



U.S. Department of Agriculture



Office of Inspector General  
Financial & IT Operations

# Audit Report

## Fiscal Year 2004 Federal Information Security Management Act Report

Report No. 50501-1-FM  
October 2004

---



UNITED STATES DEPARTMENT OF AGRICULTURE



OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: OCT - 6 2004

REPLY TO  
ATTN OF: 50501-1-FM

SUBJECT: Fiscal Year 2004 Federal Information Security Management Act Report

TO: Scott Charbo  
Chief Information Officer  
Office of the Chief Information Officer

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

Your response to our draft report is included in its entirety as exhibit B, with excerpts incorporated in the findings and recommendations section of the report. Based on the information in your response, we have reached management decision for Recommendation No. 2. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer. For Recommendation No. 1, additional actions are needed to reach management decision. Please refer to the OIG Response section of the report for specific details.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation of the outstanding recommendation noted above. Please note that the regulation requires management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

The courtesies and cooperation extended to the auditors during our security audits are appreciated.

Phyllis K. Fong  
Inspector General

# ***Executive Summary***

## ***Fiscal Year 2004 Federal Information Security Management Act Report***

---

### **Results in Brief**

This report presents the results of our audit of the Department's efforts to improve the management and security of its information technology (IT) resources. Fieldwork for this audit was performed at the Department Office of the Chief Information Officer (OCIO) and three selected agencies. In addition, we included the results of (1) IT control testing performed by contract auditors at three additional agencies, (2) our most recent application control reviews, and (3) our general controls reviews at the Department's two data centers. In total, our report is based on our reviews at 12 agencies conducted from October 2003 through August 2004. The OCIO annually reports on compliance with the Federal Information Security Management Act (FISMA) as of September 30 and, in some cases such as computer security awareness training and system certification and accreditation, completes, or documents the completion of, a significant amount of the required actions in the month of September. As such, the Department and its agencies may have implemented controls or completed corrective actions that, due to the timing of our fieldwork, may not be reflected in this report.

Historically, U.S. Department of Agriculture (USDA) agencies and departmental staff offices have independently addressed their respective IT security and infrastructure needs. This resulted in a broad array of technical and physical solutions that did not provide assurance that Department-wide security was obtained. The efforts of 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 IT security. The Department and its agencies should be commended for their efforts during the year toward completion of the certification and accreditation of their systems; however, we still found significant weaknesses in the Department's security program that can be attributed to management's lack of commitment to implementing an effective security program within their respective agencies. USDA management must remain involved and committed toward implementing an effective security program within the Department. Both the OCIO and OIG reported the lack of agency management involvement as a material weakness in prior FISMA<sup>1</sup> reports. This is the third year we have reported this issue as a material weakness. Agency managers are ultimately responsible and should be held accountable for committing the appropriate resources to ensure compliance.

The Department and its agencies have made progress in addressing the lack of compliance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, but weaknesses continue to exist. Specifically, OIG

---

<sup>1</sup> FISMA superseded the Government Information Security Reform Act that expired in November 2002.

found that (1) the Department was still unable to produce a reliable inventory of applications and general support systems, (2) not all documents produced through the agencies' certification and accreditation processes complied with OMB and other Federal requirements, and (3) a significant majority of the Department's applications were not certified until near the end of the fiscal year.

Despite the Department's site license for vulnerability scanning software and a formal scanning policy, the agencies have not been timely in identifying and correcting known and exploitable vulnerabilities in their systems. The agencies we reviewed cited varying reasons for not performing vulnerability scans, including a lack of training and guidance on how to use the tools, and a lack of formal policies and procedures in place to periodically use the tools and mitigate the identified vulnerabilities. As a result, significant vulnerabilities go undetected and uncorrected, increasing the risk that attackers, both internal and external, could compromise mission-critical IT resources and data.

Further, we again identified access control weaknesses in every agency reviewed. This occurred because agencies did not have policies and procedures 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. We also found inadequate controls over the physical access to computer systems and critical network components in 6 of the 12 agencies reviewed. As a result, there is reduced assurance that agencies can effectively protect their mission-critical systems and data from unauthorized modification, disclosure, loss, or impairment.

Finally, in the past several years, OCIO has strengthened its oversight of agencies' security programs; however, improvements could be made which would significantly strengthen the Department's security posture. Specifically, OCIO needs to (1) formalize its tracking system for USDA cyber security incidents to ensure timely followup and resolution, and (2) increase the number and frequency of its agency reviews. We found that OCIO's current method of tracking security incidents is not effective in ensuring that agencies timely and adequately followup on security incidents. Further, despite continual requests for additional resources, OCIO acknowledges that it has not had the significant resources it needs to increase its review and enforcement efforts over agencies' security programs. Despite its efforts over the past several years, OCIO's inability to strengthen its oversight and enforcement role has hindered its ability to effectively manage the Department's security program.

**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 are made in agency reports. Therefore, we are not making additional recommendations related to those conditions in this report. We have, however, recommended that the OCIO (1) establish guidance in identifying systems within the Department and its agencies; and (2) implement a formal tracking system for cyber security incidents to ensure the timely followup, resolution, and reporting of those incidents.

**Agency Response**

OCIO agreed with many of the findings and one recommendation in the report. OCIO disagreed with OIG's methodology of preparing this report, which uses the results of its audits conducted throughout the year without acknowledging the final set of achievements made at year-end. OCIO acknowledged that security weaknesses continue to exist, but stated that action plans are being developed to eliminate these weaknesses. Such actions will continue throughout the coming year. OCIO's response to the official draft has been included in its entirety as exhibit B of this report.

**OIG Position**

OIG recognizes that differences will occur due to the methodologies used in preparing the two reports. However, the scope of our audit and the time needed to effectively evaluate the status of the Department's security program do not allow us to perform extensive audit work at fiscal year-end. OIG further recognizes that achievements were made during the last month of the fiscal year and that OCIO and the agencies have plans to continue their efforts in improving the Department's IT security position.

## ***Abbreviations Used in This Report***

---

AMS	Agricultural Marketing Service
APHIS	Animal and Plant Health Inspection Service
BIA	Business Impact Analysis
CCC	Commodity Credit Corporation
CIO	Chief Information Officer
CSREES	Cooperative State Research Education and Extension Service
DA	Departmental Administration
DR	Departmental Regulation
FIPS	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FISCAM	Financial Information System Control Audit Manual
FSA	Farm Service Agency
FS	Forest Service
FSIS	Food Safety and Inspection Service
FY	Fiscal Year
GAO	Government Accountability Office (formerly the General Accounting Office)
GISRA	Government Information Security Reform Act
GSS	General Support System
HSPD	Homeland Security Presidential Directive
ISSPM	Information System Security Program Manager
IT	Information Technology
IG	Inspector General
LAN	Local Area Networks
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
NRCS	Natural Resources Conservation Service
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OIG	Office of Inspector General
PED	Personal Electronic Devices
PKI	Public Key Infrastructure
POA&M	Plan of Actions and Milestones
RMA	Risk Management Agency
SP	Special Publication
TCP/IP	Transmission Control Protocol/Internet Protocol
US-CERT	United States Computer Emergencies Readiness Team
USDA	U.S. Department of Agriculture

# Table of Contents

---

<b>Executive Summary</b> .....	<b>i</b>
<b>Abbreviations Used in This Report</b> .....	<b>iv</b>
<b>Background and Objectives</b> .....	<b>1</b>
<b>Findings and Recommendations</b> .....	<b>4</b>
<b>Section 1. Management Commitment Needed for an Effective Security Program</b> .....	<b>4</b>
Finding 1    Management Involvement and Commitment is Needed to Ensure a Successful and Effective Security Program .....	4
<b>Section 2. OMB and FISMA Compliance</b> .....	<b>7</b>
Finding 2    Progress is Made, but Noncompliance with Federally Mandated IT Security Requirements Continues .....	7
Recommendation No. 1.....	13
Finding 3    Agencies Are Not Vigilant in Identifying and Mitigating System Vulnerabilities .....	14
Finding 4    Access Controls Continue to be a Significant Weakness in the Department.....	15
Finding 5    Improvements in OCIO’s Oversight Role would Benefit the Department .....	17
Recommendation No. 2.....	20
<b>Scope and Methodology</b> .....	<b>21</b>
<b>Exhibit A – OMB Reporting Requirements and OIG Position</b> .....	<b>22</b>
<b>Exhibit B – OCIO’s Response to the Draft Report</b> .....	<b>37</b>

# ***Background and Objectives***

---

## **Background**

Improving the overall management and security of information technology (IT) resources should be 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 (P.L. 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 the OCIO's progress in establishing a Department-wide security program;

- assessing the corrective action taken by selected agencies on previously identified control weaknesses; and
- evaluating the agency and OCIO's Plan of Actions and Milestone (POA&M) consolidation and reporting process.

