



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

SECURITY OVER USDA INFORMATION
TECHNOLOGY RESOURCES NEEDS
IMPROVEMENT



**Audit Report No.
50099-27-FM
March 2001**



UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF INSPECTOR GENERAL
Washington D.C. 20250



DATE: March 30, 2001

REPLY TO
ATTN OF: 50099-27-FM

SUBJECT: Security Over USDA Information Technology Resources

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

This report presents the results of our audit of the Security Over UDSA Information Technology Resources. The report identifies serious weaknesses in the Department's ability to protect its critical information technology resources. While the OCIO has substantial actions underway, additional measures are needed to further strengthen information technology security in the Department.

Your response to our draft report is included in its entirety in exhibit C, with excerpts incorporated in the findings and recommendations section of the report. Based on the information provided in the response, we have reached management decision for Recommendations Nos. 4, 5, 8, and 12. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer.

We concur with your proposed actions for Recommendations Nos. 1, 2, 3, 11, 14, 15, and 16. However, to achieve management decision, you need to provide us with timeframes for implementing the cited actions. To reach management decision for Recommendations Nos. 6, 7, 9, 10, and 13 we need additional information. Please refer to the OIG Response sections 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 recommendations 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.

We appreciate the courtesies and cooperation extended to us during this audit.

/s/

ROGER C. VIADERO
Inspector General

EXECUTIVE SUMMARY

SECURITY OVER USDA INFORMATION TECHNOLOGY RESOURCES NEEDS IMPROVEMENT

AUDIT REPORT NO. 50099-27-FM

RESULTS IN BRIEF

We identified serious weaknesses in the Department's ability to adequately protect its (1) assets from potential fraud and misuse, (2) sensitive information from inappropriate disclosure, and (3) critical operations from potential disruptions. Significant information security weaknesses were reported in each of the seven agencies¹ tested, with inadequately restricted access to sensitive data being the most widely reported problem. This and other identified weaknesses place critical departmental operations, as well as the assets associated with these operations, at high risk. The Department relies on its information technology (IT) infrastructure and individual agency systems to issue billions of dollars in payroll and loan disbursements; supply market-sensitive data on commodities to the agricultural economy; and manage other critical departmental programs.

The Office of the Chief Information Officer (OCIO) has demonstrated its commitment to protecting the Department's IT infrastructure through recent, substantial increases in IT security measures. The Chief Information Officer (CIO) has taken the following steps to strengthen the Department's IT security program:

- hiring a senior manager for Cyber-Security, and assigning staff members to work on the cyber-security team; and hiring additional staff with expertise in physical security, configuration management, and access controls;
- implementing 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 to assist in designing standards and policies; analyzing the Department's wide area network security needs to detect and monitor network traffic;

¹ Testing at one agency was limited to vulnerability scans.

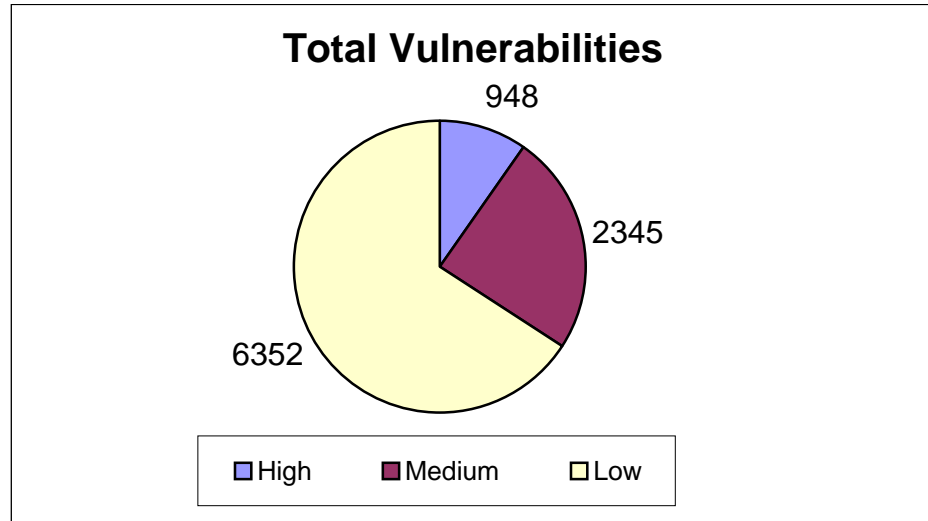
- assembling a permanent cyber-security response team to protect sensitive systems; and
- implementing three new policies concerning gateways and firewalls, securing sensitive information on server computers, and security procurement standards.

