OCIO semi-annual inventory reconciliation process, and therefore were not included in the Department's oversight. In addition, while the semi-annual inventory reconciliation did provide good oversight of overall systems, it did not differentiate between agency owned and contractor systems. As a result, at least one contractor system was not recorded in the official Department inventory.

- The Department made improvements in its plan of action and milestones (POA&M) recording, tracking, and closures. However, individual agencies are responsible to accurately input, track, and close POA&Ms. Our review disclosed that the agencies did not add POA&Ms based on the C&A testing and evaluation for 9 of the 10 systems we reviewed. In addition, scanning vulnerabilities not mitigated within 30 days were not tracked by all six agencies we reviewed. In addition, we reviewed 19 closed POA&Ms during this review and found 5 were closed improperly and 3 had inadequate documentation that the weaknesses had been properly corrected and/or mitigated. Based upon our work during the fiscal year, we have no assurance that agencies were entering, tracking, and adequately closing POA&Ms.

- Our review of the Automated Security Self-Evaluation and Remediation Tracking (ASSERT) tool disclosed 10 systems that did not apply the appropriate risk levels to their systems in accordance with Federal guidelines.[1] For instance, one system had two high risk security objectives, yet the system was categorized as moderate. According to Federal guidelines, any security objective that is high defines the system categorization as high. This occurred because Department did not always provide adequate oversight of system categorization. Without a proper risk level assignment, the agencies cannot design their security programs to ensure the appropriate security controls are in place to protect the confidentiality, integrity, and availability of their systems.

- We noted that the C&A process within the Department was not adequate. Our detailed review of 10 C&As showed agencies had not followed NIST guidance.[2] Specifically, we found (1) nine security plans, seven risk assessments, and nine disaster recovery plans that

[1] Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated December 2003.

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

did not follow NIST guidance, and did not provide complete, accurate, and consistent information; (2) for three systems the independent testing and evaluation processes did not provide adequate assurances that controls were in place and operating effectively; (3) in nine of the systems controls chosen for continuous monitoring had not been documented; and (4) eight systems were accredited in spite of serious weaknesses.

- The Department had implemented a concurrency review (quality assurance program) of agency C&A submissions prior to accreditation. Based on our review, the concurrency reviews were not providing adequate oversight to ensure that agency system documentation met NIST guidance and that agency controls were properly safeguarding agency systems and data. We found that the concurrency reviews were not denying authority to operate to systems that did not have controls in place to protect the system, performing followup to ensure weaknesses identified during the reviews were mitigated, and/or accurately reviewing agency C&A documentation.

- Privacy Act implementation within the Department continued to be inadequate. We found that in our review of 89 systems, 18 Privacy Impact Assessments (PIA) had not been completed and 8 more were still in draft. Of the 71 PIAs provided and reviewed, 36 did not meet Departmental[3] standards. In addition, the content of the PIAs was not always clear and/or information was contradictory regarding the usage of personally identifiable information (PII) on those systems. If PII information is in the system, a Statement of Record Notice (SORN) is required to be published in the Federal Register for any new or intended use of personal information. We found that 11 of 38 required SORNs had not been published. Finally, of eight Privacy Act Officers interviewed, none were aware of key requirements such as formulating policy, handling privacy incidents, or analyzing business flows for privacy implications.

- The Department had taken some steps to implement the provisions of OMB Memorandum No. M-06-15, but had yet to fully achieve that goal.[4] One positive step was the recent granting of a blanket purchase agreement to encrypt mobile devices with a planned completion date of March 31, 2008. Until this is fully implemented, the Department is very susceptible to PII incidents as noted by the 50 incidents that occurred this fiscal year. In addition, some legacy systems within the Department use the social security number as a piece of identifying information. Also, we found that there were at

[3] Departmental Manual (DM) 3515-002, *Privacy Impact Assessment*, dated February 17, 2005.
[4] OMB Memorandum No. M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006.

least 181 unencrypted wireless access points (AP) at selected locations within the Department which could potentially broadcast PII in clear text.[5]

- An adequate Departmental configuration policy did not exist with checklists for each operating system. To determine the level of security and configurations within the Department, we scanned six agencies' networks using commercially available software to look for known security vulnerabilities. In addition, we reviewed the level of security software patches that were applied at seven agencies. We found that (1) over 700 high risk vulnerabilities were present and unmitigated or the acceptance of risk was not documented, and (2) over 240,000 patches were not applied to over 26,000 devices.[6] We also reviewed the running configurations of network routers, switches, and firewalls at six agencies using commercially available software. We noted over 900 configuration errors within those agencies' devices. In addition, we noted that some of these agencies had stated in their July 2007 scorecard that they were 100 percent patched and scanned. Agencies were not reporting their accurate security posture in the scorecards and OCIO was not validating the information when received.