# **Findings and Recommendations**

## **Section 1. Management Commitment Needed for an Effective Security Program**

---

### **Finding 1**

#### **Management Involvement and Commitment is Needed to Ensure a Successful and Effective Security Program**

While progress has been made, we have reported for the third year in a row that agency management needs to demonstrate involvement and commitment to ensure the ultimate success of their security programs. We believe that this lack of involvement and commitment continues to be a material weakness in achieving an effective security program within the Department, and remains an impediment to ensuring that its security programs are adequately designed and properly carried out. The Department and its agencies should be commended for their efforts during the year toward completion of the certification and accreditation of its systems; however, we still found significant weaknesses in the Department's security program that can be attributed to management's lack of commitment to implementing an effective security program within their respective agencies. Specifically, they cannot ensure compliance with OMB Circular A-130 requirements (see Finding No. 2) that security vulnerabilities are timely identified and mitigated (see Finding No. 3), and that adequate physical and logical access controls are in place (see Finding No. 4). These requirements are longstanding and the lack of adherence has been reported previously by the Office of Inspector General (OIG). Agency managers are ultimately responsible and should be held accountable for committing the appropriate resources to ensure compliance.

NIST Special Publication (SP) 800-12 states that, "A natural tension often exists between computer security and operational elements. In many instances, operational components – which tend to be far larger and therefore more influential – seek to resolve this tension by embedding the computer security program in computer operations. The typical result of this organizational strategy is a computer security program that lacks independence, has minimal authority, receives little management attention, and has few resources. As early as 1978, the Government Accountability Office (GAO) identified this organizational mode as one of the principal basic weaknesses in Federal agency computer security programs."

Departmental Regulation (DR) 3140-1, "USDA Information System Security Policy," dated May 15, 1996, states that agencies should assign the Information System Security Program Manager (ISSPM) to a level within the organization that can independently report to the appropriate program and/or departmental officials. The ISSPM must be able to assure security across the

entire agency's programs. Further, OMB Circular A-123, "Management Accountability and Control," dated June 21, 1995, requires agencies to ensure that appropriate authority, responsibility, and accountability are defined and delegated to accomplish the mission of the organization, and that an appropriate organizational structure is established to effectively carry out program responsibilities.

During the fiscal year, the Department's CIO implemented a Department-wide initiative to certify and accredit all major applications and general support systems (see Finding No. 2), a major component of compliance with OMB Circular A-130, Appendix III. While this effort is far from complete, the Department's accomplishments in this effort might not have been obtained if left solely to the discretion of individual agency management. Despite the longstanding requirements of OMB Circular A-130, agency managers have been reluctant to comply without the guidance and emphasis of the Department's CIO.

Last year we reported a common symptom of a lack of management involvement was that agency security personnel have not been given the authority needed to effectively implement and manage their agency's security programs. Our followup reviews in fiscal year 2004 continue to show that agency security personnel alone have not been able to ensure compliance with Federal IT security guidelines. The same weaknesses we previously reported, such as access control weaknesses and vulnerability mitigation, still existed in all 12 agencies. In addition, despite our recommendations, some agencies have not realigned their CIOs and ISSPMs within their organizations or emphasized their oversight and enforcement authority sufficient to implement the agency's security program. The following examples illustrate some of the continued weaknesses we identified.

- Our review at one agency found material internal control weaknesses in the area of access controls and application change controls for the second year in a row. While the agency took action to correct the specific problems we identified, it failed to address the underlying internal control weakness. Further, despite our recommendations, the agency had not taken sufficient actions to address the weaknesses we identified in its organizational structure and oversight of contractor personnel.
- The CIO for another agency lacked the authority to ensure that the agency's security program was operating effectively. Specifically, the CIO was unable to (1) provide us a list of users on all agency systems, (2) identify all contractors and whether or not they received security-related training, or (3) identify all staff within the agency that had significant IT security responsibilities. Further, the CIO was not aware that a POA&M had been completed for one of the agency's systems.

Unlike the other issues in this report, we do not believe the weakness in this finding can be corrected by policy or guidance issued by the Department OCIO. Only after agency managers demonstrate their commitment to ensuring compliance with OMB Circular A-130 and other federally mandated security guidelines, will an effective Department-wide security program be achieved. The issues raised in this report have been reported in specific agency reports. Therefore, we make no additional recommendations herein.

## **Section 2. OMB and FISMA Compliance**

---

The Department and its agencies have made significant progress toward accomplishing compliance with OMB Circular A-130 and other federally mandated security requirements; however, not all of the Department's agencies were fully compliant. This is our fourth report in 4 years where we have reported this weakness, and the third year that we have noted that management involvement and commitment remains a material weakness toward ensuring compliance and improving IT security. Management's challenge is to ensure that every IT system deployed and managed by the Department complies with major security disciplines required by Federal law and guidance. While most agency security staffs have done what they can, many of the issues we raised will not be corrected until agency management commits the needed resources. The Department heavily relies on hundreds of information systems operated within USDA to deliver its programs and meet its missions. The weaknesses we continue to report jeopardize the confidentiality, integrity, and availability of these resources.

---

### **Finding 2**

#### **Progress is Made, but Noncompliance with Federally Mandated IT Security Requirements Continues**

The Department and its agencies have made progress in addressing the lack of compliance with OMB Circular A-130, Appendix III, but weaknesses continue to exist. Specifically, we found that (1) the Department was still unable to produce a reliable inventory of applications and general support systems (GSS), (2) not all documents produced through the agencies' certification and accreditation processes complied with OMB and other Federal requirements, and (3) a significant majority of the Department's applications were not certified until near the end of the fiscal year.<sup>2</sup> OIG continues to identify weaknesses within the agencies and the lack of management's demonstrated commitment and involvement remains a key barrier to compliance (see Finding No. 1). Agency managers are ultimately responsible for ensuring that their agencies comply with laws and regulations governing IT management and security. The fact that these weaknesses have been reported for 4 years indicates that management has not yet established adequate controls or committed the appropriate resources to ensure compliance. The Department and its agencies rely on their IT infrastructures and systems to issue billions of dollars in payroll, loans, and entitlement benefits; supply market-sensitive data on commodities to the agricultural economy; and manage consumer protection programs. The Department's

---

<sup>2</sup> The fact that most agencies did not have certification and accreditation in place for a majority of the fiscal year makes them, as a whole, materially non-compliant with OMB A-130 for the fiscal year.

ability to accomplish its mission could be jeopardized if it does not properly manage and secure its IT infrastructure.

The foundation for security over IT resources is found in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." This Circular establishes a minimum set of controls for agencies' automated information security programs, including certifying to the security of any systems that maintain sensitive data; establishing contingency plans and recovery procedures in the event of a disaster; providing security awareness training to employees and contractors; and establishing a comprehensive security plan. Homeland Security Presidential Directive (HSPD) – 7, "Critical Infrastructure Identification, Prioritization, and Protection," dated December 17, 2003, requires agencies to identify, prioritize, assess, remediate, and protect their internal critical infrastructure and key resources.

In December 2002, FISMA<sup>3</sup> permanently reauthorized the framework laid out in the GISRA which expired in November 2002, and establishes NIST as the authority for establishing technical guidance for the Federal Government. OMB guidance for implementing these laws lays out a framework that contains timeframe requirements and procedures for annual IT security reviews, reporting, and remediation planning for Federal agencies.

#### Inventory of Applications and General Support Systems

The Department still does not have a reliable inventory of applications and GSS from which to manage Department-wide IT security. The Department relies on agencies to provide a comprehensive list of their major applications and GSS systems; however, the OCIO has been unable to verify the accuracy or reliability of those agency-provided inventories. As a result, the OCIO cannot be assured that all systems are properly accredited. Further, we question how the OCIO can properly manage a Department-wide security program without an accurate inventory of all agency applications and GSS systems.

As part of its Year 2000 conversion efforts, the Department identified a list of mission-critical applications. OCIO officials acknowledged that this initial list was incomplete mainly due to the lack of understanding across all agencies of what constituted a "system." In fiscal year 2004, in preparation for our nationwide audit for application controls, we selected seven systems from the OCIO's list of major applications dated December 2003. Our review disclosed that three of the seven applications we selected were scheduled to be replaced or would no longer be used by the end of the fiscal year, one application was in the initial stages of development and therefore not far enough along for the certification process, and one system was an ad hoc database containing historical data no longer used by the agency but

---

<sup>3</sup> The Electronic Government Act, Title III, signed into law December 17, 2002.

“scheduled” to be brought back on-line sometime during the year. Further, we noted that between December 2003 and August 20, 2004, OCIO provided us with at least 4 different lists of systems or certification progress updates showing the total number of departmental systems ranging between 594 and 460. OCIO officials acknowledged that the Department’s inventory of systems had evolved throughout the year, and will continue to do so; however, officials informed us that through their work with the agencies during the certification and accreditation process, the current list of departmental systems represents an improvement over prior efforts.

