U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

GOVERNMENT INFORMATION SECURITY REFORM ACT – FISCAL YEAR 2001

Report No.
50099-32-FM
August 2001

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20250

DATE: August 31, 2001

REPLY TO
ATTN OF: 50099-32-FM

SUBJECT: Government Information Security Reform Act – FY 2001

TO: Ira L. Hobbs
Acting Chief Information Officer
Office of the Chief Information Officer

Attached is the final report which presents the results of our independent evaluation of the Department's efforts to improve the management and security of its information technology resources. The report does not contain any recommendations; therefore, a reply is not necessary.

The courtesies and cooperation extended to the auditors was appreciated.

/s/

ROGER C. VIADERO
Inspector General

EXECUTIVE SUMMARY

GOVERNMENT INFORMATION SECURITY REFORM ACT – FY 2001
AUDIT REPORT NO. 50099-32-FM

PURPOSE

Our audit was performed in accordance with Public Law 106-398, "Government Information Security Reform Act (GISRA)," to provide an independent evaluation of the Department's information security program.

RESULTS IN BRIEF

Our audit found that U.S Department of Agricultural (USDA) has initiated actions to strengthen information technology (IT) security in the Department. The Department, through its Chief Information Officer (CIO) has established a Department-wide security program, implemented a departmental security incident response program, and strengthened their oversight function through implementation of program reviews of agencies' security programs. Despite these actions, however, the Department has still not reached its goal of adequately securing its critical IT resources. Office of Management and Budget (OMB) reporting requirements as outlined in OMB Memorandum No. 01-24 and our position on each requirement are presented in Exhibit A of this report.

Our audits have disclosed the following IT security weaknesses within the Department:

- The Department is not fully compliant with several requirements of OMB Circular A-130 and Presidential Decision Directive (PDD) 63. Agencies have not prepared and tested contingency and business continuity plans (the Department's mainframe operations had adequate disaster and contingency plans in place), have not properly certified to the security controls in place on their systems, and have not assessed the risks to their systems and established plans to mitigate those risks.

- Agencies' networks and systems are vulnerable to internal and external intrusion. Using a commercially available software program we identified over 3,400 high and medium-risk vulnerabilities in the nearly 1,300 systems we have scanned during our audits.

- Agencies have not established adequate physical and logical access controls to ensure that only authorized users can access critical agency data. While Office of Chief Information Officer (OCIO) has begun to address these areas since our initial audits, additional progress is needed to ensure that only authorized users can access critical agency data.

- Nine of the 11 agencies we reviewed had not assessed the risks to their systems and initiated a plan to eliminate or mitigate those risks. The Department's OCIO is in the process of implementing its risk assessment program by providing agencies with checklists that will assist the agencies in evaluating the risks to their systems.

- Our audit included tests at four agencies to ascertain the adequacy of training provided to employees. We found that agencies recognized the need for adequate training, but two of the four agencies were unable to provide the specific training given to their technical staff. Currently, the Department does not have a minimum standard, based on continuing education hours or other quantitative means, by which to measure the sufficiency of training given to IT personnel.

- The Department has a documented security incident response procedure now in place and, based upon our review, it is operating effectively at the Department level. However, the Department is not able to monitor all agencies' networks requiring additional actions at the agency level. Our ongoing agency audit work will provide additional insight on how agencies effectively implement this program.

- We reviewed the performance measures established by OCIO and four agencies in our review. The OCIO has established a performance measure to implement a Department-level risk management program; however, there are no performance measures in place to ensure that individual agencies conduct risk assessments, implement security plans, or test and evaluate security controls and techniques.[1]

- The Department has established a comprehensive Capital Planning and Investment Control (CPIC) program. Additional audit work in this area is ongoing; however, our initial review disclosed that the agencies were generally following the CPIC program and using Information Technology Investment Portfolio System (I-TIPS) to track their IT investments.

- Our initial review of contractor oversight at four agencies found that

[1] This performance measure relates to Government Performance and Results Act performance measures. There are no performance measures in place specifically for compliance with the GISRA.

most do not ensure that contractors have the proper security clearances or background checks, or ensure that they are sufficiently trained in Federal security requirements. Only two of the four agencies we reviewed included Federal requirements in their statements of work, and only one of those two had a process in place to ensure that contractors understand Federal requirements before awarding the contract.

KEY RECOMMENDATIONS

This report presents the results of our audit work in assessing the security over the Department's information technology resources. Recommendations we made to correct the deficiencies identified in this evaluation either were made in prior reports, or will be made in audits currently underway. Therefore, no recommendations are made in this report.

AGENCY COMMENTS

This report was discussed with the Acting CIO and other Senior OCIO officials on August 28, 2001. These officials agreed with the issues presented. A written response was not requested to this report.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

Information security, improving the overall management of information technology (IT) resources, and the transition to electronic business (e-government), are top priorities with the U.S. Department of Agriculture (USDA). The USDA is rapidly entering the e-government era. 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 disruptions. Threats range from those posed by insiders, and recreational and institutional hackers to attacks by intelligence organizations of other countries.

Several laws have emphasized the need to protect agencies' sensitive and critical data, including the Privacy Act of 1974, the Computer Security Act of 1987, and the Paperwork Reduction Act of 1995. Departmental responsibilities regarding information security were recently reemphasized in the Clinger-Cohen Act of 1996 and Presidential Decision Directive (PDD) 63, "Policy on Critical Infrastructure Protection."

On October 30, 2000, the President signed into law the Fiscal Year (FY) 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform Act (GISRA)." The Act seeks to ensure proper management and security for the information resources supporting Federal operations and assets. Essentially, the Act codifies the existing requirements of Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, and reiterates security responsibilities outlined in the Computer Security Act of 1987, the Paper Work Reduction Act, and The Clinger-Cohen Act of 1996. It also requires agencies to incorporate security into the life cycle of agency information systems, as well as requiring annual security program reviews, and annual reporting requirements.

The Chief Information Officer (CIO) is the Department official responsible for developing policy and procedures to ensure security is provided over the Department's computers, data, and telecommunication networks.

OBJECTIVES

The objectives of this audit were to perform reviews of agency information technology security operations to address the requirements in Public Law 106-398, "Government Information Security Reform Act." Specifically, we evaluated whether: (1) agencies assessed the risks to their operations and assets, maintained an up-to-date security plan, and tested and evaluated security controls and techniques; (2) the Department's CIO adequately maintains a Department-wide security program; (3) agencies ensure that employees are sufficiently trained in their security responsibilities; (4) agencies have documented procedures for reporting security incidents and sharing information regarding common vulnerabilities; (5) agencies integrate security into their capital planning and investment control process; (6) agencies have identified, prioritized, and protected critical assets within their enterprise architecture; (7) agencies ensure that the agency's information security plan is practiced throughout the life cycle of each agency system; (8) agencies have integrated their information technology security program with their critical infrastructure protection responsibilities; and (9) agencies ensure that contractor-provided services are adequately secure and meet Federal guidelines.