- NIST guidance states that "while the solutions to IT security are complex, one basic yet effective tool is the security configuration checklist."[7] The Department had issued guidance to achieve this NIST requirement by issuing checklists for some operating systems.[8] We reviewed six agencies to determine whether the Department's standard checklists for configuring systems were being used. We found checklists were not being used to configure the systems in four of six agencies and they could not provide documentation to support why the checklists were not used. In addition, checklists were not available to the agencies until August 2007 because they had been removed from the website and OCIO could not locate them. Fortunately, OIG was able to provide copies from our previous audit work. Also, as noted in the fiscal year 2006 FISMA audit report, not all checklists had been created. As a result, USDA systems were vulnerable to many threats, ranging from remotely launched network service exploits to malicious code spread through e-mails, malicious web sites, and file downloads.

[5] In computer networking, a wireless AP is a device that connects wireless communication devices together to form a wireless network. The AP usually connects to a wired network and can relay data between wireless devices and wired devices. APs had Internet Protocol (IP) addresses for configuration.

[6] High risk vulnerabilities are those which provide access to the computer, and possibly the network of computers.

[7] NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers,* dated December 2006.

[8] DM 3540-002, *Risk Assessment and Security Checklists*, dated April 19, 2004.

- OCIO made progress in tracking incident responses. During the fiscal year it implemented the Cyber Security Incident Response Management database to facilitate tracking and closeout of incidents. The database tracks the ticket number, open and close dates, categories of incidents, PII information, and whether the incident was forwarded to other Federal agencies. However, we found policies and procedures for incident handling were not being followed and that incidents were not closed properly or timely, or were not reported to necessary authorities. As a result, OCIO had limited assurance that incidents were being appropriately and timely reported and that security problems were being adequately addressed. We reviewed the incident tracking database and found 92 of the 399 incidents did not have documented closure within 30 days and that 75 incidents did not have United States Computer Emergency Readiness Team (US-CERT) numbers (agency officials stated that these were mainly false positives).[9] However, our review found that they should have been reported based on the US-CERT category in the database. In addition, we found over 100 incidents that had not been reported to OIG because OCIO did not have a standard distribution list.

- The Internet Protocol Address Database (IPAD) is vital to the timeliness of incident response. IPAD is the Department's internet protocol (IP) address repository. This tool is used to determine the agency and location of the device when an incident occurs. It includes agency contact information, and whether PII is present on that system. Although OCIO had made progress in the implementation of the IPAD, more work is needed. We found that IPAD still did not have a complete and accurate listing of USDA IP addresses in the Department's tracking database for three out of the six agencies reviewed. This was due to a lack of management commitment to monitor IPAD to ensure that a complete and accurate inventory of IP addresses was maintained.

- We reviewed e-authentication risk assessments, required by OMB, at six agencies.[10] We found one agency that did not use e-authentication. Of the remaining five, only one could provide documentation to show it had conducted an assessment. The agencies were either unaware that a separate risk assessment was required or were not aware of a requirement to keep the documentation. Without doing and/or documenting a risk assessment for e-authentication there is no assurance that business transactions have the required level of verification for authentication.

[9] US-CERT is required to be notified for certain incidents by DM 3505-000, *USDA Computer Incident Response Procedures Manual*, dated March 20, 2006.

[10] OMB Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, dated December 16, 2003.

Authentication risks with potentially higher consequences require higher levels of assurance.

Recommendation In Brief

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

Abbreviations Used in This Report

AP	access point
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
FAS	Foreign Agricultural Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FNS	Food and Nutrition Service
FS	Forest Service
FSA	Farm Service Agency
FSIS	Food Safety and Inspection Service
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
IG	Inspector General
IP	internet protocol
IPAD	Internet Protocol Address Database
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 action and milestones
PIA	Privacy Impact Assessment
PII	personally identifiable information
RMA	Risk Management Agency
SORN	Statement of Record Notice
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture

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 also has 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 of the Act 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;

- evaluating the agencies’ and OCIO’s plan of action and milestones consolidation and reporting processes;

- reviewing Privacy Act implementation and oversight; and

- reviewing the adequacy of e-authentication risk assessments.