While we agree that OCIO’s current list of systems provides a starting point, we believe that the errors we found support the need to have a well-established definition of “system” and reasonable assurance that agencies are reporting their systems in accordance with that definition. Further, we believe that the OCIO needs to be fully aware of all applications and GSS that reside on the Department’s network to ensure that agencies are in compliance with OMB and FISMA requirements, and to effectively manage its security program.

#### Risk Assessments

Agencies reviewed during fiscal year 2004 had not adequately assessed the risk to their mission-essential IT resources. OMB A-130 requires a risk-based approach to security and consistent with FISMA, HSPD – 7 requires agencies to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Additionally, according to NIST SP 800-34, business impact analysis (BIA) helps to fully characterize system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The BIA’s purpose is to correlate specific system components with the critical services they provide, and based on that information, to characterize the consequences of a disruption to the system components. Hence, the BIA needs to be completed to aid in the adequate completion of various certification and accreditation documents.

One agency we reviewed performed risk assessments for only two of its seven mission-critical systems. Further, one of the two risk assessments had very little detail and followed, generically, the outline suggested in NIST guidance. The agency’s CIO informed us that the various divisions of the agency maintained their own systems and the CIO did not have the resources or enforcement authority over those divisions to ensure compliance with Federal guidelines. Based on the results of our audit, the certification and accreditation documents produced by the agency’s contractor were sent back for revisions.



Two other agencies did not evaluate their security policies based on the identified risks, nor had they taken any actions to eliminate or otherwise mitigate the identified risks. Agency officials informed us that a different contractor prepared its risk assessments, and that agency officials did not ensure that the information was communicated to the contractor preparing the security plan.

### Security Plans

Agencies still had not prepared all required security plans, or ensured that the plans adequately addressed all requirements of OMB Circular A-130 and other Federal security guidance. OMB requires agencies to prepare a security plan to provide an overview of the security requirements of their major applications and GSS. Security plans should define who has responsibility for system security, who has authority to access the system, appropriate limits on interconnectivity with other systems, and security training of individuals authorized to use the system.

One of the agencies we reviewed had not completed security plans for its telecommunications network, which included its routers, firewalls, and intrusion detection system. OMB requires security plans for GSS since these systems provide interconnectivity among systems and provide the first level of security controls to protect the confidentiality, integrity, and availability of other systems. In many cases, the GSS provides the only security for non-critical applications. The agency recognized that these actions need to be completed and has identified them in its POA&Ms. Agency officials stated that meeting the requirements involves major effort and requires time and resources to comply thoroughly.

At another agency, we found that the agency had accepted inadequate security plans from its contractor. We found that the agency had recently made significant changes to its GSS; however, the security plan provided by the contractor did not (1) reflect the current operating environment, (2) identify the system owner, or (3) identify the security officer responsible for the system. At a third agency, the security plans lacked essential information such as interconnectivity with other systems, physical security standards and enforcement, and the training requirements necessary for the users of the system.

Until security plans are completed for all major applications and GSS, the Department cannot be assured that it has adequately addressed its security needs and that its security policies and practices have become an integral part of its operations.

## Contingency/Disaster Recovery

Agencies we reviewed had not prepared contingency and disaster recovery plans, or ensured that their disaster recovery plans were executable. Despite the longstanding requirement in OMB Circular A-130 that agencies prepare and test contingency plans, agencies still have not addressed this critical step. OMB also states that contingency plans should be tested, as untested or outdated contingency plans create a false sense of the ability to recover in a timely manner. NIST SP 800-12, “An Introduction to Computer Security,” Section 11.6, states a contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. Furthermore, the plan will become dated as time passes and as the resources used to support critical functions change. Additionally, NIST<sup>4</sup> requires a BIA to help fully characterize system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The BIA’s purpose is to correlate specific system components with the critical services they provide, and based on that information, to characterize the consequences of a disruption to the system components.

One agency had prepared a contingency plan for only one of its seven major applications, and this plan had not been tested. Even though this agency’s systems affected the safety of all Department employees, the agency did not consider disaster recovery planning a priority. Furthermore, the agency had not planned on testing its one disaster recovery plan because it believed that the Department’s CIO was responsible for conducting this testing.

Our review of one major application contingency plan at another agency found that the agency had begun to identify and prioritize critical data and operations, determine the resources needed to support those operations, and establish emergency priorities. However, we found that the agency’s staff had not been trained in how to implement the contingency plan in the event of an emergency. Further, the contingency plan we reviewed was still under development because the BIAs had not been finalized and reviewed by management.

Three agencies did not have disaster recovery plans in place that were sufficiently comprehensive to ensure adequate recovery of their applications in the event of a major disruption. Agency officials indicated that they were relying on the certification and accreditation process to ensure that their contingency and disaster recovery plans were adequately tested.

Without effective, executable plans for the Department’s major applications and GSS, it cannot be assured that it will be able to continue delivery of its programs and meet its missions. Department CIO officials informed us that

---

<sup>4</sup> NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems,” dated June 2002.

they are planning an initiative to assist agencies in the preparation and testing of contingency and disaster recovery plans.

### System Certification, Accreditation, and Authorization

At the time of our fieldwork, the agencies we reviewed had not completed system certifications and accreditations on their major applications or GSS. Agencies' officials have informed us that they are completing the certifications in accordance with the Department's directives and intend to have this process completed by September 30, 2004.<sup>5</sup> This process, required by OMB Circular A-130 and emphasized in NIST SP 800-37,<sup>6</sup> requires agencies to (1) document significant security controls within the system, (2) perform an independent accreditation of the effectiveness of those controls, and (3) formally approve, with signature authority by program management, use of the system in the production environment. Despite the longstanding requirement by OMB to complete this certification and accreditation process prior to system implementation, the requirement has been largely ignored and not enforced. Department CIO officials have informed us that they are committed to ensuring that the certification and accreditation process is fully implemented into every agency's system development lifecycle process.

### Security Awareness and Training

We found that agencies had processes and resources in place to provide their employees with security awareness training, and that system and network administrators have a means to acquire specialized training relating to their responsibilities; however, they had not established adequate controls to ensure all employees received the necessary training. OMB Circular A-130 requires agencies to ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system, and that persons with significant responsibilities over systems be provided training commensurate with their responsibilities. Further, DR-3140-1 states agency security programs are to ensure that all employees and contractors receive annual security awareness training. While all agencies we reviewed had offered some type of training related to security, the agencies did not ensure that every employee received the training. For example:

- In one agency, we found that only about 51 percent of the employees took security awareness training. Additionally, the agency could not provide an up-to-date listing of contractors, contractor training, or contractor background checks because no controls had been put into place to track these individuals.

---

<sup>5</sup> OCIO Officials have revised the target date for completing certification and accreditation to the end of calendar year 2004.

<sup>6</sup> NIST SP 800-37, dated May 2004, replaced Federal Information Processing Standards Publication (FIPS) 102, "Guidelines for Computer Security Certification and Accreditation," dated September 27, 1983. FIPS 102 discusses these issues in Sections 1.5.2, 2.7, and 2.7.3.

- Another agency provided a list of 351 system administrators, but could produce documentary support that only 65 had received specialized training relating to their responsibilities. While the agency recognized the need for specialized training for its system administrators, the agency made the training voluntary rather than mandatory.

The Department established an enterprise-wide security awareness-training program through which all agencies have participated. This system allows agencies to track those individuals that have received the required training. Since most agencies within the Department emphasize the need for this training toward the end of the fiscal year we have not validated whether all agencies have completed this training for the current year.

Despite the significant emphasis placed on certification and accreditation, the Department and its agencies still have significant progress to make before it has fully complied with OMB and other Federal IT security requirements. It is OIG's opinion that the progress made to date would not have occurred without the commitment of the Department's OCIO. However, as reported elsewhere in this report, agencies are ultimately responsible for the security and management of their IT resources, and agency management needs to ensure compliance with laws and regulations through the commitment of the necessary resources.

Most of the issues we raised have been reported in agency-specific reports and therefore we make no additional recommendations on those issues. However, to better determine the total number of systems within the Department, we are recommending that the OCIO, in consultation with the agencies, define "system" for the Department and ensure that agencies report and track systems under their control.

## **Recommendation No. 1**

The OCIO should establish guidance in identifying systems within the Department and its agencies.

**Agency Response.** OCIO stated that it challenged agencies, during the fiscal year's certification and accreditation effort, to develop sound inventories of their systems. Throughout the certification and accreditation effort, adjustments to systems inventory occurred due to contract expertise establishing the appropriate scope for testing, as well as combining like systems and elimination of others that have been or soon will be replaced. OCIO stated that this constant attention throughout the year has resulted in a sound listing of all USDA major and non-major applications and general support systems. OCIO expects the systems inventory to be a baseline and not static.

**OIG Position.** OIG recognizes that an inventory of systems is not static and will change as new systems are developed and old ones are no longer needed. However, defining and inventorying systems has been a problem within USDA since its initial effort during the year 2000 conversion process. OMB's definition of a system in Circular A-130, Appendix III, has been broadly interpreted and not consistently applied within the agencies of the Department. Without clear and definite guidance from OCIO, the agencies will continue to inconsistently apply the definition of a system and make the Department's inventory of systems only marginally effective in managing the Department's security program. In order to reach management decision, the OCIO must provide us with how it will ensure that the Department and its agencies will consistently apply OMB's definition of a system and ensure compliance by the agencies.