While substantial actions are underway, we believe additional measures must be taken to further strengthen IT security in the Department. The Department has not yet fully implemented a comprehensive security program. The OCIO advised that the office has been hampered from establishing and maintaining a comprehensive security program because of lack of funding and personnel. Also, historically, Departmental agencies and staff offices have separately addressed their respective IT security and infrastructure needs, thus making decision and policy implementation even more difficult. These isolated approaches taken by individual agencies have resulted in a disparate array of technical and physical solutions that do not always assure that comprehensive department-wide security is obtained.

To test the vulnerability of the Department to the threat of security intrusions, we conducted an assessment of selected USDA agencies' networks, using a commercially available software product, which is designed to identify risk indicators associated with various operating systems. Our assessments, performed between June and December 2000, on over 1,200 USDA network devices, identified nearly 3,300 high and medium IT security vulnerabilities² at the 7 agencies in our review. As we concluded each assessment, we communicated the results to agency management, who took immediate action to mitigate the vulnerabilities within their respective systems.³ In addition, we identified numerous low-risk vulnerabilities, many of which, while not critical to system security, can be an indication of poor systems administration. The following chart summarizes the vulnerabilities we identified:

² 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.

³ The agencies have advised us that many of the vulnerabilities have been corrected. However, we have not conducted a formal review of these corrections.



To illustrate the seriousness of the problems, a few examples are detailed below:

- 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 a system; therefore, the Administrator has complete control over the system and can perform any function.
- Administrator accounts on three other systems were set to allow access by using a password that was the same as the Administrator’s Login Identification (ID).

Our audit testing also disclosed that all agencies tested had poor controls over physical and logical access to sensitive data and systems. These types of weaknesses make it possible for an individual or group to inappropriately modify or destroy sensitive data or computer programs or inappropriately obtain and disclose confidential information. These weaknesses, coupled with the vulnerabilities noted above substantially increases the security vulnerabilities within the Department. 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. Further, these weaknesses place a broad range of critical operations and assets at great risk of fraud, misuse, and disruption. For example, weaknesses at one agency increase the vulnerability of various market sensitive data, while weaknesses at another agency increase the risk of fraud associated with billions of dollars of USDA payments. In addition, information security weaknesses place an enormous amount of highly sensitive data at risk of inappropriate disclosure.

As significant as the weaknesses identified are, it is likely that the full extent of control problems at individual agencies have not yet been identified because key areas of controls at many agencies have not been assessed. Our audit, while disclosing numerous security weaknesses, was limited to only selected sites at seven agencies. Additionally, in a prior audit,⁴ we disclosed that agency managers, who are primarily responsible for ensuring adequate security, have not fully identified risks to their systems or evaluated the adequacy of their computer-based controls.

Based on the extent and magnitude of the problems noted, we believe that IT security vulnerabilities are systemic in the Department, and if not timely and effectively corrected could negatively impact the Department's most sensitive data and financial-related systems. With assets of \$124 billion and an extensive range of critical missions related to public health, rural development, food safety, etc., it is imperative that corporate level actions are taken to identify problems and initiate necessary remediation efforts.

KEY RECOMMENDATIONS

We recommended that OCIO:

- Redirect OCIO resources to the security areas noted in this report until funding is obtained to implement a comprehensive security program within USDA;
- monitor agency corrective actions on all security weaknesses identified by our audit to ensure weaknesses have been corrected;
- 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;
- revise OCIO instructions on the preparation of Agency Security Plans to include all areas required by Office of Management and Budget (OMB) A-130;
- 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;
- require agencies to prepare, test, 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;

⁴ Audit Report 50099-28-FM, "PCIE/ECIE Critical Infrastructure Protection Review," dated July 18, 2000.