Scope and Methodology

The scope of our review was Departmentwide and agency audits relating to IT completed during fiscal year 2007. We conducted this performance audit in accordance with generally accepted *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Fieldwork for this audit was performed at the Department OCIO from June through September 2007. 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 2007 audit work covered 12 agencies and/or staff offices: Animal and Plant Health Inspection Service (APHIS), Agricultural Marketing Service (AMS), Agricultural Research Service (ARS), Food and Nutrition and Service (FNS), Food Safety and Inspection Service (FSIS), Foreign Agricultural Service (FAS), Forest Service (FS), Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), Office of the Chief Financial Officer (OCFO), OCIO, and Risk Management Agency. These agencies and staff offices operate approximately 216 of the OCIO estimated 259 general support and major application systems within the Department.[11]

To accomplish our audit objectives, we performed the following procedures at Headquarters and selected field offices.

- 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 (OIG) and GAO audit reports.

- Gathered the necessary information to address the specific reporting requirements outlined in OMB Memorandum No. M-07-19, dated July 25, 2007.

[11] The Department identified 259 systems in its plan of action and milestones system as of August 6, 2007.

- Performed detailed testing specific to FISMA requirements at selected agencies as detailed in this report.[12]

[12] Those agencies were APHIS, ARS, AMS, FAS, FNS and NRCS.

Exhibit A *– OMB Reporting Requirements and USDA OIG Position*

Section C: Inspector General Questions

1. **As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.**

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

   Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self-reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

   (See table on next page.)

2. For the Total Number of Systems reviewed by Component/Bureau and Federal Information Processing Standards (FIPS) Systems Impact Level in the table for Question 1, identify the number and percentage of systems which have a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

Bureau Name (OIG Reviewed)	**FIPS 199 System Impact Level**	**Question 1.**						**Question 2. – Agency Reported**					
		1.a. Fiscal year 2007 Agency Systems. As of 8/6/07		**1.b. Fiscal year 2007 Contractor Systems. As of 8/6/07**		**1.c. Fiscal year 2007 Total Number of Systems (Agency and Contractor systems)**		**2.a[13] Number of systems certified and accredited As of 9/17/07**		**2.b.[14] Number of systems for which security controls have been tested and evaluated in the past year. As of 9/17/07**		**2.c.[15] Number of systems for which contingency plans have been tested in accordance with policy. As of 8/24/07**	
		Total #	**# Rev.**	**Total #**	**# Rev**	**Total #**	**# Rev**	**Total #**	**Percent of Total**	**Total #**	**Percent of Total**	**Total #**	**Percent of Total**
1. FS	High	1	0	0	0	1	0	0	0%	0	0%	*N/R	*N/R
	Moderate	14	13	0	0	14	13	1	7%	0	0%	*N/R	*N/R
	Low	2	1	0	0	2	1	1	50%	0	0%	*N/R	*N/R
	Sub-total	17	14	0	0	17	14	2	12%	0	0%	*N/R	*N/R
2. FSIS	High	4	3	0	0	4	3	4	100%	0	0%	*N/R	*N/R
	Moderate	8	7	0	0	8	7	8	100%	1	13%	*N/R	*N/R
	Low	1	1	0	0	1	1	1	100%	0	0%	*N/R	*N/R
	Sub-total	13	11	0	0	13	11	13	100%	1	8%	*N/R	*N/R
3. RMA	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	*N/R	*N/R
	Moderate	17	3	0	0	17	3	1	6%	1	6%	*N/R	*N/R
	Low	1	0	0	0	1	0	0	0%	0	0%	*N/R	*N/R
	Sub-total	18	3	0	0	18	3	1	6%	1	6%	*N/R	*N/R
4. OCFO-NFC	High	4	3	0	0	4	3	4	100%	3	75%	*N/R	*N/R
	Moderate	9	2	0	0	9	2	6	67%	4	44%	*N/R	*N/R
	Low	0	0	0	0	0	0	N/A	N/A	N/A	N/A	*N/R	*N/R
	Sub-total	13	5	0	0	13	5	10	77%	7	54%	*N/R	*N/R

[13] These numbers come from the OCIO as of September 17, 2007, and identified systems that had under gone a C&A. These do not include systems with an Interim Authority to Operate or 86 systems scheduled to undergo a completed C&A by September 30, 2007. For an assessment of the quality of the C&A process, see Question 5.