SCOPE

The scope of our review was Department-wide and covered audits relating to information technology security completed during FY 2000 and 2001 through July 31, 2001.

Fieldwork for this audit was performed in May through August 2001. We conducted our testing at Office of Chief Information Officer (OCIO), Farm Service Agency, Rural Development, Agricultural Marketing Service, and Department Administration. In addition, the results of our most recent reviews and OCIO's corrective actions on our recommendations were considered and incorporated into this report. Those audits include: 50099-27-FM, "Security Over USDA Information Technology Resources Needs Improvement;" 50099-28-FM, "PCIE/ECIE Critical Infrastructure Protection Review;" 23099-1-FM, "Security Over Data Transmission in the Department Needs Improvement," 88099-3-FM, "National Information Technology Center – General Controls Review Fiscal Year 2000," and 11401-7-FM, "Fiscal Year 2000 National Finance Center Review of Internal Controls." In total, our audit work covered 11 agencies and staff offices which operate 258 of the estimated 340 general support and major application systems within the Department.

On July 2, 2001, the OCIO required agencies to prepare self-assessments of their security programs and provide those assessments to OCIO no later than July 31, 2001. Not all agencies had provided their assessments to OCIO, and due to time constraints, we were unable to review the results of those self-assessments. Further, our reviews of agency training, capital planning, and use of contractors has been limited to selected audit procedures at four agencies to satisfy the requirements of GISRA. Future audit work should provide additional insight into the adequacy of the agencies' operations in these areas.

We conducted this audit in accordance with Government Auditing Standards.

METHODOLOGY

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

- Consolidated the results and analyzed the issues from our prior IT security audit work. Our audit work consisted primarily of performing selected audit procedures found in the General Accounting Office's Financial Information System Control Audit Manual,
- evaluated OCIO's progress on implementing its Action Plan to Improve USDA Information Security,[2]
- evaluated OCIO's progress on implementing recommendations to correct material weaknesses in prior Office of Inspector General (OIG) and General Accounting Office (GAO) audit reports,
- evaluated the Department's security incident response procedures,
- conducted selected audit procedures on the adequacy of agency training and use of contractor-provided IT services, and
- conducted testing of four agencies' security program[3] and their compliance with existing laws and regulations.

[2] In response to prior OIG and GAO reports, the Secretary of Agriculture instructed the Department's Chief Financial Officer and CIO to develop a plan to improve information security across the Department. In August 1999, the CIO issued its plan, "An Action Plan to Strengthen USDA Information Security."

[3] Not all agencies reported the results of their assessments to OCIO by the July 31, 2001, deadline, and due to time constraints, we were unable to review their adequacy.

FINDINGS

CHAPTER 1	PROGRESS HAS BEEN MADE TO IMPROVE DEPARTMENT-WIDE INFORMATION SECURITY, BUT MORE IS NEEDED.

FINDING NO. 1

THE DEPARTMENT NEEDS TO IMPROVE THE MANAGEMENT AND SECURITY OF IT RESOURCES

The Department, despite its actions to date, has weaknesses in the management of its IT resources and its information security program. Prior to the appointment of the Associate Chief Information Officer for Cyber-Security, Departmental agencies and staff offices had separately addressed their respective IT security and infrastructure needs. These isolated approaches taken by individual agencies have resulted in a disparate array of technical and physical solutions that did not always assure that comprehensive department-wide security was obtained. The Department relies on its IT infrastructure and individual agency 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 ability to accomplish its mission could be jeopardized if it does not properly 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, and establishing a comprehensive security plan. Further, PDD 63, "Policy on Critical Infrastructure Protection," requires agencies to assess the risks to their networks and establish a plan to mitigate the identified risks. Most recently, the GISRA, effective November 29, 2000, codifies the requirements of OMB A-130, Appendix III, requires agencies to conduct self-assessments, and prepare a report to be attached to the Department's budget submission on the state of IT security within the Department.

In August 1999, in response to OIG and GAO audits, and the Secretary's concern of security over USDA's IT resources, the OCIO issued its, "An Action Plan to Strengthen USDA Information Security." The OCIO has begun to address these issues including: (See Exhibits B and C for a complete listing of the actions taken by the OCIO to address their action plan and recommendations made in prior OIG audit reports.)

- hiring a senior manager for Cyber-Security, assigning staff members to work on the Cyber-Security team; and hiring additional staff with expertise in physical security, configuration management, and access controls;

- establishing a comprehensive information security program starting with establishing baseline security architecture for USDA county-level offices, and the evaluation of appropriate encryption techniques to secure sensitive data;

- establishing a Risk Assessment Work Group and Telecom Technical Advisory Board to assist in designing standards and policies, and analyzing the Department's wide area network security needs;

- assembling a permanent Cyber-Security incident response team to protect sensitive systems;

- implementing nine new policies covering topics such as: security plan preparation, incident response, logical access controls, physical security standards, server and firewall security, and capital planning and investment control; and

- strengthening its oversight functions by staffing a Cyber-Security team to conduct security program reviews of the agencies' IT security program.

Despite OCIO's efforts, the Department is still deficient in its compliance with the requirements of OMB A-130 and PDD 63.

Risk Assessment and Mitigation

In July 2000, we issued our audit report on the Department's compliance with PDD 63. We reported that the Department's Critical Infrastructure Assurance Plan fairly and accurately reflected the requirements of PDD 63, but had not been adequately carried out. In identifying its mission essential infrastructure, the Department selected the 52 Department priority systems that were originally identified during its Year 2000 conversion process.

However, beyond this initial determination, the Department had done very little to identify potential or existing threats to these systems.

Our recent work at four agencies found that each agency had established its own method of identifying, prioritizing, and determining the criticality of its systems. One agency used a matrix of integrity, availability, and confidentiality to identify and prioritize its critical IT assets. The others did not prioritize their systems, merely identifying all of their systems as major applications. The Department needs to identify potential and existing threats to its mission-critical systems and networks, prepare and implement a mitigation plan to minimize the effects of those risks, prepare and test contingency/disaster recovery plans, practice security plans throughout system lifecycles, and ensure that agency systems are properly certified and authorized. Only then can the Department be assured that all necessary controls are in place, and implemented in the most cost effective manner, to secure its mission critical and sensitive systems.