- 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;
- establish Departmental policy requiring agencies to scan their systems on a routine basis and take prompt action to eliminate noted vulnerabilities;
- require agencies to adopt a corporate level approach to configuration management;
- update the firewall policy to require that agencies' implement firewalls between their networks and the Department's backbone; and
- 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.

AGENCY RESPONSE

The OCIO agreed with our recommendations and has initiated significant corrective actions.

OIG POSITION

We concurred with the OCIO's proposed corrective actions in most areas. However, we need additional information to enable us to reach management decision in several areas.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
RESULTS IN BRIEF	i
KEY RECOMMENDATIONS	iv
AGENCY RESPONSE.....	v
OIG POSITION	v
TABLE OF CONTENTS	vi
INTRODUCTION	1
BACKGROUND.....	1
OBJECTIVES	3
SCOPE	3
METHODOLOGY	4
FINDINGS AND RECOMMENDATIONS.....	5
CHAPTER 1.....	5
USDA HAS NOT ENSURED COMPLIANCE WITH FEDERALLY MANDATED SECURITY GUIDELINES AND IS LACKING IN ITS OVERALL MANAGEMENT OF INFORMATION TECHNOLOGY RESOURCES.....	5
FINDING NO. 1	5
RECOMMENDATION NO. 1.....	11
RECOMMENDATION NO. 2.....	11
RECOMMENDATION NO. 3.....	11
RECOMMENDATION NO. 4.....	12
RECOMMENDATION NO. 5.....	13
RECOMMENDATION NO. 6.....	13
RECOMMENDATION NO. 7.....	14
RECOMMENDATION NO. 8.....	14
RECOMMENDATION NO. 9.....	15

CHAPTER 2..... 16
VULNERABILITIES EXPOSE DEPARTMENT SYSTEMS TO THE RISK OF MALICIOUS ATTACKS FROM INTERNAL THREATS AND FROM THE INTERNET 16
FINDING NO. 2..... 16
RECOMMENDATION NO. 10..... 19
RECOMMENDATION NO. 11..... 20
RECOMMENDATION NO. 12..... 20
RECOMMENDATION NO. 13..... 21
CHAPTER 3..... 22
WEAK ACCESS CONTROLS THROUGHOUT THE DEPARTMENT JEOPARDIZE THE INTEGRITY AND CONFIDENTIALITY OF ITS CRITICAL DATA 22
FINDING NO. 3..... 22
RECOMMENDATION NO. 14..... 24
RECOMMENDATION NO. 15..... 25
RECOMMENDATION NO. 16..... 25
EXHIBIT A – Status of Recommendations in the Action Plan to Strengthen USDA Information Security 27
EXHIBIT B – Status of Recommendations in From Prior Audits 29
EXHIBIT C – Auditee Response To Draft Report..... 31
ABBREVIATIONS 36

INTRODUCTION

BACKGROUND

Information security, improving the overall management of information technology (IT) resources, and the transition to electronic business (e-government), has emerged as a top priority within 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 disruptions. Threats range from those posed by insiders, and recreational and institutional hackers to attacks by intelligence organizations of other countries.

Various 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 1997 and Presidential Decision Directive (PDD) 63, "Policy on Critical Infrastructure Protection." Additionally, the Government Information Security Reform Act was enacted on October 30, 2000; which essentially codifies the existing requirements of Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources. 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.

Considerable guidance on information security has also been developed. The National Institute of Standards and Technology (NIST)⁵ has issued numerous Federal Information Processing Standards, as well as a comprehensive description of basic concepts and techniques entitled An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, October 1995, and Generally Accepted Principles and Practices for Security Information Technology Systems, published in September 1996.

⁵ The Computer Security Act of 1987 assigned NIST primary responsibility for developing technical standards and providing related guidance. Their responsibilities were reemphasized in the Clinger-Cohen Act of 1996.