[14] OIG cannot determine an accurate number of systems that have self-assessments completed. We reviewed self-assessments done in six agencies (APHIS, ARS, AMS, FAS, NRCS, and FNS) and found that all six could not provide documentation of testing on any controls not undergoing the C&A process. Numbers, therefore, are those C&A'd in 2007.

[15] The numbers here are based solely on work performed by OIG for our six selected agencies. *N/R means we did not review that agency.

		Question 1.						Question 2. – Agency Reported					
Bureau Name (OIG Reviewed)	FIPS 199 System Impact Level	1.a. Fiscal Year 2007 Agency Systems. As of 8/6/07		1.b. Fiscal Year 2007 Contractor Systems. As of 8/6/07		1.c. Fiscal year 2007 Total Number of Systems (Agency and Contractor systems)		2.a[16] Number of systems certified and accredited As of 9/17/07		2.b.[17] Number of systems for which security controls have been tested and evaluated in the past year. As of 9/17/07		2.c.[18] Number of systems for which contingency plans have been tested in accordance with policy. As of 8/24/07	
		Total #	# Rev.	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
5. OCIO	High	6	3	0	0	6	3	1	17%	0	0%	*N/R	*N/R
	Moderate	14	1	0	0	14	1	7	50%	5	36%	*N/R	*N/R
	Low	7	2	0	0	7	2	2	29%	1	14%	*N/R	*N/R
	Sub-total	27	6	0	0	27	6	10	37%	6	22%	*N/R	*N/R
6. FSA	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	*N/R	*N/R
	Moderate	22	2	0	0	22	2	6	27%	6	27%	*N/R	*N/R
	Low	3	0	0	0	3	0	0	0%	0	0%	*N/R	*N/R
	Sub-total	25	2	0	0	25	2	6	24%	6	24%	*N/R	*N/R
7. AMS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	3	3	0	0	3	3	3	100%	3	100%	0	0%
	Low	16	16	0	0	16	16	16	100%	16	100%	0	0%
	Sub-total	19	19	0	0	19	19	19	100%	19	100%	0	0%
8.ARS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Low	15	15	0	0	15	15	8	53%	8	53%	0	0%
	Sub-total	15	15	0	0	15	15	8	53%	8	53%	0	0%
9.APHIS	High	6	1	0	0	6	1	5	83%	0	0%	0	0%
	Moderate	22	15	1	0	23	15	15	65%	2	9%	5	33%
	Low	9	5	0	0	9	5	3	33%	0	0%	1	20%
	Sub-total	37	21	1	0	38	21	23	61%	2	5%	6	29%

[16] These numbers come from the OCIO as of September 17, 2007, and identified systems that had under gone a C&A. These do not include systems with an Interim Authority to Operate or 86 systems scheduled to undergo a completed C&A by September 30, 2007. For an assessment of the quality of the C&A process, see Question 5.

[17] OIG cannot determine an accurate number of systems that have self-assessments completed. We reviewed self-assessments done in six agencies (APHIS, ARS, AMS, FAS, NRCS, and FNS) and found that all six could not provide documentation of testing on any controls not undergoing the C&A process. Numbers, therefore, are those C&A'd in 2007.

[18] The numbers here are based solely on work performed by OIG for our six selected agencies. *N/R means we did not review that agency.