---

### Finding 3

#### **Agencies Are Not Vigilant in Identifying and Mitigating System Vulnerabilities**

Despite the Department's site license for vulnerability scanning software and a formal scanning policy, the agencies have not been identifying and correcting known and exploitable vulnerabilities in their systems in a timely manner. The agencies we reviewed cited varying reasons for not performing vulnerability scans, including a lack of training and guidance on how to use the tools, and had no formal policies and procedures in place to periodically use the tools and mitigate the identified vulnerabilities. As a result, significant vulnerabilities go undetected and/or uncorrected, increasing the risk that attackers, both internal and external, could compromise mission-critical IT resources and data.

OMB Circular A-130 requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce the threat or amount of potential loss. Departmental guidance requires agencies to keep an inventory of their network, to perform monthly network scans, and to develop and implement corrective action plans to address critical vulnerabilities. In addition, DR-3140 establishes policies to ensure comprehensive security programs are in place to safeguard all information IT resources.

Eleven of the twelve<sup>7</sup> agencies we reviewed had failed to establish effective controls to identify and mitigate vulnerabilities in their systems as required by Department policy in a timely manner. In 2001, the Department, based on our audit results, purchased a Department-wide license for a commercially

---

<sup>7</sup> One agency had established effective controls over its own scanning process.

available vulnerability scanning software tool. The tool identifies vulnerabilities exploitable in operating systems that use Transfer Control Protocol/Internet Protocol, the protocol used on the global Internet, and categorizes vulnerabilities into high, medium, and low-risk.<sup>8</sup> Some agencies we reviewed scanned their systems once every few months but not on a consistent basis, other agencies scanned their systems using one of the software's built-in policies that does not identify all known vulnerabilities that can be exploited by attackers, and other agencies failed to scan critical components of their networks such as their routers and firewalls.

As we reported last year as well, many of the vulnerabilities we discovered were not caused by poorly written software or the operating system, but rather carelessness by agency personnel to assign strong passwords to system accounts, or failure to properly configure systems settings to ensure secure operations. For instance, at one agency we found nearly 50 high and medium-risk vulnerabilities on one server alone. We later found that the IT staff had connected a development system to the production network that had not been properly configured or "hardened."

The issues raised in this report have been reported to the Department's OCIO and in specific agency reports. Therefore, we make no additional recommendations herein.

---

#### **Finding 4**

#### **Access Controls Continue to be a Significant Weakness in the Department**

We again identified access control weaknesses in every agency reviewed. This occurred because agencies did not have policies and procedures in place to (1) remove user accounts when no longer needed in a timely manner, (2) periodically reconcile user accounts to current employees and contractors, and (3) assign users only those permissions needed to perform their job responsibilities. We also found inadequate controls over the physical access to computer systems and critical network components in 6 of the 12 agencies reviewed. As a result, there is reduced assurance that agencies can effectively protect their mission-critical systems and data from unauthorized modification, disclosure, loss, or impairment.

NIST SP 800-12, "Introduction to Computer Security," states that effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication,

---

<sup>8</sup> High-risk vulnerabilities are security issues that allow immediate remote or local access, or immediate execution of code or commands with unauthorized privileges. Medium-risk vulnerabilities are security issues that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures. Low-risk vulnerabilities are security issues that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not directly gain unauthorized access.

and access authorizations. The process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations augments this. Finally, system administrators should timely modify or remove access for employees who are reassigned, promoted, or terminated or who retire. Both OMB and NIST require physical access controls that restrict the entry and exit of personnel from the area, such as the office building, suite, data center, or room containing a local area network (LAN) server. Physical access controls guard against theft, disablement, or other modification of network hardware that could lead to the loss of critical data that reside on that hardware. Physical access controls (such as locked server room doors) ensure that only authorized personnel can physically handle and perform maintenance on network servers and other critical network hardware.

### Physical Access

We found physical access control weaknesses in 6 of the 12 agencies reviewed. At one agency, we found an inadequate process was in place to reconcile computer room access records maintained by the Office of Operations with agency records. According to Office of Operation access records, 70 people had physical access to the room where critical systems were located. Agency records indicated only 24 individuals had authorized access to the computer facility, and 8 of those 24 individuals were no longer employed by the agency. Additionally, agency personnel were unable to identify 48 of the 70 people shown by the Office of Operations to have access to the agency computer room.

Another agency, which conducts oversight reviews of private-sector companies, allowed its computer systems to be left unattended for long periods of time in unsecured places. This allowed unauthorized users, including persons subject to the agency's oversight, to access these systems and potentially modify application data without being detected.

### Logical Access

In all of the 12 agencies reviewed, we identified logical access control weaknesses. The agencies did not have formal procedures established to timely remove users that no longer needed access to their systems, or ensure that access is restricted to data that employees need to perform their job functions. Logical access controls such as user names, passwords, and access permissions ensure that only authorized users have access to network resources from across the network, and that users are granted only the access that is needed to conduct their job responsibilities. In today's global network environment, strong access controls help ensure that malicious users, both internal and external to the agency's network, do not gain access to critical data. The following describes some of the logical access control weaknesses identified.

- We found that one agency (1) had not configured its systems to limit access to sensitive files to only authorized users, (2) was allowing the use of generic user accounts, which hinders the agency's ability to hold users accountable for their actions, (3) had not configured the system to expire users' passwords in accordance with Department regulations, (4) granted administrative privileges to an excessive number of users, some of which conflicted with their job responsibilities, and (5) stored critical account passwords in a central file that was accessible by at least six agency personnel that did not need access to these passwords to perform their job functions.
- At five agencies, our review of user access permissions to data were inconsistent with their job responsibilities. In one application, the agency programmed its application to allow access to data based on one of six different user profiles, which limited the user to certain data-input screens in the application. However, this was not sufficient to limit access based on job function. For instance, all users in the agency's district offices, from the office supervisor to administrative support personnel, had access to add or modify data in the application. In another application, approximately 47 agency personnel had access to the application. Of those 47, 36 had administrative access, allowing complete control to add, modify, or delete the data in the application. During our fieldwork, the agency recognized that not all 36 persons needed this level of access and reduced it to only 9 users.

The issues raised in this report have been reported to the Department's OCIO and in specific agency reports. Therefore, we make no additional recommendations herein.

---

## **Finding 5**

### **Improvements in OCIO's Oversight Role would Benefit the Department**

In the past several years, OCIO has strengthened its oversight of agencies' security programs; however, improvements could be made which would significantly strengthen the Department's security posture. Specifically, OCIO needs to (1) formalize its tracking system for USDA cyber security incidents to ensure timely followup and resolution, and (2) increase the number and frequency of its own agency reviews. Despite its efforts over the past several years, OCIO's inability to strengthen its oversight and enforcement role has hindered its ability to effectively manage the Department's security program.

The Clinger-Cohen Act requires the head of executive agencies to ensure that the information security policies, procedures, and practices of the executive



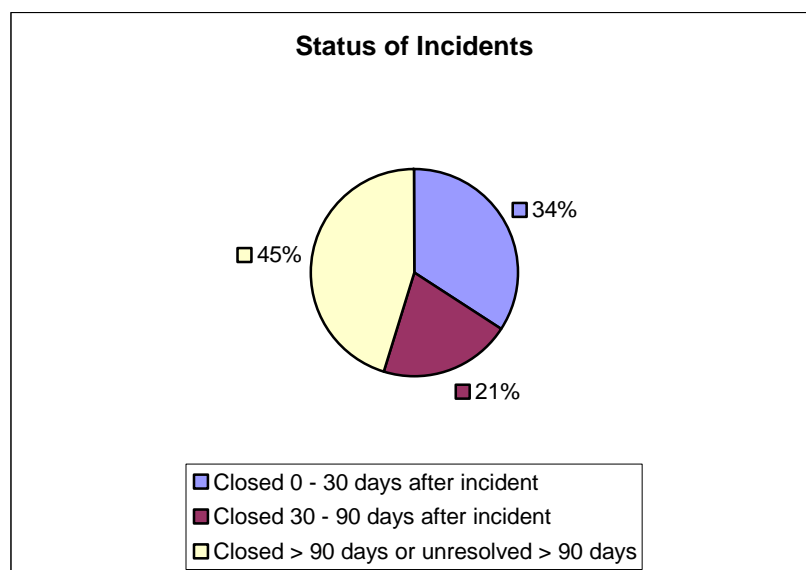
agency are adequate. The Act established the CIO in the Department and requires it to monitor the performance of USDA's IT programs. In addition, FISMA requires the CIO to (1) ensure that the Department effectively implements and maintains information security policies, procedures, and control techniques; (2) evaluate the effectiveness of the information security program, by periodically testing and evaluating information security controls and techniques; and (3) implement appropriate remedial actions based on that evaluation. Finally, FISMA also requires the Department to report to OMB and Congress on the results of the above tests and evaluations, and the progress of remedial actions.