Nine of 11 agencies we reviewed have not conducted risk assessments of their networks or critical systems and initiated a plan to eliminate or mitigate those risks. Since the issuance of our audit of IT security within the Department,[4] the OCIO has begun developing risk assessment checklists that cover the various system platforms used within the Department. The OCIO currently has three of the eight checklists completed, and anticipates having the remaining checklists completed in the first quarter of FY 2002. The OCIO will require agencies to use these checklists in assessing the risks to their systems, and use the checklists, itself, in conducting program reviews of agency systems. However, until the OCIO finalizes these checklists and requires their use, the Department is not in compliance with PDD 63 and cannot ensure that the risks to its critical systems and infrastructure have been identified and properly mitigated.

Contingency/Disaster Recovery

Eight of the 11 agencies we reviewed are not adequately prepared in the event of a natural disaster or other contingency that disrupts mission-critical systems and networks. (The Department's mainframe operations had adequate disaster and contingency plans in place.) Despite the requirement in OMB A-130 that agencies prepare and test contingency plans, the Department has not enforced this requirement or provided guidance to the agencies on the preparation and testing of contingency plans. In our prior audit, we found that the Department and its agencies were using Year 2000 contingency plans but those plans were not sufficiently comprehensive to address all potential service disruptions. In

[4] Audit Report No. 50099-27-FM, "Security Over USDA Information Technology Resources Needs Improvement," dated March 30, 2001.

response to that audit, the OCIO stated that it recognized the importance of contingency planning and testing, but stated that it could not implement a comprehensive, Department-wide contingency plan or require such actions by each agency due to the lack of funding and human resources required to implement such a program. Without contingency plans in place and properly tested to ensure effectiveness, the Department cannot be assured that its network and key agency operations can be quickly and effectively recovered to accomplish its mission in the event of an emergency.

System Certification and Authorization

In a prior audit of IT security,[5] we identified that four of the seven agencies in that review had not prepared or timely updated their systems' certification and authorizations. In addition, we noted at the time of our audit that the OCIO had not fully addressed the area of monitoring agencies' compliance with system certifications and authorization requirements. OMB A-130 requires agencies to provide a written authorization by a designated management official for the system to process information. Management authorization is based on managerial, operational, and technical controls in place to ensure that the system can be operated securely. Once initial authorization is in place, reauthorization should occur subsequent to a significant change in the system or when there is a high risk and potential of harm, but at least every 3 years.

Since that audit, the OCIO has begun to develop a database to track system certifications, authorizations, and agency contacts. The OCIO recognizes the requirement that agency systems, particularly those that process, handle, or store sensitive and classified data, be certified. However, OCIO does not intend to implement its Sensitive Certification Program until FY 2002. Without these authorizations in place, the Department cannot be assured that adequate security controls have been established for those systems and that those controls are operating effectively.

[5] Audit Report No. 50099-27-FM, "Security Over USDA Information Technology Resources Needs Improvement," dated March 30, 2001.

Security Incident Response

The Department has a well documented security incident response procedure in place and appears to be operating effectively at the Department level. However, the Department is not able to monitor all agencies' networks requiring monitoring at the agency level. At the Department level, the security incident response procedure ensures that the responsible agency personnel investigate and report on security incidents identified by the agencies or the Department's Intrusion Detection System; the procedure establishes requirements for working with external reporting entities such as the General Services Administration (GSA) Federal Incident Response Center (FedCIRC), ensuring that information on known vulnerabilities are timely distributed to the agencies, and communication with law enforcement, as necessary. Our review disclosed that suspect intrusion incidents detected at the Department level are being forwarded to agency personnel for follow up. Agencies are reporting their follow up results to the OCIO, and the OCIO is forwarding the results of intrusion incidents to the GSA FedCIRC. Our review also disclosed that the OCIO is working closely with the OIG in referring security incidents that require the involvement of external law enforcement entities.

Government Information Security Reform Act

In order to comply with the reporting requirements of the GISRA, OMB recommended that agencies conduct self-assessments of their security program. On July 2, 2001, the OCIO requested that each agency complete an OCIO-prepared self-assessment by July 31, 2001. The results of those assessments, along with the annual security plans submitted by the agencies on June 16, 2001, would serve as the basis of the overall security assessment for the Department. As of July 31, 2001, only a few of the Department's agencies had submitted those assessments to the OCIO. The OCIO is working closely with those agencies that have not submitted their assessments. Due to time constraints, we did not review the self assessments, and thus cannot report on the accuracy or adequacy of the self assessments.

IT Security Performance Measures

We reviewed the performance measures established by the OCIO and four agencies in our review. The OCIO has established a performance measure to implement a Department-level risk management program, ensuring that the Department's mission-critical systems are Year 2000 compliant, and meet the mandate of PDD 63 by developing a plan to protect USDA's critical infrastructures and putting the processes in place to implement the plan and update the plan on a 2-year cycle. However, there are no performance measures in place to ensure that individual agencies conduct risk assessments, implement security plans, or test and evaluate security controls and techniques. The OCIO reported that it met or exceeded its goals[6] in all but two performance goals, “Establishing a Department-level risk management program,” and “Developing an Information and Telecommunications Security Architecture.” The OCIO’s goal was to have 25 percent of the agencies identify mission-critical assets and assess the risks to those assets. However, the OCIO reported that only 20 percent of the agencies had completed this task. The year 2000 performance measures had not established a goal toward developing an information and telecommunications security architecture.

Our work in assessing the need for the Department and its agencies to establish IT related goals and performance measures is on-going and will be reported in Audit Report No. 50099-33-FM, “Security Over USDA Information Technology – Phase II.”