The USDA uses a wide range of computers and telecommunication systems to process and manage its programs. These systems account for billions in assets and payments, and store vast amounts of sensitive and critical data. Some of the data that is processed through these systems include transactions that:

- control the issuance of billions of dollars in payroll and administrative expenses;
- provide market sensitive data on commodities and the agricultural economy;
- control the issuance of billions of dollars in loan, grant and farm programs payments; and,
- enable access to sensitive and Privacy Act databases on borrowers, Government personnel, and numerous other critical programs/operations.

Historically, USDA agencies and departmental staff offices have separately addressed their respective IT security and infrastructure needs. These isolated approaches have resulted in a broad array of technical and physical solutions that do not assure that complete department-wide security is obtained.

The Federal Critical Infrastructure Assurance Office, organized to implement the requirements of PDD 63, has designated USDA as one of the 14 civilian agencies having systems, which, if sabotaged, could cripple the Nation's economy and security. With assets of \$124 billion and an extensive range of critical missions related to public health, rural development, food safety, etc., it is imperative that corporate level actions are taken to identify problems and initiate necessary remediation efforts.

Protecting these assets must be a top priority for USDA's program managers as well as information technology staffs, especially as the Department makes more programs and information available over the Internet. Safeguards such as encryption, data backup procedures, network intrusion detection systems, disaster recovery and contingency planning can be employed to afford some degree of security. However, due to the increasing interconnectivity of computer systems, vulnerabilities on one system can lead to exploits on other systems; therefore, the Department is only as secure as its weakest link.

In May 1998, the General Accounting Office (GAO) issued its report, "Executive Guide, Information Security Management, Learning from Leading Organizations." This report emphasized risk management principals that leading organizations have implemented, including (1) periodically assess risks and needs, (2) establish a central management

focal point, (3) implement appropriate policies and controls, (4) promote awareness of prevailing risks and mitigating controls, and (5) monitor and evaluate the effectiveness of established controls. One key aspect of effective security planning and management is establishing appropriate policies and procedures governing a complete computer security program. Such policies and procedures should integrate all security aspects of an organization's interconnected environment, including network and mainframe security. The integration of network and mainframe security is particularly important as computer systems become more and more interconnected.

The Chief Information Officer (CIO) is the departmental official responsible for developing policy and procedures to ensure security is provided over the Department's computers, data and telecommunication networks. The CIO recently completed a preliminary analysis that identified the Department's risks and outlined plans to strengthen IT security in the Department. Exhibit A summarizes OCIO's progress on its plan to strengthen information security within USDA.

OBJECTIVES

The objectives of this audit were to (1) determine if the OCIO has developed, disseminated, and put into operation adequate security policies and procedures, including those established to address the prior Secretary's concerns, (2) assess the threat of penetration of departmental payment/data systems by intruders, (3) determine the adequacy of the security over the Local and Wide Area Networks, and (4) assess agency managements' involvement in IT security through review of the agencies' management structure, security plans, contingency plans, and other managerial controls in place.

SCOPE

This was a nationwide audit. We reviewed controls established to ensure the integrity of information security over the USDA network at various offices of seven USDA agencies.

Fieldwork was performed from May 2000 through December 2000. We conducted our testing at selected offices of OCIO, Food and Nutrition Service, Natural Resources Conservation Service, Forest Service, Farm Service Agency, and National Agricultural Statistical Service. Additionally, vulnerability scans were conducted on selected networks at the Agricultural Research Service. We judgmentally selected, for detailed testing, over 1,200 network components that were connected to the Department's network. The sample was selected based upon location and, in one case, at the request of the agency being tested.

We conducted this audit in accordance with Government Auditing Standards. .

METHODOLOGY

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

- We reviewed IT security policies and procedures from OCIO, and individual agencies.
- We interviewed responsible OCIO and agency officials managing the computer systems.
- We performed scans on various agency networks.
- We performed detailed testing of agencies' entity-wide security programs, both physical and logical access controls, segregation of duties, and service continuity by analyzing records and controls established to ensure that the security of the USDA's computer systems was sufficient.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	USDA HAS NOT ENSURED COMPLIANCE WITH FEDERALLY MANDATED SECURITY GUIDELINES AND IS LACKING IN ITS OVERALL MANAGEMENT OF INFORMATION TECHNOLOGY RESOURCES
------------------	---