#### Tracking of Cyber Security Incidents

For the past 4 years, OCIO has been operating the Department's intrusion detection system that alerts OCIO officials to potentially threatening or destructive intrusions to the Department's networks and systems. This process has served the Department well by identifying the presence of Internet worms, use of software to download copyright or inappropriate materials, and potential hacking attempts on critical systems. However, despite our prior recommendation, the Department's OCIO has not formalized its tracking of cyber-related incidents.

As the OCIO identified potential threats, OCIO personnel reacted by informing the affected agency of the incident. OCIO's policy requires that the agency prepare and submit an incident report which describes the nature of the incident and what actions were taken to correct the effects of the incident. Our review showed that OCIO, while timely communicating potential threats to agency personnel, was not ensuring that the agency responded quickly to the incident or timely prepared an incident report. Our review shows that only if the Department's intrusion detection system detected a repeat instance of the threat did the OCIO quickly initiate followup with the agency.

The Department identified 179 security incidents during the fiscal year through August 20, 2004. As shown in the chart below, incidents were not always closed by the agencies in a timely manner.



Despite our prior recommendation to implement a formal incident tracking system, the OCIO has tracked cyber security incidents by using one OCIO employee’s e-mail. While this tracking method may be conducive to communicating incidents with agency personnel, it is not an effective method to track the timely followup, resolution, and reporting by the agencies.

Increasing Agency Reviews

In the past few years, OCIO has decreased the number of its own reviews of agencies’ security programs. With limited resources, the OCIO has directed its efforts toward issuing policy and initiating Department-wide efforts such as the certification and accreditation process. While these activities are critical components of OCIO’s oversight role, we believe that the lack of OCIO’s onsite presence has contributed, in part, to agencies not:

- Preparing security planning documentation and implementing security policies;
- implementing effective vulnerability scanning and mitigation efforts;
- enforcing access control policies;
- deploying patch management software; and
- preparing timely, complete, and supportable capital planning and investment control documentation.

While OIG has played a significant role in identifying these issues, OIG can only provide periodic independent assessments of agency operations. Ultimately it is each agency’s and the Department’s management’s responsibility for ensuring that internal controls, including information security controls, are adequate and effectively implemented on an ongoing basis. We believe that OCIO needs to increase its own reviews of agency

operations to effectively oversee and administer the Department's overall security program.

## **Recommendation No. 2**

OCIO should implement a formal tracking system for cyber security incidents to ensure timely followup, resolution, and reporting.

**Agency Response.** OCIO concurred with this recommendation and has taken the necessary steps to procure and deploy a commercial off the shelf package for tracking cyber security incidents. This new tracking system will replace the one currently in use in the Department and will permit an effective method to track the timely followup, resolution and reporting by the agencies and the Department. The new tracking system will be implemented no later than October 30, 2004.

**OIG Response.** We concur with OCIO's management decision.

# Scope and Methodology

---

The scope of our review was Department-wide and agency audits relating to IT completed during fiscal year 2004 through August 31, 2004. We conducted this audit in accordance with Government Auditing Standards.

Fieldwork for this audit was performed at the Department OCIO and three selected agencies from June to August 2004. 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 2004 audit work covered 12 agencies and staff offices, which operate approximately 229 of the estimated 460<sup>9</sup> general support and major application systems within the Department.

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

- Consolidated the results and issues from our prior IT security audit work. Our audit work consisted primarily of audit procedures found in the GAO Financial Information System Control Audit Manual (FISCAM),
- 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 OMB's Memorandum No. M-04-25, dated August 23, 2004.

---

<sup>9</sup> The total number of systems within the Department is based on OCIO's Certification and Accreditation update spreadsheet dated August 20, 2004. As presented in Finding No. 2, OCIO's data is agency-supplied and not verified or audited. Therefore we have no assurance that these figures are accurate. The number of systems in the 12 agencies in our review is based on independent auditor verification and may not be consistent with the number of systems reported by OCIO for Certification and Accreditation purposes.

# Exhibit A – OMB Reporting Requirements and OIG Position

## Section A: System Inventory and IT Security Performance

**A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.**

**A.1.a. FY04 Programs**

There are approximately 26 agency and staff offices within the US Department of Agriculture. The agencies we reviewed, total number of systems identified in each of those agencies, and the number of systems we selected for review are shown in section A.1.b.

**A.1.c. FY04 Contractor Operations or Facilities**

Out of the 12 agencies we reviewed, we identified one agency that used three contractors and one subcontractor to support a major Department application that has not been certified and accredited. The application contractor developed and maintains the application. The facility contractor stores agency-owned servers and other hardware on its property in a secure and protected room. The hardware maintenance contractor provides maintenance functions for hardware switch configuration and supports the firewalls used to protect the application. The firewall subcontractor manages the firewall and intrusion detection systems.

**A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.**

Bureau Name	A.1.		A.2.		A.2.		A.2.	
	A.1.b.		A.2.a.	A.2.b.	A.2.c.	A.2.d.	A.2.e.	
	Total # <sup>10</sup>	# Rev. <sup>11</sup>	Number of systems certified and accredited	Number of systems with security control costs integrated into the life cycle of the system.	Number of systems for which security controls have been tested and evaluated in the last year	Number of systems with a contingency plan	Number of systems for which contingency plans have been tested	
	Total #	Total #	Total #	Total #	Total #	Total #	Total #	
1. AMS	15	1	0	-	0	-	-	
2. APHIS	36	1	0	-	-	-	-	
3. CCC	-- <sup>12</sup>	7	0	0	0	0	0	
4. CSREES	4	1	1	-	0	0	0	
5. DA	7	1	1	1	2	1	0	
6. FSA	26	3	0	0	0	1	0	
7. FSIS	12	1	0	0	0	0	0	
8. FS	66	29	7	66	0	15	0	
9. NFC	30	6	0	-	-	-	-	
10. NITC	11	4	0	-	-	1	1	
11. NRCS	3	2	0	0	0	0	0	
12. RMA	19	3	0	-	-	-	-	
<b>Totals</b>	<b>229</b>	<b>59</b>	<b>9</b>	<b>67</b>	<b>2</b>	<b>18</b>	<b>1</b>	

Note 1: Dashes indicate that the information was not within the scope of our review.

Note 2: OIG-reported totals will differ from OCIO-reported totals due to the sampling of agencies we reviewed and to the timing of our fieldwork.

<sup>10</sup> Based on independent auditor verification and may not be consistent with the number of systems reported by OCIO.

<sup>11</sup> Reviews conducted from October 1, 2003 through August 31, 2004.

<sup>12</sup> See FSA for total number of systems.

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

---

Exhibit A – Page 2 of 15

**A.3. 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 Comment area provided below.**

- a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.**

USDA has employed 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 do not believe the agencies have adequately employed methods to ensure that contractor provided services meet the requirements of the Security Act, OMB, and NIST guidelines. However, 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, OMB, and NIST guidelines.

- b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.**

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. Under FISMA, agencies use the NIST self-assessment guide to identify those areas where they are not compliant with federally mandated guidelines.

- c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.**

For conducting FISMA self-assessments, we found that the Department and its agencies generally follow NIST Special Publication 800-26, however as we reported in Finding No. 2, not all agencies have followed NIST guidance when preparing security plans, risk assessments, and disaster recovery plans.

- d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.**

The Department does not have a reliable inventory of applications and general support systems from which to manage Department-wide IT security. The Department relies on

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

---

Exhibit A – Page 3 of 15

agencies to provide a comprehensive list; however, with limited resources, OCIO is unable to verify the accuracy or reliability of those agency-provided inventories. (See Finding No. 2.)

- e. The OIG was included in the development and verification of the agency’s IT system inventory.**

OIG was not involved in the development and verification of agency IT system inventory.

- f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.**

While we agree that OCIO’s current list of major applications provides a starting point, we believe that the errors we found (See Finding No. 2) support the need to have a well-established definition of a system and ensure that agencies are reporting their systems in accordance with that definition. Further, we believe that the 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. For example, in preparation of our FY 2004 nationwide audit of application controls, we selected seven systems from the OCIO’s list of major applications dated December 2003. Our review disclosed that three of the seven applications we selected were scheduled to be replaced or no longer used by the end of the fiscal year, one application was in the initial stages of development and therefore not far enough along for the certification process, and one system was an ad-hoc database containing historical data no longer used by the agency but “scheduled” to be brought back on-line sometime during the year. Further, we noted that between December 2003 and August 20, 2004, OCIO provided us with at least four different lists of systems or certification progress updates showing the total number of departmental systems ranging between 594 and 460.

- g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.**

The Department has a comprehensive Capital Planning and Investment Control process in place where each agency submits major IT investment information for review and approval by the Department’s CIO.