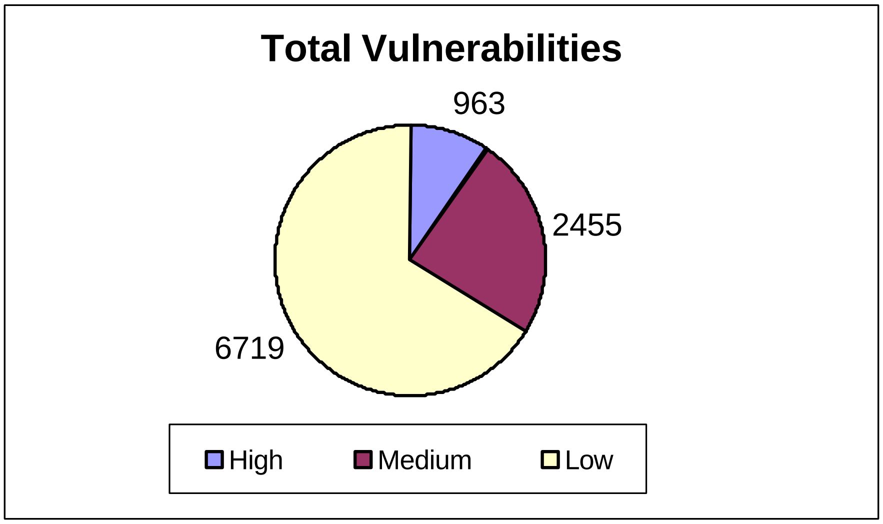
FINDING NO. 2

THE DEPARTMENT NEEDS TO IMPROVE MITIGATION OF KNOWN OPERATING SYSTEM VULNERABILITIES

Agencies need to take additional steps to better identify and mitigate known vulnerabilities in their servers’ operating systems. Most agencies cited a lack of financial and human resources to conduct these vulnerability assessments. Using a commercially available software program we identified over 3,400 potentially high and medium-risk[7] vulnerabilities in the nearly 1,300 systems we have scanned during our audits. This leaves the Department systems vulnerable to both internal and external threats, including Internet hackers, jeopardizing the integrity and confidentiality of the Department’s critical program, financial, and economic data.

[6] Performance measurements cited here were reported by OCIO and have not been independently validated by OIG.

[7] High-risk vulnerabilities are those that provide access to the computer, and possibly the network of computers. Medium-risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher-risk vulnerabilities. Low-risk vulnerabilities are those that provide access to sensitive, but less significant network data.



We conducted vulnerability assessments of selected network components at seven agencies. Our assessments were conducted from June 2000 to April 2001. The software used during our testing identifies vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP), the same protocol used on the global Internet.

Detailed below are a few examples of the high-risk vulnerabilities disclosed during our scans of the various agencies' systems:

- An error in the system's log could allow an attacker to run programs, including malicious programs, and disguise themselves as having full administrative privileges. For instance, an attacker could execute some type of Trojan horse, virus, or denial of service program that could cause substantial harm to the data and/or system.

- A system was configured to allow anyone to sign on as the Administrator by using a blank password. The Administrator is the most trusted user on the system and has complete control over the computer and can perform any function.

- Administrator accounts on several systems were set to allow access to the systems using a password that was the same as the Administrator's user Identification (ID).

- Software applications used to manage computer networks were left configured with their original default settings, which are well known by attackers. These vulnerabilities could allow an attacker to easily obtain or change system information and gain information about open connections with other systems.

We reported the weaknesses found at agency locations directly to agency management. Agency officials agreed with our results and reported taking immediate action to correct the problems. In some cases, we conducted a follow up assessment and found that significant progress had been made in correcting the identified vulnerabilities.

The OCIO has recently negotiated a Department-wide license to use the same vulnerability scanner software we used during our audits. Once the contract is in place, OCIO intends to issue a policy requiring agencies to periodically scan their systems and immediately correct the high and medium-risk vulnerabilities.

FINDING NO. 3

WEAK ACCESS CONTROLS COULD IMPACT THE INTEGRITY AND CONFIDENTIALITY OF THE DEPARTMENT'S CRITICAL DATA

Most agencies in our audits have not adequately, physically or logically, secured their network resources. Agencies have been lax in ensuring that network equipment is located in a secure area, that users are properly authorized to access network resources, and that users' access authority is not excessive as it relates to the performance of their assigned job functions. In today's increasingly interconnected computing environment, inadequate access controls can expose an agency's information and operations to attacks from remote locations by individuals with minimal computer or telecommunications resources and expertise.

Access controls over network resources include both physical and logical access controls and should provide reasonable assurance that computer resources (data files, application programs, and computer equipment) are protected against unauthorized modification, disclosure, loss, or impairment. 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 hardware. Logical access controls such as user names, passwords, and access permissions, ensure that only authorized users have access to network resources from their workstations, and that users are granted only the access that is needed to conduct their job responsibilities.

Physical Access Controls

- One audit disclosed that agencies share computer room space, allowing employees from all the combined agencies access to the other agencies' systems. Many of those systems contained sensitive and critical data. Those same agencies combine systems networking and telecommunications equipment in the same area, leaving telecommunication contractors inappropriate access to networking equipment. We witnessed contractor personnel leaving network equipment closets open and unattended; giving anyone unauthorized access to critical network hardware.

- We found inoperable locks; poor controls over electronic access equipment, such as key-card systems; and placement of network equipment rooms in high-traffic areas where physical access to systems could be easily obtained.

Logical Access Controls

- Nearly all agencies' systems we tested contained inactive or expired user accounts, accounts that belonged to users no longer employed, and/or accounts that did not limit login attempts.
- Five of the seven agencies could not provide an accurate list of system users, while four of the seven used shared user accounts and passwords.
- Many of the agencies we reviewed had not routinely reconciled a list of system users to a list of current employees and contractors.

An agency's inability to enforce its logical access controls exposes that agency's system settings and the data that reside on those systems to unauthorized modification, disclosure, or deletion.

FINDING NO. 4

SECURITY TRAINING AND CONTRACTOR COMPLIANCE WITH FEDERAL REQUIREMENTS NEED TO BE ADDRESSED

Our audit included tests at four agencies to ascertain the adequacy of training provided to employees. We found that agencies recognized the need for adequate training, but two of the four agencies were unable to provide evidence of the specific training given to their technical staff. The Computer Security Act of 1987 requires that agencies ensure their staffs receive periodic security awareness training; however, the Act does not define standards on training sufficiency. Currently, the Department does not have a minimum standard, based on continuing education hours or other quantitative means, by which to measure the sufficiency of training given to IT personnel. However, the OCIO has provided training to its Cyber-Security and incident response teams in furthering its oversight function, and also provided training to agency IT specialists on emerging technologies. Future audit work in IT security should provide additional insight into how agencies ensure their staffs are adequately trained, continued professional education standards that should be met, and costs associated with the training provided.

Our review of the Department's use of contractors that provide IT services has been limited to date, however future audit work in this area will be conducted. The Department uses numerous contractors to provide IT support, conduct risk assessments, prepare security plans, and provide network communication. Our initial review of contractor oversight at four agencies found that three do not ensure that contractors have the proper security clearances or background checks, or ensure that they are sufficiently trained in Federal security requirements. Only two of the four agencies we reviewed included Federal requirements in their statements of work, and only one of those two had a process in place to ensure that contractors understand Federal requirements before awarding the contract.