Bureau Name (OIG Reviewed)	FIPS 199 System Impact Level	Question 1.						Question 2. – Agency Reported					
		1.a. Fiscal Year 2007 Agency Systems. As of 8/6/07		1.b. Fiscal Year 2007 Contractor Systems. As of 8/6/07		1.c. Fiscal Year 2007 Total Number of Systems (Agency and Contractor systems)		2.a[19] Number of systems certified and accredited As of 9/17/07		2.b.[20] Number of systems for which security controls have been tested and evaluated in the past year. As of 9/17/07		2.c.[21] Number of systems for which contingency plans have been tested in accordance with policy. As of 8/24/07	
		Total #	# Rev.	Total #	# Rev	Total #	# Rev	Total #	Percent of Total	Total #	Percent of Total	Total #	Percent of Total
10. FAS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	3	3	0	0	3	3	0	0%	0	0%	3	100%
	Low	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	3	3	0	0	3	3	0	0%	0	0%	3	100%
11. FNS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	7	2	4	1	11	3	11	100%	5	45%	1	33%
	Low	1	1	0	0	1	1	1	100%	0	0%	0	0%
	Sub-total	8	3	4	1	12	4	12	100%	5	42%	1	25%
12. NRCS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Moderate	3	3	0	0	3	3	3	100%	3	100%	3	100%
	Low	0	0	0	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
	Sub-total	3	3	0	0	3	3	3	100%	3	100%	3	100%
13. OCFO-FS	High	0	0	0	0	0	0	N/A	N/A	N/A	N/A	*N/R	*N/R
	Moderate	13	3	0	0	13	3	11	85%	11	85%	*N/R	*N/R
	Low	0	0	0	0	0	0	N/A	N/A	N/A	N/A	*N/R	*N/R
	Sub-total	13	3	0	0	13	3	11	85%	11	85%	*N/R	*N/R
Totals	High	**21**	**10**	**0**	**0**	**21**	**10**	**14**	**67%**	**3**	**14%**		
	Moderate	**135**	**57**	**5**	**1**	**140**	**58**	**72**	**51%**	**41**	**29%**		
	Low	**55**	**41**	**0**	**0**	**55**	**41**	**32**	**58%**	**25**	**45%**		
	Total	**211**	**108**	**5**	**1**	**216**	**109**	**118**	**55%**	**69**	**32%**		

[19] These numbers come from the OCIO as of September 17, 2007, and identified systems that had under gone a C&A. These do not include systems with an Interim Authority to Operate or 86 systems scheduled to undergo a completed C&A by September 30, 2007. For an assessment of the quality of the C&A process, see Question 5.

[20] OIG cannot determine an accurate number of systems that have self-assessments completed. We reviewed self-assessments done in six agencies (APHIS, ARS, AMS, FAS, NRCS, and FNS) and found that all six could not provide documentation of testing on any controls not undergoing the C&A process. Numbers, therefore, are those C&A'd in 2007.

[21] The numbers here are based solely on work performed by OIG for our six selected agencies. *N/R means we did not review that agency.

3. Evaluation of Agency Oversight of Contractor Systems and Quality of 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. (OIG's Response is underlined below.)

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.

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**

Our review showed that agencies that had contractor systems attached to their networks could not provide documentation to validate that sufficient oversight and evaluation activities were in place to ensure information systems used or operated by a contractor of the agency, or other organization on behalf of the agency, met the requirements of FISMA, OMB, and NIST guidelines. This occurred because the Department did not have written policies or procedures in place to provide guidance to the agencies for oversight of contractor systems. In addition, the agencies had not developed written agency policies and procedures for contractor oversight and evaluation. Consequently, the Department cannot be assured of the security over contractor systems.

b. The agency has developed complete 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.

Response Categories:

- **The inventory is approximately 0-50 percent complete**
- **The inventory is approximately 51-70 percent complete**

- **<u>The inventory is approximately 71-80 percent complete</u>**
- **The inventory is approximately 81-95 percent complete**
- **The inventory is approximately 96-100 percent complete**

While OCIO made significant improvements in their oversight of the Departmental inventory records, the process did not include tracking system interfaces or contractor systems. In addition, guidance regarding contractor systems had not been developed and provided to agencies. A review of 14 system security plans revealed that 6 systems interfaced with other systems; however, none of those interfaces appeared within the official Department inventory. System interfaces were not part of the OCIO semi-annual inventory reconciliation process, and therefore were not included in the Department's oversight. In addition, while the semi-annual inventory reconciliation did provide good oversight of overall systems, it did not differentiate between agency owned and contractor systems. As a result, at least one contractor system was not identified as belonging to a contractor in the official Department inventory. Another system was questioned by OIG as to whether it should be a contractor system, but because of the lack of a clear definition, neither the agency nor OIG could make that determination. We considered the system inventory to be accurate. However, we considered the interfaces to be only 25 percent accurate. Therefore, we are assigning inventory with an overall 75 percent completion percentage.

Our review of the Automated Security Self-Evaluation and Remediation Tracking (ASSERT) tool disclosed 10 systems that did not apply the appropriate risk levels to their systems in accordance with Federal guidelines[22]. For instance, one system had two high risk security objectives, yet the system was categorized as moderate. According to Federal guidelines, any security objective that is high defines the system categorization as high. This occurred because Department did not always provide adequate oversight of system categorization. Without a proper risk level assignment, the agencies cannot design their security programs to ensure the appropriate security controls are in place to protect the confidentiality, integrity, and availability of their systems.

c. The IG generally agrees with the CIO on the number of agency-owned systems. <u>Yes</u> or No.