# Exhibit A – OMB Reporting Requirements and OIG Position

**h. The agency has begun to assess systems for e-authentication risk.**

While the Department has begun to use e-authentication on its systems<sup>13</sup> and has issued guidance regarding the use of Public Key Infrastructure (PKI) technology,<sup>14</sup> OIG has only performed limited e-authentication system assessments during our reviews. We have plans to expand our audit efforts into the Department’s e-authentication and e-government initiatives during fiscal year 2005.

**i. The agency has appointed a senior agency information security officer that reports directly to the CIO.**

The Department has appointed a CIO to oversee the security program within the Department. Our reviews at the agency level have shown that agencies have identified their own CIO and ISSPM to manage their individual security programs. However, as noted in Finding No. 1 of the Findings and Recommendations section of this report, we have found that agency managers have not always committed to or maintained involvement in their security programs. As a result, the Department and its agencies are not compliant with OMB Circular A-130 and other federally mandated security guidelines.

<b>Section B: Identification of Significant Deficiencies<sup>15</sup></b>				
<b>B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&amp;M has been developed. Insert rows as needed.</b>				
<b>Bureau Name</b>	<b>Total Number</b>	<b>Number Repeated from FY 03<sup>16</sup></b>	<b>Identify and Describe Each Significant Deficiency</b>	<b>POA&amp;M developed? Yes or No</b>
AMS	4	Yes	Inadequate security plans	No
		Yes	Systems not certified and accredited	No
		Yes	System scans not performed	No
		Yes	Inadequate logical controls	No
APHIS	4	Yes	Systems not certified and accredited	No
		Yes	Security awareness training not completed	No
		Yes	Inadequate logical controls	No
		Yes	System scans not performed	No
CCC	-		See FSA below.	
CSREES	8	No	Inadequate risk assessments	No
		No	Inadequate security plans	No
		No	Inadequate contingency plans and/or no testing of plan	Yes
		No	Security awareness training not completed	No

<sup>13</sup> Agencies are currently in the process of having their users subscribe to use Gov Online Learning Center (www.golearn.gov), which requires e-authentication.

<sup>14</sup> In January and March 2002, the Department issued guidance regarding the use of Public Key Infrastructure (PKI) Technology.

<sup>15</sup> All OIG-reported weaknesses are, in our opinion, significant deficiencies.

<sup>16</sup> Deficiency repeated from a prior year’s audit but may not have been from fiscal year 2003 review.



# Exhibit A – OMB Reporting Requirements and OIG Position

Bureau Name	Total Number	Number Repeated from FY 03 <sup>17</sup>	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
CSREES – Cont'd		No	Systems not certified and accredited	Yes
		No	Inadequate physical controls	No
		No	Inadequate logical controls	No
		No	System scans not performed	No
DA	10	Yes	Inadequate risk assessments	Yes
		Yes	Inadequate security plans	No
		Yes	Inadequate contingency plans and/or no testing of plan	Yes
		Yes	Security awareness training not completed	No
		Yes	Systems not certified and accredited	No
		No	Background investigations not performed	No
		Yes	Inadequate physical controls	No
		Yes	System scans not performed	No
		Yes	Inadequate patch management	No
		Yes	Inadequate logical controls	No
FSA	11	No	Inadequate risk assessments	Yes
		Yes	Inadequate security plans	Yes
		Yes	Inadequate contingency plans and/or no testing of plan	Yes
		Yes	Security awareness training not completed	Yes
		No	Systems not certified and accredited	Yes
		No	Background investigations not performed	Yes
		Yes	Inadequate physical controls	Yes
		Yes	System scans not performed	Yes
		Yes	Inadequate patch management	Yes
		Yes	Inadequate logical controls	Yes
		No	Capital asset plans not timely prepared and/or do not include required elements	No
FSIS	8	Yes	Inadequate risk assessments	No
		Yes	Inadequate contingency plans and/or no testing of plan	No
		Yes	Systems not certified and accredited	No
		Yes	Inadequate physical controls	No
		Yes	Inadequate logical controls	No
		No	System scans not performed	No
		No	Inadequate patch management	No
		No	Inadequate system documentation and change management	No
FS	9	Yes	Inadequate risk assessments	No

<sup>17</sup> Deficiency repeated from a prior year's audit but may not have been from fiscal year 2003 review.

# Exhibit A – OMB Reporting Requirements and OIG Position

Bureau Name	Total Number	Number Repeated from FY 03 <sup>18</sup>	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
FS - Cont'd		Yes	Inadequate security plans	No
		Yes	Inadequate contingency plans and/or no testing of plan	No
		Yes	Security awareness training not completed	No
		Yes	Systems not certified and accredited	No
		No	Background investigations not performed	No
		Yes	Inadequate physical controls	No
		No	Inadequate patch management	No
		Yes	Inadequate logical controls	No
NFC	3	Yes	Systems not certified and accredited	Yes
		Yes	Inadequate logical controls	No
		Yes	Inadequate system documentation and change management	No
NITC	8	No	Inappropriate/Unlicensed software used	No
		Yes	Inadequate risk assessments	No
		Yes	Inadequate security plans	No
		Yes	Inadequate contingency plans and/or no testing of plan	No
		Yes	Systems not certified and accredited	No
		No	System scans not performed	No
		Yes	Inadequate logical controls	No
		Yes	Inadequate system documentation and change management	No
NRCS	10	Yes	Inadequate risk assessments	No
		Yes	Inadequate security plans	No
		Yes	Inadequate contingency plans and/or no testing of plan	No
		No	Systems not certified and accredited	No
		No	System scans not performed	No
		No	Inadequate patch management	No
		No	Capital asset plans not timely prepared and/or do not include required elements	No
		No	Inadequate system documentation and change management	No
		Yes	Inadequate logical controls	No
		Yes	Inadequate physical controls	No
RMA	5	Yes	Inadequate contingency plans and/or no testing of plan	No
		Yes	Security awareness training not completed	No

<sup>18</sup> Deficiency repeated from a prior year's audit but may not have been from fiscal year 2003 review.

# Exhibit A – OMB Reporting Requirements and OIG Position

Bureau Name	Total Number	Number Repeated from FY 03 <sup>19</sup>	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
RMA - cont'd		Yes	Inadequate logical controls	No
		Yes	Inadequate system documentation and change management	No
		Yes	System scans not performed	No
<b>Totals</b>	<b>80</b>	<b>54 (Yes) 26 (No)</b>		<b>15 (Yes) 65 (No)</b>
		<b>67.5% (Yes) 32.5% (No)</b>		<b>19% (Yes) 81% (No)</b>

## Section C: OIG Assessment of the POA&M Process

**C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. 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 Comment area provided below.**

- a. Known IT security weaknesses, from all components, are incorporated into the POA&M.**

Overall the Department has developed and implemented a process to manage the Department-wide consolidation and reporting of POA&M weaknesses. However, agencies are not always supplying all of the information requested by OMB such as the source of the funds to correct the weakness. We determined that not all known IT security weaknesses were included in agencies POA&Ms. 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.

- b. Program officials develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.**

The Department and its agencies have not prepared POA&Ms for each of its systems. We attribute this, in part, to a lack of risk assessments and security plans; therefore, not all security weaknesses have been identified for reporting purposes. In fiscal year 2004, the Department implemented a Department-wide initiative to certify and accredit all major applications and general support systems of which assessing risks is part of this process. However, the effort is far from complete. (See Finding No. 2.)

<sup>19</sup> Deficiency repeated from a prior year's audit but may not have been from fiscal year 2003 review.

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

---

Exhibit A – Page 8 of 15

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

Our review disclosed that not all agencies report complete POA&M data on a timely basis. The agencies we reviewed did not have controls in place to ensure that POA&M data reported to the Department’s CIO was complete and accurate.

- d. CIO develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.**

The Department and its agencies have not prepared POA&Ms for each of its systems. We attribute this, in part, to a lack of risk assessments and security plans; therefore, not all security weaknesses have been identified for reporting purposes. In fiscal year 2004, the Department implemented a Department-wide initiative to certify and accredit all major applications and general support systems of which assessing risks is part of this process. However, the effort is far from complete. (See Finding No. 2.)

- e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.**

The Department OCIO maintains a tracking system that the agencies use to track all POA&M weaknesses and milestones on a quarterly basis. However, as stated in question C.1.c., not all agencies not have controls in place to ensure that the reported information is complete and accurate.

- f. The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.**

We do not believe the Department’s centralized tracking system of POA&M weaknesses has matured to the level of being an authoritative agency and IG management tool. Our reviews of agency-prepared POA&Ms have found that not all weaknesses are identified, and that not all of the information required by OMB is properly reported. Therefore, OIG has not relied on POA&Ms as an effective management tool for its reviews.

- g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).**

Not all agencies have prepared POA&Ms for every system, and in many cases, the source of security funds are not captured in POA&M reports. Therefore, we cannot say

with certainty whether all POA&Ms are tied to the system budget request as required by OMB Circular A-11.