EXHIBIT A – OMB REPORTING REQUIREMENTS AND OIG POSITION

OMB REPORTING INSTRUCTIONS[8]	OIG COMMENTS
2. Identify the total number of programs included in the program reviews or independent evaluations.	We conducted IT security audits at 11 agencies and staff offices, which operate 258 of the estimated 340 general support and major application systems within the Department.
3. Describe the methodology used in the program reviews and the methodology used in the independent evaluations.	In performing our audit, we: (1) consolidated the results and analyzed the issues from our prior IT security audit work. Our audit work consisted primarily of performing selected audit procedures found in the General Accounting Office's Financial Information System Control Audit Manual, (2) evaluated OCIO's progress on implementing its Action Plan to Improve USDA Information Security, (3) evaluated OCIO's progress on implementing recommendations to correct material weaknesses in prior OIG and GAO audit reports, (4) evaluated the Department's security incident response procedures, (5) conducted selected audit procedures on the adequacy of agency training and use of contractor-provided IT services, and (6) conducted testing of four agencies' security program and their compliance with existing laws and regulations. Our audits were conducted in accordance with Government Auditing Standards.
4. Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law.	The following material weaknesses were identified as a result of our audit work. Agencies have not: (1) prepared/tested contingency or business continuity plans, (the Department's mainframe operations had adequate contingency and business continuity plans in place) (2) properly certified security controls on systems, (3) assessed the risks to their systems nor established plans to mitigate those risks, (4) established adequate controls to ensure only authorized users can access critical agency data, or (5) periodically identify and mitigate known operating vulnerabilities that may exist on their systems.

[8] OMB M-01-24, dated June 22, 2001 does not require OIG's to address reporting requirement No. 1.

EXHIBIT A – OMB REPORTING REQUIREMENTS AND OIG POSITION

5. The specific measures of performance used by the agency to ensure that agency program officials have: (1) assessed the risk to operations and assets under their control; (2) determined the level of security appropriate to protect such operations and assets; (3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and (4) tested and evaluated security controls and techniques. Include information on the actual performance for each of the four categories.	• Nine of 11 agencies have not assessed the risks to their systems or initiated plans to mitigate those risks. • Department OCIO is developing checklists to assist agencies in evaluating risks. • OCIO requested agencies conduct overall self-assessments of their IT security operations (Results not available in time for our evaluation.) • Department cannot determine level of security appropriate to protect mission critical IT resources. • Agencies are preparing security plans annually through OCIO guidance. • Agencies needed to practice security plan throughout their systems' life cycle. Our audits found: (1) Non-existent or inadequate access controls (logical/physical), (2) no controls in place to identify/mitigate known vulnerabilities in Operating Systems, and (3) outdated or nonexistent system certifications.
6. The specific measures of performance used by the agency to ensure that the agency CIO: 1) adequately maintains an agency-wide security program; 2) ensures the effective implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories.	Thus far, the OCIO has: • Established a Department-wide security plan. • Chartered committees comprised of agency IT professionals and business managers to evaluate standards/policies. • Staffed a Cyber-Security team to conduct reviews of agencies' security programs. • Assembled Cyber-Security response team to protect sensitive systems. • Established nine new policies covering topics such as: security plan preparation, incident response, logical access controls, physical security standards, server and firewall security, and capital planning and investment control. • OCIO now requires annual reporting of agency security plans, requiring they be transmitted through agency's administrators. • OCIO Office of Cyber-Security has begun conducting agency security program reviews. OCIO has completed 3 such reviews.

EXHIBIT A – OMB REPORTING REQUIREMENTS AND OIG POSITION

7. How the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.	Tested four agencies to ascertain the adequacy of training provided. Our work was limited in this area; however, we plan to cover this area further in future audits. • Computer Security Act of 1987 requires agencies ensure staff receives periodic security awareness training, although does not define standards. • Currently, the Department does not have a minimum standard, based on continuing education hours or other quantitative means, by which to measure the sufficiency of training given to IT personnel. • Agencies recognized need for adequate training. • Two of four were unable to provide specific training documentation given to technical staff. • OCIO has provided training for cyber security and incident response teams in furthering its oversight function. • OCIO also coordinates some training for agency IT specialists.
8. The agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's FedCIRC. Include information on the actual performance and the number of incidents reported.	Department has documented security incident response procedure in place. • Based on our review, it is operating effectively at the Department level. • Ensures responsible agency personnel investigate/report security incidents identified by agencies or Departments Intrusion Detection System. • Establishes procedure for working with external reporting entities. • Suspect intrusion incidents are being forwarded to agency personnel for investigation. • Agencies are reporting investigation results to OCIO. • OCIO is forwarding results to GSA FedCIRC. • OCIO is working closely with OIG in referring security incidents requiring involvement of external law enforcement entities. • Agencies need to conduct their own comprehensive monitoring to ensure an effectively implemented security incident response program.

EXHIBIT A – OMB REPORTING REQUIREMENTS AND OIG POSITION

9. How the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY 2002 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not?	Our work was limited in this area; however, we plan to cover this area in future audits. Department has established comprehensive CPIC program that: (1) requires agencies to identify security requirements of proposed systems, (2) requires agencies to quantify costs of security requirements, (3) integrates I-TIPS to track/report status of IT investments throughout GAO-recommended select, control, and evaluate approach, and (4) calls for review/approval at each stage in major, Department priority systems by a Department review board. Although additional work is needed to ensure the effectiveness at the agency level, our initial review disclosed that agencies were following CPIC program, and were using ITIPS to track IT investments.
10. The specific methodology (e.g., Project Matrix review) used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented.	The Department identified, during Year 2000 conversion, over 340 systems that it operates, 52 of which designated by Secretary as mission critical. Our review at 4 agencies showed each agency established their own method of identifying, prioritizing, and determining criticality of systems. One agency used matrix of integrity, availability, and confidentiality, while the others did not prioritize systems, merely identifying all as major applications in their security plans. Our review also disclosed that agencies have not taken steps to properly protect their IT assets. We found: • Inadequate logical access controls such as failure to remove user IDs of separated employees. • Use of easily guessed passwords on administrator accounts. • Vulnerability scans identifying over 3,400 potentially high and medium severity threats to agency systems using TCP/IP protocol.