As noted in 3b above, OCIO had made significant improvements in its processes. OIG concurs with the number of systems in the Departmental inventory.

[22] Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated December 2003.

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.

As noted in 3b above, we found a missing contractor system and confusion within the Department as to an accurate definition of a contractor system. Therefore, we could not determine that an accurate inventory of contractor systems existed within the Department.

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

As noted in 3b above, OCIO had made significant improvements in its processes. The Department had been doing a semi-annual review of inventory.

f. If the agency IG does not evaluate the agency's inventory as 96 percent-100 percent complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier associated with the system as presented in your FY 2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.

As noted above, OIG concurs with the total number of systems, but the tracking of interfaces within the inventory system was inadequate. The systems were accurately entered into the inventory system but we had no assurance that a complete listing of interfaces had been documented.

4. Assess whether the agency has developed, implemented, and is managing an agency–wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4a through 4f, select the response categories that best reflects the agency's status. (OIG's Response is underlined 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.

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**

The Department had made improvements in this area. However, it is up to the agencies to accurately input, track, and close POA&Ms. During fiscal year 2007, OCIO began working with the Office of the Chief Financial Officer on a comprehensive process for POA&M closure. This effort concentrated mainly on financial systems within the Department. An essential driver for this process is that actions are undertaken to adequately close the POA&M. To achieve this goal, the Department initiated a Quality Assurance Working Group late in the fiscal year to provide independent verification and validation of documentation submitted to support agency requests to close IT security vulnerabilities. These new actions should improve the POA&M process.

Although improvements have been made, it will take time for the processes to mitigate the issues OIG and the Department have found. OCIO issued a report on June 20, 2007, based on its review of the closure of POA&Ms by several agencies within the Department. Twenty-four POA&Ms were selected from a total of 461 closed from October 1, 2005, to September 30, 2006. OCIO found that the documentation lacked sufficient detail to show that the systemic cause of the POA&M weakness had been corrected. Further, agencies did not maintain support to show that an internal control was placed in operation to prevent recurrence of the weakness, or that the control was sufficiently tested for effectiveness before closing a POA&M.

In addition, our reviews during fiscal year 2007 identified areas where POA&Ms were not being developed and entered into the tracking tool to report known IT security weaknesses. Details are shown below.

- POA&Ms were not added for weaknesses identified during security testing and evaluation performed on 9 of the 10 C&A packages we reviewed.

- All six agencies in our review had not created POA&Ms for identified scanning vulnerabilities that were open more than 30 days as required by Departmental guidance.

- Two agencies did not create POA&Ms as a result of weaknesses identified during OCIO security reviews.

In addition, we reviewed 19 closed POA&Ms during this review and found 5 were closed improperly and 3 had inadequate documentation that the weaknesses had been properly corrected and/or mitigated. Based upon our work during the fiscal year, we have no assurance that agencies were entering, tracking, and adequately closing POA&Ms.

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).

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**

See response to 4a above.

c. Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).

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**

Although the agencies reported their progress on security weakness remediation on a monthly basis, as noted above in 4a, we can give no assurance that the reporting is accurate.

d. Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.

Response Categories:

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

As noted above, OCIO centrally maintains, tracks, and reviews POA&Ms on a monthly basis. In addition, OCIO reviews (on a monthly basis) the status of corrective actions on POA&Ms and any late completion dates are discussed with agency CIOs. However, based on our findings in 4a, we cannot assure that the reporting by the agencies to the Department is accurate. The Department has put significant effort into correcting these deficiencies.

e. IG findings are incorporated into the POA&M process.

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**
- **<u>Almost Always, for example, approximately 96-100 percent of the time</u>**

OCIO made significant improvement determining whether POA&Ms for OIG findings were in the tracking system. Audit findings were tracked in the POA&Ms we reviewed.

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.

Response Categories:

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

As noted in 4a above, OCIO had made progress with regard to financial systems within the Department. However, the POA&M tracking system does not have the capability to prioritize IT weaknesses.

5. Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate. (OIG's Response is underlined below.)

Agencies shall follow NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* dated May 2004, for

certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004, to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

a. The IG rates the overall quality of the Agency's certification and accreditation process.

Response Categories:

-Excellent
-Good
-Satisfactory
<u>-Poor</u>
-Failing

b. The IG quality rating included or considered the following aspects of the C&A process.