**h. OIG has access to POA&Ms as requested.**

OIG has access to POA&M records.

**i. OIG findings are incorporated into the POA&M process.**

OIG findings are not always incorporated into the POA&M process. Officials at the agencies we reviewed stated that the certification and accreditation process, which is scheduled to be completed September 30, 2004, would eliminate the POA&M weakness identified in OIG's reports. OIG does not agree with this assessment since many of the weaknesses we identified require long-term solutions that require to be tracked with the POA&M process.

**j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.**

POA&M weaknesses are not prioritized; however, agencies use the POA&Ms to identify milestones accomplished toward meeting the necessary actions to correct the weaknesses.

## **C.2 OIG Assessment of the Certification and Accreditation Process**

**Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "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. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.**

At the time of our fieldwork, the agencies we reviewed had not completed system certifications and accreditations on their major applications or general support systems. Agencies officials

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

informed us that they are completing the certifications in accordance with the Department's directives and intend to have this process completed by September 30, 2004. Despite the longstanding requirement by OMB to complete this certification and accreditation process prior to system implementation, the requirement has been largely ignored and not enforced. Department CIO officials have informed us that they are committed to ensuring that the certification and accreditation process is fully implemented into every agency's system development lifecycle process. (See Finding No. 2.)

### **Section D**

**D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. For example: If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.**

**D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?**

- D.1.a. Windows XP Professional**
- D.1.b. Windows NT**
- D.1.c. Windows 2000 Professional**
- D.1.d. Windows 2000**
- D.1.e. Windows 2000 Server**
- D.1.f. Windows 2003 Server**
- D.1.g. Solaris**
- D.1.h. HP-UX**
- D.1.i. Linux**
- D.1.j. Cisco Router IOS**
- D.1.k. Oracle**
- D.1.l. Other. Specify:**

OCIO has provided the agencies security assessment guidelines for the Windows , Solaris, HP-UX, and Linux operating systems. In addition, the Department has similar security assessment guidelines for mainframe, classified systems, personal electronic devices (PED), telecommunications, Web Farms, and AS400s. The Department has an ongoing initiative to prepare specific security configuration policies to be used as suggested baselines for each of the above operating environments.

**D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.**

**D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?**

The OCIO has issued guidance on patch and configuration management and has encouraged agencies to deploy patch management software. However, few agencies have taken advantage of this software to manage patches. During our reviews, we identified system vulnerabilities by performing tests using the scanning product available to all agencies for their use. Our scans identified vulnerabilities that would have been mitigated if agencies had timely applied patches or if agencies would have vigilantly used the Department-provided scanning software to identify and timely mitigate vulnerabilities on their systems.

## **Section E: Incident Detection and Handling Procedures**

**E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.**

**a. The agency follows documented policies and procedures for reporting incidents internally.**

The Department's OCIO has a comprehensive incident response program in place. It operates effectively at the Department level. The program includes intrusion detection capability on the Department's backbone network and communication with the United States Computer Emergency Readiness Team and law enforcement authorities. However, we found that the Department's CIO has not developed an effective tracking system for security incidents to ensure that agencies timely address and report on security incidents. (See Finding No. 5.)

**b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.**

See response for E.1.a. above.

**c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT).**

See response for E.1.a. above.

## **E.2. Incident Detection Capabilities.**

### **a. How many systems underwent vulnerability scans and penetration tests in FY04?**

At 11 of the 12<sup>20</sup> agencies we reviewed, the agencies had failed to establish effective controls to timely identify and mitigate vulnerabilities on their systems as required by Department policy. In 2001, the Department, based on our audit results, purchased a Department-wide license for a commercially available vulnerability scanning software tool. The tool identifies vulnerabilities exploitable in operating systems that use TCP/IP, the protocol used on the global Internet, and categorizes vulnerabilities into high, medium, and low risk.<sup>21</sup> Some agencies we reviewed scanned their systems once every few months but not on a consistent basis, other agencies scanned their systems using one of the software's built-in policies that does not identify all known vulnerabilities that can be exploited by attackers, and other agencies failed to scan critical components of their networks such as their routers and firewalls. (See Finding No. 3.)

### **b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?**

Agencies have sporadically employed various tools, techniques, and technologies to mitigate IT security risks including ISS Internet Scanner, Bindview, Nessus, Patch Link, Microsoft Baseline Analyzer, McAfee Virus Protection Software, and Symantec AntiVirus.

---

<sup>20</sup> One agency had established effective controls over its own scanning process.

<sup>21</sup> High-risk vulnerabilities are security issues that allow immediate remote or local access, or immediate execution of code or commands with unauthorized privileges. Medium-risk vulnerabilities are security issues that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures. Low-risk vulnerabilities are security issues that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not directly gain unauthorized access.



# Exhibit A – OMB Reporting Requirements and OIG Position

<b>Section F: Incident Reporting and Analysis</b>						
<b>F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below.</b>						
<b>F.2. Identify the number of systems affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.</b>						
	<b>F.1.a. Reported Internally</b>	<b>F.1.b. Reported to FedCIRC</b>	<b>F.1.c. Reported to Law Enforcement</b>	<b>F.2.a. Systems with Complete and up to date C&amp;A<sup>22</sup></b>	<b>F.2.b. Systems<sup>23</sup> without complete and up to date C&amp;A</b>	<b>F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?</b>
I. Root Compromise	39	28	3	0	162	9
II. User Compromise	45	9	9	0	44	0
III. Denial of Service Attack	2	1	0	0	4	1
IV. Website Defacement	1	1	0	0	1	0
V. Detection of Malicious Code	10	5	1	1	10	4
VI. Successful Virus/Worm Introduction	79	53	1	0	525	55
VII. Other	3	0	1	0	3	0
<b>Totals:</b>	<b>179</b>	<b>97</b>	<b>15</b>	<b>1</b>	<b>749</b>	<b>69</b>
Incidents reported from October 1, 2003 through August 20, 2004.						

## Section G: Training

**G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.**

**a. Total number of employees in FY04**

As of August 29, 2004, the Department has 116,603 employees.<sup>24</sup> The Department does not have a central database of all contractors. Therefore, an accurate count of contractors is not available.

<sup>22</sup> To determine if the system was certified and accredited, OIG determined if the agencies' local area networks were certified and accredited.

<sup>23</sup> These numbers represent the number of IP addresses reported as being affected by the incident. Because the incident is reported by IP address, OIG was not able to identify the systems.

<sup>24</sup> Based on National Finance Center (NFC) payroll system data.

**b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50.**

Agencies we reviewed had processes and resources in place to provide its employees with security awareness training, and that system and network administrators have a means to acquire specialized training relating to their responsibilities; however, agencies had not established adequate controls to ensure all employees received the necessary training. In one agency, OIG found that almost all employees had received security awareness training. However, in another agency only about 51 percent of the employees took security awareness training, and the agency could not provide an up to date listing of contractors, contractor training, or contractor background checks because no controls had been put into place to track these individuals. The OCIO annually reports on compliance with the Federal Information Security Management Act (FISMA) as of September 30 and, in some cases such as computer security awareness training and system certification and accreditation, completes, or documents the completion, of a significant amount of the required actions in the month of September. As such, the Department and its agencies may have implemented controls or completed corrective actions that, due to the timing of our fieldwork, may not be reflected in this report.

**c. Total number of employees with significant IT security responsibilities.**

Not all agencies have established controls to ensure that all employees with significant IT security responsibilities are provided training related to those responsibilities. Based on our FISMA review at three USDA agencies, one agency had not identified employees with significant IT responsibilities. For the other two agencies, there are 501 employees with significant responsibilities. We found that only 165 of the 501 received specialized training. These three agencies have a total of 36,112 employees.

**d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16**

See G.1.c. response above.

**e. Briefly describe training provided.**

The reviews we conducted showed that OCIO and agencies had various training initiatives. Provided and/or planned training included:

- Certification and accreditation training,
- Responsibilities of agency Information System Security Program Managers (ISSPMs),

- General Security Awareness,
- USDA Security Awareness course (available August 4, 2004),
- Securing Local Area Networks,
- Managing Network Security,
- Identifying Viruses,
- Fundamentals of Internet Security, and
- An Executive Briefing Handbook for Senior Executives that includes rules, regulations, references, and executive briefing training material.

**f. Total costs for providing IT security training in FY04 (in \$'s)**

This information is not readily available for all agencies. For the three agencies we reviewed, one agency had not determined these costs. For the other two agencies, \$222,000 was spent on IT security training to its employees.

**G.2. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?**

Our reviews focus on whether or not agencies have controls in place to provide security awareness training to all employees, and whether those with significant IT security responsibilities are provided specialized training. Our reviews, up to now, have not included a comprehensive review of the content of the security training offered or provided by each agency.