EXHIBIT A – OMB REPORTING REQUIREMENTS AND OIG POSITION

11. The measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance.	While agencies have prepared security plans, we question the agencies' implementation of those plans. Our audits have found: (1) Non-existent or inadequate physical/logical access controls, (2) No controls in place to identify/mitigate known vulnerabilities in operating system software, and (3) Outdated or non-existent system certifications. OCIO has begun addressing this issue by: (1) Requiring security plans be forwarded to them through agency administrators, and (2) conducting its own program reviews of agencies' security programs. The OCIO has established a performance measure to implement a Department-level risk management program, ensuring that the Department's mission-critical systems are Year 2000 compliant, and meet the mandate of PDD 63 by developing a plan to protect USDA's critical infrastructures and putting the processes in place to implement the plan and update the plan on a 2-year cycle. However, there are no performance measures in place to ensure that individual agencies conduct risk assessments, implement security plans, or test and evaluate security controls and techniques.
12. How the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., physical and operational).	Our work was limited in this area; however, we plan to cover this area in future audits. • Department has prepared Critical Infrastructure Assurance Plan which fairly and accurately reflects requirements of PDD 63, but it was not adequately carried out. • OCIO has begun to address issues of risk assessment/mitigation by developing risk assessment checklists usable by agency officials to identify risks to various IT systems.
13. The specific methods (e.g., audits or inspections) used by the agency to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and Nation Institute of Standards and Technology guidance, national security policy, and agency policy.	Our work was limited in this area; however, we plan to cover this area in future audits. Our initial review of contractor oversight at four agencies found most do not ensure contractors have: (1) Proper security clearances or background checks, and (2) Sufficient training in Federal security requirements.

EXHIBIT B – STATUS OF RECOMMENDATIONS IN THE ACTION PLAN TO STRENGTHEN USDA INFORMATION SECURITY

ACTION PLAN RECOMMENDATIONS SECURITY PROGRAM MANAGEMENT	OCIO ACTIONS to DATE	STATUS
Designate an Associate CIO for Cyber-Security and establish a central management focal point to carry out key activities.	An Associate CIO was appointed as the head of Cyber-Security in February 2000. His duties include developing and implementing a cyber-security program.	Reported as completed February 2000
Establish structures to provide the central group and agency IT staffs ready and independent access to senior executives.	The Cyber-Security Advisory Council was established in 2nd quarter FY 2001. The Council consists of senior executive program officials and IT personnel from across the Department. It brings agency business and technology perspectives to decisions regarding security controls, costs, and management.	Reported as established 2nd quarter FY 2001
Establish procedures to hold program and business managers accountable.	OMB has issued guidance on capital planning/investment control requiring all new applications for budget requests to include components on security as part of the IT system and architecture. OCIO is using this guidance on the budget process to hold business managers accountable and ensure they address IT security concerns throughout their programs.	Reported as completed February 2000
PERSONNEL		
Assess Cyber-Security staffing needs.	The Associate CIO for Cyber-Security has increased staffing from 10 to 19 full-time employees.	Reported as completed 3rd quarter FY 2001
Implement systematic training to enhance IT staff professionalism and technical skills.	Training is conducted on a continual basis for OCIO staff and agency personnel. In the 3rd quarter FY 2001, the Cyber-Security Incident Response Team completed training on detecting and responding to hacker activity. Training on router security architecture was provided to agency personnel, and the OCIO facilitated a computer forensics course for agency security specialists and systems administrators.	On-going

EXHIBIT B – STATUS OF RECOMMENDATIONS IN THE ACTION PLAN TO STRENGTHEN USDA INFORMATION SECURITY

ACTION PLAN RECOMMENDATIONS	OCIO ACTIONS to DATE	STATUS
Implement user-friendly strategies to educate users and others on risks and related policies.	A contract for user/manager training on risk analysis is underway. The contractors will develop a checklist for each platform to aid in the identification of risks. The training will teach the users/managers how to properly use the checklists as risk management tools. The contractor will conduct one assessment for each platform. The users/managers will then use the checklist to complete assessments of all 52 mission critical systems.	Three of the eight risk analysis checklists have been completed. OCIO reports that the remaining five checklists are to be completed by 1st quarter FY 2002.
Establish a close link between human resources processes and information security.	The Associate CIO for Cyber-Security has increased its staff from 10 to 19 full-time employees.	On-going
POLICY AND PROGRAM OPERATIONS		
Develop practical risk assessment procedures that link security to business needs; manage risks on a continuing basis.	Managers/users will be undergoing risk assessment training utilizing contractor prepared, platform specific, checklists. Further, the OCIO has established the Cyber-Security Advisory Council, which brings both business and technology perspectives to decisions regarding security controls, costs, and management.	OCIO reported that training is provided as contractor-supplied checklists are being completed. OCIO reports that the final checklists are scheduled to be completed 1st quarter FY 2002.

EXHIBIT B – STATUS OF RECOMMENDATIONS IN THE ACTION PLAN TO STRENGTHEN USDA INFORMATION SECURITY

ACTION PLAN RECOMMENDATIONS	OCIO ACTIONS to DATE	STATUS
Implement appropriate policies and related controls that are linked to the Department's business risks.	The Office of Cyber-Security has drafted or finalized 9 information technology security-related policies. These policies include (1) mainframe security, (2) incident reporting, (3) security plan guidance, (4) security requirements for the use of private Internet access providers, (5) user ID and password requirements, (6) privacy policy on the use of customer information (i.e., cookies), (7) server and firewall security, use of network protocol analyzers, (8) physical security standards and use of configuration management, and (9) guidance on security requirements relating to CPIC.	On going
Immediately clarify management's support for security policies and guidelines.	The established Cyber-Security Advisory Council includes senior executive program officials allowing business perspectives to be recognized in decisions regarding security controls and management. Further, the OCIO has stressed the importance of annual security plans by requiring agency administrators to approve and submit the plans to the OCIO.	On going
Establish procedures to monitor and evaluate policy and control effectiveness; use the results to direct future activities.	The OCIO has a dedicated policy coordinator that is responsible for monitoring and evaluating policies and their subsequent effectiveness.	Reported as completed 2nd quarter FY 2001
Be alert to and implement new monitoring tools and techniques.	New firewalls were installed across the backbone in the Fall of 2000. An intrusion detection system (IDS) has been placed in service. The IDS system is monitored continually and security incidents are reported to appropriate agency staff for follow up. The OCIO has established incident reporting procedures that guide agencies to follow up on and report possible security incidents. This guidance has provisions for working with law enforcement officials when appropriate.	Reported as completed December 2000