(Check all that apply.)

Security plan	X
System impact level	X
System test and evaluation	X
Security control testing	X
Incident handling	X
Security awareness training	X
Configurations/patching	X
Other: Contingency/Disaster Recovery/Risk Assessments	X

C&A process comments:

The Department made improvements in the C&A process. We reviewed 10 C&As and found 1 that met NIST guidance.[23] In addition, we found an improved independent testing and evaluation process. Although improvements were made, we found that the process was still not adequate. Our review of the other nine C&As showed that agencies had not followed NIST guidance. Specifically, we found (1) nine security plans, seven risk assessments, and nine disaster recovery plans that did not follow NIST guidance, and did not provide complete, accurate, and consistent information; (2) three C&As where the processes did not provide adequate assurances that controls were in place and operating

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

effectively; (3) nine systems where controls chosen for continuous monitoring were not documented; and (4) eight systems that were accredited in spite of serious weaknesses. This was caused by a general lack of agency oversight and commitment to security. As a result, not all system controls may have been documented and tested, and systems may be at risk if controls were not implemented effectively.

Also, the Department had implemented a quality assurance program known as a concurrency review to assess agency C&A submissions, prior to accreditation. But based on our review, OCIO concurrency reviews were not providing adequate oversight to ensure that agency system documentation met NIST guidance and that controls were properly safeguarding agency systems and data. We found concurrency reviews were not adequately reviewing agency C&A documentation, denying authority to operate for systems that did not have controls in place to protect the system, and/or performing followup to ensure weaknesses identified during the reviews were mitigated. OCIO stated that it did not have adequate resources to perform concurrency reviews on a large number of Departmental systems in a small amount of time. In addition, concurrency review procedures were in draft. As a result, USDA can not be assured that all system controls have been documented and tested, and systems are operating at an acceptable level of risk if controls were not implemented effectively.

6. IG Assessment of Agency Privacy Program and Privacy Impact Assessment Process

a. Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4, including adherence to existing policy, guidance, and standards. (OIG's Response is underlined below.)

Response Categories:

-Excellent
-Good
-Satisfactory
-<u>Poor</u>
-Failing

Comments:

During fiscal year 2007, OCIO conducted a review of agency Privacy Act documentation. Its review noted that of 215 PIAs, only 98 followed the correct format and provided adequate responses. Of the remaining PIAs, 78 needed corrections and/or additions and 43 did not follow the correct format. In addition, of the 215 PIAs reviewed, 40 systems that indicated personally identifiable information (PII) was present did not have a reference to and/or a published Statement of Record Notice (SORN), as required.

We also reviewed the Privacy Act implementation within the Department and came to a similar conclusion. The Department required a PIA for all systems. We found that in our review of 89 systems, 18 PIAs had not been completed and 8 more were still in draft. Of the 71 PIAs provided and reviewed, 36 did not meet Departmental standards by failing to include required questions.[24] In addition, the content of the PIAs were not always clear and/or information was contradictory regarding the usage of PII in those systems. If PII information is in the system, a SORN was to be published in the Federal Register for any new or intended use of personal information. We found that 11 of 38 required SORNs had not been published. Finally, of 8 Privacy Act Officers interviewed, none were aware of key requirements such as formulating policy, handling privacy incidents, and/or analyzing business flows for privacy implications.

b. Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, *Safeguarding Personally Identifiable information,* since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect PII.

Response Categories:

-Excellent
-Good
-Satisfactory
-Poor
-<u>Failing</u>

Comments:

The Department had taken some steps to implement the provisions of OMB Memorandum No. M-06-15, but had yet to fully achieve that goal. One positive step taken was the recent granting of a blanket purchase agreement to encrypt mobile devices with a planned completion date of March 31, 2008. Until this is fully implemented, the Department is very susceptible to PII incidents as noted by the 50 such incidents which occurred during the fiscal year. In addition, some legacy systems within the Department use the social security number as the key component. We also found that there were at least 181 unencrypted wireless access points within the Department, which could potentially broadcast PII in clear text.[25]

[24] Departmental Manual (DM) 3515-002, *Privacy Impact Assessment*, dated February 17, 2005.

[25] In computer networking, a wireless AP is a device that connects wireless communication devices together to form a wireless network. The AP usually connects to a wired network, and can relay data between wireless devices and wired devices. APs had Internet Protocol addresses for configuration.