# Exhibit B – OCIO's Response to the Draft Report

Exhibit B – Page 1 of 5

United States  
Department of  
Agriculture



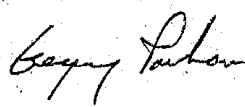
Office of the Chief  
Information Officer

1400 Independence  
Avenue S.W.

Washington, DC  
20250

September 30, 2004

TO: Robert W. Young, Assistant Inspector General for Audit  
Office of Inspector General

FROM: Gregory Parham, Acting Associate Chief Information Officer  
Cyber Security 

SUBJECT: Office of Inspector General Official Draft Report #50501-1-FM  
"Fiscal Year 2004 Federal Information Security Management Act Report"

Attached is the Office of the Chief Information Officer's response to the subject report.

If additional information is needed, I can be reached on (202) 690-0048.

Attachment

cc: Scott Charbo, Chief Information Officer (w/attachment)

AN EQUAL OPPORTUNITY EMPLOYER

## Exhibit B – OCIO Response to the Official Draft Report

While this audit is only partially directed toward the Office of the Chief Information Officer (OCIO), OCIO is providing a Department response to several of the issues raised and recommendations provided therein.

OCIO agrees with many of the findings and recommendation arising from the audit. However, for a few of the findings and declarations made by the Office of the Inspector General (OIG), we disagree. We believe this difference of opinion or perception is directly linked to the methodology used by OIG to conduct the audit. In particular, the timing of the audit (concluded in August, 2004), does not allow OIG to acknowledge the final set of achievements attained during the fiscal year. We believe that some context and clarification in certain areas will provide a more complete picture of the status of Information Technology (IT) security within USDA. We offer the following specific responses:

1. Within the Executive Summary and other areas of the audit, OIG focuses on lack of management commitment as a contributing factor to the weaknesses found within USDA’s security program. OIG cites some specific examples they attribute to lack of management involvement in Finding 1, Management Involvement and Commitment is Needed to Ensure a Successful and Effective Security Program. Within the narrative supporting this finding OIG states: “Agency managers should be held accountable for committing the appropriate resources to ensure compliance.”

OCIO Response: The notion of accountability and appropriate resources is not an actionable item to provide a specific response. The implication of this finding is that managers should be penalized if security is found lacking. The penalties are neither defined nor suggested. Furthermore, such recourse must first be preceded by well-defined personal performance standards and a standardized and fair scoring mechanism, neither of which has been widely adopted across the Federal government.

Since it first became a requirement years ago, USDA had not certified and accredited (C&A) many of its information systems. However, for fiscal year 2004, USDA established as one of its goals the accreditation of all its general support systems and major applications, and subsequently expanded this goal to include ALL systems. USDA agrees with Federal security guidelines that accreditation is an overarching exercise that provides evidence that a Federal agency is conscious of and attentive to security issues.

Early in the fiscal year, dialogue was initiated with the most senior of USDA’s managers to explain the C&A process and to obtain commitment. These conversations included the OIG. Agencies were challenged to inventory and categorize their systems and develop plans such that the USDA objective would be achieved by the end of the fiscal year.

AN EQUAL OPPORTUNITY EMPLOYER

Agency technical staffs, with senior management encouragement and involvement (including the sub-cabinet) have been completely engaged throughout the year.

Using an OCIO contract specifically designed for obtaining external expertise, agencies hired security firms to assist them in their C&A activities. Over \$21 million dollars and countless staff hours have been devoted to this effort. Hundreds of previously missing security documents have been developed, independent assessments have been conducted, and final security evaluations have been presented to respective agencies.

*Now as the end of the year approaches, USDA is able to report that over 90 per cent of its general support systems, major applications, and non-major applications have been accredited.* The balance of systems are currently in the process of accreditation. By December 2004, USDA expects to be able to report accreditation of all its systems.

Despite all of this attention, effort, time and money devoted to security C&A, OIG chose to minimize this achievement. Their audit report states that due to the fact that accreditation, if achieved, would come so late in the year it would not warrant consideration.

OCIO submits that this effort demonstrates clearly that management and security staffs are serious about addressing security. OCIO and USDA agencies acknowledge that security weaknesses continue to exist, but action plans are being developed to eliminate these weaknesses.

Furthermore, OCIO maintains that a security program, like most management endeavors, is a process rather than an event. If the efforts of both management and staff are not acknowledged, the incentive to continue is diminished. Rather than acknowledge USDA agencies for their C&A accomplishments, OIG chose to use C&A as an example of security failure. We believe OIG’s position is does not produce an accurate status of USDA’s security position or achievement.

Throughout the coming year, USDA will focus on completing the action plans arising from the C&A effort. Management will continue to be apprised of progress, and when necessary, will be asked to become actively involved. OCIO has every reason to believe that progress will continue to be made. We continue to look at OIG as a partner in this effort.

2. Within the audit report, OIG cites the absence of a reliable systems inventory as an example of poor security management. OIG also recommends that USDA establish a “well-defined definition of a system.”

OCIO Response: Throughout USDA’s effort to certify and accredit all of its’ general support systems, major applications and non-major applications during fiscal year 2004, OCIO challenged agencies to develop sound inventories of their systems. This inventory would provide a basis for assuring complete accreditation.

AN EQUAL OPPORTUNITY EMPLOYER

Many hours have been devoted to discussions about and adjustment to the system inventory. As contract expertise was hired to assist agencies with their C&A activities, additional adjustments to the inventory were necessary to establish the appropriate scope for testing and control purposes. This led to combinations of like systems and elimination of others that have been or soon will be replaced.

This constant attention throughout the year to the integrity of the system inventory has resulted in a sound listing of all the USDA major and non-major applications and general support systems. This listing has always been available to OIG upon request. OCIO expects the systems inventory to be a baseline and not static. This will serve as a dynamic inventory that is now manageable.

As to the issue of system definition, OCIO believes USDA is bound in this regard, by the Office of Management and Budget (OMB) FISMA guidelines. The OMB FISMA guide states: “An inventory of each agency’s major information systems has been required for many years by the Paperwork Reduction Act and, more recently, by the 1996 Electronic Freedom of Information Act amendments. The definition of ‘major information system’ is found in OMB Circular A-130...”

3. Within Finding 2, Progress Made, but Noncompliance with Federally Mandated IT Security Requirements Continues, OIG cites several issues that they suggest provides evidence that weaknesses exist within USDA’s security program.

OCIO Response: Among the citations of security deficiencies, OIG includes:

- Lack of a reliable inventory. OCIO maintains that a reliable inventory does exist.
- A significant majority of the Department’s applications were not certified until near the end of the fiscal year. OCIO maintains that improving from a few accredited systems at the end of FY 2003 to accreditation of over 90 percent at the end of FY 2004 is a significant improvement rather than a sign of poor progress. The FISMA report should accurately reflect our posture on C&A as of September 30, 2004.
- Inadequate assessment of risk. OCIO maintains that this is another area of significant improvement. For all systems that were accredited during FY 2004 (over 90 %) a risk assessment was performed. Except for those systems categorized as low-risk/low-impact, all of these assessments were conducted by independent contractors. OCIO attributes this difference in perception to the timing of the OIG audit.
- Inadequate security plans. Again, OCIO maintains that this is an area in which agencies greatly improved. For every accredited system (over 90 %), security plans were re-visited for compliance. For many, an independent contractor was engaged to review or re-write the security plan prior to accreditation. OCIO attributes this difference in perception to the timing of the OIG audit.
- Poor performance in regards to security awareness and training. As an example of progress in this area, OCIO has established a web-based

AN EQUAL OPPORTUNITY EMPLOYER

training program that satisfies the federal requirements for security awareness training. This program is available to all USDA employees and provides a count, by agency, of employees who have successfully completed the course. This training program was not deployed until August, after the field work for this audit was completed. To date over 70,000 USDA employees have completed this training, many using this course. In addition, the Department declared September to be Security Awareness Month at USDA. Special events were held to heighten awareness of security awareness issues and security responsibilities.

4. Exhibit A of the audit report shows OIG’s Position on OMB Reporting Requirements. Section B addresses Significant Deficiencies. OIG lists a number of deficiencies, by agency, and a report on whether or not a POA&M has been developed.

OCIO Response: OCIO takes exception to OIG’s list of deficiencies and POA&M’s. OCIO is aware that many of the deficiencies listed no longer exist as a result of the C&A activities completed during the past year. Furthermore, the identification of POA&M’s was made prior to OCIO’s distribution of OMB’s current year FISMA guidance to agencies. Agencies had not even developed current year POA&M’s at the time the OIG audit fieldwork was concluded. OCIO attributes this difference in perception to the timing of the OIG audit.

5. OIG Recommendation – OCIO should implement a formal tracking system for cyber security incidents to ensure followup, resolution and reporting.

OCIO Response: OCIO concurs with this recommendation and has taken the necessary steps to procure and deploy a COTS package for tracking cyber security incidents. This new tracking system will replace the one currently in use in the department and will permit an effective method to track the timely follow-up, resolution and reporting by the agencies and the Department. The new tracking system will be implemented by no later than October 30, 2004.

AN EQUAL OPPORTUNITY EMPLOYER