EXHIBIT B – STATUS OF RECOMMENDATIONS IN THE ACTION PLAN TO STRENGTHEN USDA INFORMATION SECURITY

ACTION PLAN RECOMMENDATIONS	OCIO ACTIONS to DATE	STATUS
TECHNICAL INFRASTRUCTURE		
Coordinate the design and implementation of department-wide information security architecture.	OCIO recently received a budget increase to be used specifically for architecture. A contractor is finalizing its analysis of the backbone network security needs. Funding has been set-aside in the FY 2001 and FY 2002 budgets to procure the needed components to improve on the architecture. OCIO is also exploring a web-farm strategy. These are groups of computers that will support internet-based applications. This development, if successful, will become the model for future Internet activity.	OCIO reported that the contractor analysis was completed 2nd Quarter FY 2001 and that procurement of equipment will extend through 4th Quarter FY 2002
Establish a common telecommunications wide area network to include a central telecommunications operations center.	OCIO has established a Telecom Technical Advisory Board, which has a representative from each Under Secretary mission area. A project manager for the Universal Telecommunications Network (UTN) begins July 30, 2001.	OCIO reported that the advisory board and the UTN manager are in place; however the UTN operations are on-going
Centrally coordinate current USDA Cyber-Security initiatives.	Security initiatives have been developed and centralized in the office of the Associate CIO for Cyber-Security.	Reported completed February 2000

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 50099-28-FM, "PCIE/ECIE Critical Infrastructure Protection Review."

Recommendation	Actions to Date	Estimated Completion Date
Revise the Critical Infrastructure Assurance Plan to update timeframes for USDA PDD-63 compliance.	OCIO is contracting for risk assessment checklists that will allow agencies to assess the risks to various system platforms used within the Department.	OCIO reported that the final risk assessments checklists are scheduled to be completed 1st quarter 2002. OCIO reports to initiate plans to have the USDA mission-critical systems assessed by second quarter 2003 with mitigation strategies for these systems by third quarter 2003.
Continue to seek funding to ensure adequate resources and staff to carryout the requirements of PDD-63.	OCIO obtained funding in FY 2001 to implement a risk management program. OCIO is in the process of procuring for risk assessment checklists that can be used by the Department to continually assess the risks to its networks.	OCIO reported that the final risk assessments checklists are scheduled to be completed 1st quarter 2002.
Propose a council to ensure senior management is involved in cyber security and PDD-63 compliance activities.	OCIO established a Risk Management Work Group to assist in implementing its risk management program. This program requires training of agency technicians and functional managers to institutionalize risk management within the Department.	OCIO reports that training provided to technicians and functional managers will be completed by 4th quarter 2001.

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 23099-1-FM, "Security over Data Transmission in the Department Needs Improvement."

Recommendation	Actions to Date	Estimated Completion Date
Eliminate the risk of fraud and misuse of sensitive information posed by agencies transmitting unencrypted data over the Internet and Department networks.	OCIO contracted for a risk assessment and analysis of the Department backbone security needs.	OCIO reports that it has received the results of the assessment and are still analyzing it to determine the proper course of action. OCIO reported that it intends to begin procuring encryption equipment to encrypt backbone traffic by the end of FY 2001 and will continue to procure such equipment in FY 2002.
Implement appropriate safeguards to secure the link between National Technology Information Center (NITC) and the National Finance Center (NFC).	OCIO has contracted a study of backbone security and has implemented Virtual Private Network (VPN) encryption.	OCIO reported that once backbone encryption equipment is implemented, all backbone traffic, including traffic between NITC and NFC will be encrypted. Estimated completion in FY 2002.
Strengthen DR3140-2 by requiring that all data transmitted by agencies over the Internet and Intranet be encrypted, and require that NITC and NFC no longer accept unencrypted data from any source.	OCIO has taken steps to ensure that NFC and NITC encrypt data. Further, once OCIO has encrypted the backbone, all interagency data traveling over the backbone will be encrypted.	OCIO reported that it intends to begin procuring encryption equipment to encrypt backbone traffic by the end of FY 2001 and will continue to procure such equipment in FY 2002.
Take immediate action to eliminate the vulnerabilities identified by the OIG vulnerability scans.	OCIO took immediate action to eliminate the vulnerabilities identified by OIG's vulnerability assessment.	Reported as completed 3rd quarter 2000.
Establish a process to scan the remaining computers, routers, and other equipment that are a part of the Department's network. Ensure that periodic reviews and risk assessments are performed on the network.	OCIO has negotiated a Department-wide license for vulnerability scanning software available to all agencies to scan their systems and network devices.	Department-wide negotiations for vulnerability scanning software was completed in 4th quarter 2001.

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 23099-1-FM, “Security over Data Transmission in the Department Needs Improvement.”

Recommendation	Actions to Date	Estimated Completion Date
Implement a network intrusion detection system and an emergency response team to ensure the timely detection, correction, and tracking of unauthorized activities.	OCIO has implemented an intrusion detection system at all Internet access points to the Department backbone.	Reported as completed 3rd quarter 2000.

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 50099-27-FM, "Security over USDA Information Technology Resources Needs Improvement."

Recommendation	Actions to Date	Estimated Completion Date
Redirect OCIO resources to the security areas noted in this report until funding is obtained to implement a comprehensive security program within USDA.	OCIO continues to give consideration, as appropriate, to the Cyber -Security areas noted in the report. Specifically, OCIO actions toward supporting the Cyber-Security Program during the past year include: (1) Elevating Cyber-Security Program initiative to the highest priority in our budget request formulation, (2) including Cyber-Security Program initiatives in our request for unobligated FY 2000 funds, and (3) Including Cyber-Security Program initiatives in the redistribution of unobligated Year 2000 Program funds.	On-going
Monitor agency corrective actions on all security weaknesses identified by our audit to ensure weaknesses have been corrected.	OCIO is developing a process for monitoring corrective action on all security weaknesses identified by OIG audits. This process will include not only OCIO's responsibility for oversight, but also the criteria for which actions require monitoring, timing for responses, authority for certifying corrections, and other related issues.	OCIO reported that this monitoring process will be implemented by January 2002

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 50099-27-FM, "Security over USDA Information Technology Resources Needs Improvement."