7. Configuration Management

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

Comments:

An adequate Departmental configuration policy did not exist with checklists for each operating system. To determine the level of security and configurations within the Department, we scanned six agencies' networks using commercially available software to look for known security vulnerabilities. In addition, we reviewed the level of security software patches that were applied at seven agencies. We found that (1) over 700 high risk vulnerabilities[26] were present and unmitigated or the acceptance of risk was not documented, and (2) over 240,000 patches were not applied to over 26,000 devices. We also reviewed the running configurations of network routers, switches and firewalls at six agencies using commercially available software. Our review disclosed over 900 configuration errors within those agencies' devices. In addition, we noted that some of these agencies had stated in their July 2007 scorecard that they were 100 percent patched and scanned. Agencies were not reporting their accurate security posture in the scorecards and OCIO was not validating the information when received.

b. Approximate the extent to which applicable information systems apply common security configurations established by NIST.

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**

NIST guidance states that "while the solutions to IT security are complex, one basic yet effective tool is the security configuration checklist."[27] The Department had issued guidance to achieve this NIST requirement.[28] It issued checklists for some operating systems which it required agencies to use on a yearly basis. We reviewed six agencies to determine whether the Department's standard checklist for configuring systems were being used. We found that checklists were not being used to configure the systems in four of six

[26] High risk vulnerabilities are those which provide access to the computer, and possibly the network of computers.

[27] NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers,* dated December 2006.

[28] DM 3540-002, *Risk Assessment and Security Checklists,* dated April 19, 2004.

agencies and they could not provide documentation to support why the checklists were not used. In addition, checklists were not available to the agencies until August 2007 because they had been removed from the website and OCIO could not locate them. Fortunately, OIG was able to provide copies from our previous audit work. Also, as noted in the fiscal year 2006 FISMA audit report, not all checklists had been created. As a result, USDA systems were vulnerable to many threats, ranging from remotely launched network service exploits to malicious code spread through e-mails, malicious web sites, and file downloads.

8. Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to United States Computer Emergency Readiness Team (US-CERT), and to law enforcement. 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. Yes or <u>No</u>.

b. The agency follows documented policies and procedures for external reporting to US-CERT. Yes or <u>No</u>. (http://www.us-cert.gov)

c. The agency follows documented policies and procedures for reporting to law enforcement. Yes or <u>No</u>.

Comments:

OCIO made progress in tracking incident responses. During the fiscal year it implemented the Cyber Security Incident Response Management database to facilitate tracking and closeout of incidents. The database tracks the ticket number, open and close dates, categories of incidents, PII information, and whether the incident was forwarded to other Federal agencies. However, we found policies and procedures for incident handling were not being followed and that incidents were not closed properly, timely, or reported to necessary authorities. As a result, OCIO had limited assurance that improper actions were being appropriately and timely handled and that security problems were being adequately addressed. We reviewed the incident tracking database and found 92 of the 399 incidents did not have documented closure within 30 days and that 75 incidents did not have US-CERT numbers (agency officials stated that these were mainly false positives). However, our review found that they should have been reported based on the US-CERT category in the database. In addition, we found over 100 incidents that had not been reported to OIG, as required by Departmental guidance, because OCIO did not have a standard distribution list.[29]

[29] DM 3505-001, *Incident Response Procedures*, dated March 20, 2006.

Internet Protocol Address Database (IPAD) is vital to the timeliness of incident response. IPAD is the Department's internet protocol (IP) address repository. This tool is used to determine the agency and location of the device when an incident occurs. It includes agency contact information, and whether PII is present on that system. Although the OCIO had made progress in the implementation of IPAD, more work is needed. We found that IPAD still did not have a complete and accurate listing of USDA IP addresses in the Department's tracking database for three out of the six agencies reviewed. This was due to a lack of management commitment to monitor IPAD to ensure that a complete and accurate inventory of IP addresses was maintained.

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

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

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

11. The agency has completed system e-authentication risk assessments. Yes or No.

We reviewed e-authentication risk assessments, required by OMB, at six agencies.[30] We found one agency that did not use e-authentication. For the remaining, only one could provide documentation to show it had conducted an assessment. The agencies were either unaware that a separate risk assessment was required or were not aware of a requirement to keep the documentation. Without doing and/or documenting a risk assessment for e-authentication there is no assurance that business transactions have the required level of verification for authentication. Authentication risks with potentially higher consequences require higher levels of assurance.

[30] OMB Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, dated December 16, 2003.