Recommendation	Actions to Date	Estimated Completion Date
Establish a risk assessment policy that requires agencies to keep network documentation updated, requires periodic risk assessments, sets timeframes for agency compliance, and establishes OCIO's review and oversight responsibility.	OCIO is currently contracting for a set of security assessment checklists agencies will use to conduct self-assessments and OCIO will use to conduct independent assessments. Following the assessment tool development, policies will be developed and distributed to establish assessment requirements, responsibilities, timeframes, documentation and reporting. Agency responsibilities for conducting risk assessments will be clearly defined.	OCIO reported that assessment tools will be developed through Summer and Fall of 2001. OCIO reported that a policy on implementing the assessment tools will be implemented by January 2002.
Revise OCIO instructions on the preparation of Agency Security Plans to include all areas required by OMB A-130.	OCIO's guidance to agencies for developing and submitting security plans has been revised.	Reported as completed June 2001.
Establish a security plan policy that establishes agency timeframes for completing and updating their security plans, requires these plans to be submitted to OCIO, and formalizes OCIO's review and oversight responsibility.	A policy is being developed that establishes agency timeframes for completing and updating security plans, requires plan submission to OCIO and formalizes OCIO's review and oversight responsibility.	OCIO reported that a policy will be implemented 4th quarter FY 2001.
Require agencies to prepare and submit to OCIO comprehensive and system-specific contingency plans that address protection of information resources and recovery procedures in the event of service disruptions. Establish procedures for OCIO to review and approve agencies' contingency plans.	While OCIO recognizes the importance of contingency plans, disaster recovery procedures, and business resumption plans, additional funding is required to conduct these labor-intensive, management-demanding endeavors. OCIO plans to continue funding requests for these endeavors.	OCIO reported that no timeframes have been established for requiring agencies to submit comprehensive and system-specific contingency plans.

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 50099-27-FM, "Security over USDA Information Technology Resources Needs Improvement."

Recommendation	Actions to Date	Estimated Completion Date
Require agencies to perform annual testing of their contingency plans, adjust their plans based on the results, and report their test results to OCIO.	While OCIO concurs with the recommendation, limited resources has prevented the OCIO from implementing its Information Survivability Program.	OCIO reported that no timeframes have been established by OCIO to require agencies to test their contingency plans, adjust their plans as necessary, and provide the test results to OCIO.
Ensure agency compliance with OMB A-130 requirements for system certification/ authorization by establishing a policy that formalizes OCIO's review and oversight of these certifications.	The OCIO Cyber-Security Implementation Plan schedules the initiation of a Sensitive Certification Program in FY 2002, provided additional funding is obtained.	Reported completion FY 2002.
Establish controls to ensure that an accurate and timely updated database is maintained of IP addresses and responsible agency contacts.	OCIO has developed procedures that require each agency to develop an inventory of respective agency addresses, submit these inventories to OCIO and provide updates at least quarterly. The Cyber-Security Program Office has received all IP address inventories. To manage the large number of addresses, the Cyber-Security Program Office has initiated an effort to engage a contractor to build a database with appropriate reporting and query capabilities.	OCIO reported that the IP address tracking database is anticipated to be delivered by January 2002.

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 50099-27-FM, “Security over USDA Information Technology Resources Needs Improvement.”

Recommendation	Actions to Date	Estimated Completion Date
Establish Departmental policy requiring agencies to scan their systems on a routine basis and take prompt action to eliminate noted vulnerabilities.	The Cyber-Security Program Office has negotiated a contract that will provide network scanning tools to all USDA agencies and is working with agencies to obtain funding. When put in place, training and support will be provided.	OCIO reported that by the end of November 2001, it will issue a policy that establishes agency requirements for the timing and reporting of network and system scans.
Ensure that the agencies in our review have taken the necessary corrective actions on all high and medium-risk vulnerabilities identified during our audit. Where long-term corrective actions are needed to fix system vulnerabilities, require agencies to develop interim corrective actions, subject to OCIO approval.	OCIO will develop a process for monitoring corrective action on all security weaknesses identified by OIG audits. This process will include not only OCIO’s responsibility for oversight, but also the criteria for which actions require monitoring, timing for responses, authority for certifying corrections, and other related issues.	OCIO reported that this process will be implemented by January 2002.
Require agencies to adopt a corporate level approach to configuration management. To this end, develop a policy establishing minimum security setting guidelines for the various operating systems used by the Department. Require agencies to periodically assess those settings and correct those that have been misapplied.	A security expert who specializes in configuration management has been hired to the Cyber-Security Program Office staff, has developed and delivered configuration management training to agency technicians, and is developing interim configuration management guidance.	For the long term, OCIO reported that it plans to implement Department-wide configuration management within its Sensitive System Certification and Accreditation Program, scheduled to begin in FY 2002.

EXHIBIT C – STATUS OF RECOMMENDATIONS FROM PRIOR AUDITS

Audit Report No. 50099-27-FM, “Security over USDA Information Technology Resources Needs Improvement.”

Recommendation	Actions to Date	Estimated Completion Date
Update the firewall policy to require that agencies implement firewalls between their networks and the Department’s backbone. Once implemented, monitor agencies’ compliance with the new policy.	OCIO is conducting an analysis on this recommendation.	OCIO reported that no timeframe has been estimated on the implementation of this recommendation.
Monitor agencies corrective actions on the cited access controls until the weaknesses identified have been corrected.	OCIO will develop a process for monitoring corrective action on all security weaknesses identified by OIG audits. This process will include not only OCIO’s responsibility for oversight, but also the criteria for which actions require monitoring, timing for responses, authority for certifying corrections, and other related issues.	OCIO reported that this process will be implemented by January 2002.
Establish a policy requiring agencies to routinely review system accesses to ensure that terminated employees no longer have access to agency systems. Include a requirement that agencies periodically reconcile system users and access levels with current employees and contractors and remove or modify accounts as necessary.	OCIO anticipates issuing policy regarding unauthorized access, including terminated employees by September 2001.	OCIO reported that this will be completed September 2001
Provide guidance to agencies on how to physically secure all network critical hardware and ensure that controls are in place to limit physical access to authorized individuals only.	OCIO has concluded its initial physical security vulnerability assessment checklist. Agencies will use this guide to meet the requirements of system vulnerability assessment.	OCIO reported that a policy establishing the timely and reporting of vulnerability assessments is scheduled to be issued by January 2002.

ABBREVIATIONS

CIO	Chief Financial Officer
CPIC	Capital Planning and Investment Control
e-government	Electronic Business
FedCIRC	Federal Incident Response Center
FY	Fiscal Year
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GSA	General Services Administration
ID	Identification
IDS	Intrusion Detection System
IT	Information Technology
I-TIPS	Information Technology Investment Portfolio System
NFC	National Finance Center
NITC	National Information Technology Center
OCIO	Office of Chief Information Office
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
TCP/IP	Transmission Control Protocol/ Internet Protocol
USDA	U.S. Department of Agriculture
UTN	Universal Telecommunications Network
VPN	Virtual Private Network