FINDING NO. 1

The Department needs to improve its management of IT resources, and ensure compliance with existing Federal requirements for managing and securing IT resources. The

Department and most of the agencies we reviewed have not (1) conducted the necessary risks assessments of their networks, (2) adequately planned for network security and contingencies, or (3) properly certified to the security of their major systems. In addition, the Department had not adequately tracked the use of, or responsibility for, Internet Protocol (IP)⁶ addresses. Our audit disclosed that existing policy did not provide sufficient guidance for the agencies to carry out these functions. Department officials also attributed these weaknesses to a lack of personnel and adequate financial resources. The Department, while strengthening its IT security under the newly appointed Associate Chief Information Officer of Cyber Security, must move more rapidly to assure the agencies uniformly comply with these cited guidelines. 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 may be jeopardized if it cannot properly manage its IT infrastructure.

The OMB, Circular A-130, Appendix III, "Security of Federal Automated Information Resources," established 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.

⁶ An IP address uniquely identifies each host on a network.

In response, to our prior audit⁷ and a GAO⁸ report, 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 OCIO issued, "An Action Plan to Strengthen USDA Information Security," which emphasized protecting USDA's critical assets as a top priority for the department. The plan identified weaknesses that still exist today, including the lack of:

- OCIO resources necessary to provide technical assistance, enforce and monitor policy implementation, and ensure accountability;
- a comprehensive risk assessment that assigns value to the department's assets, prioritizes vulnerabilities, establishes a risk mitigation strategy; and
- a Department-wide information security architecture.

The OCIO advised us that a lack of adequate financial resources and personnel have hindered its ability to establish a Department-wide security program. Despite this lack of resources, the OCIO has begun to address these issues. (See Exhibits A and B.) However, significant progress is still needed to ensure that USDA's IT infrastructure and its data are secure, and that it can carry on its mission in the event of an emergency or other contingency.

Risk Assessments

We found that five of the seven agencies⁹ in our review failed to perform risk assessments of their networks, as required by OMB and PDD 63. Further, the OCIO has not conducted a risk assessment of the Department's backbone network. These networks carry critical privacy and financial data. Risk assessments, as defined by OMB, are a formal, systematic approach to assessing the vulnerability of information system assets; identifying threats; quantifying the potential losses from threat realization; and developing countermeasures to eliminate or reduce the threat or amount of potential loss.

In July 2000, we issued our audit report on the Department's compliance with PDD 63.¹⁰ 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 merely selected the 52 departmental 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.

⁷ Audit Report No. 23099-1-FM, "Security over Data Transmission in the Department Needs Improvement."

⁸ Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-99-227, July 1999).

⁹ Risk assessments were not reviewed at one agency.

¹⁰ Audit Report No. 50099-28-FM, "PCIE/ECIE Critical Infrastructure Protection Review," dated July 18, 2000.

During our audit, OCIO began to address compliance with PDD 63 by establishing a risk assessment workgroup. This workgroup, comprised of agency and departmental security specialists and business managers, was formed to help define interim standards, definitions, procedures, policies, and timeframes that will govern risk assessments within the Department. In addition, the Associate CIO for Cyber Security is in the process of establishing risk assessment checklists and policies for various IT platforms that can be used by agencies and the OCIO to conduct risk assessments on its mission critical systems. The OCIO advised us that many of these actions should be completed by the end of fiscal year (FY) 2001, including the completion of risk assessments on several mission critical systems. However, until these risk assessments are completed, the Department cannot be assured that all the risks attributable to its mission critical systems are identified and that appropriate steps are taken to mitigate these risks.

Security Plans

Five of the seven agencies in our review¹¹ had not prepared security plans that adequately addressed the requirements of OMB Circular A-130. OMB requires agencies to prepare a security plan to provide an overview of the security requirements of their systems.¹² 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. In addition, USDA Departmental Manual 3140¹³ requires each agency to submit an automated data processing security plan or an annual update to an existing plan to the OCIO.

The following examples illustrate the problems noted in our audit. The security plan at one agency, which gathers and disseminates agricultural information, consisted mainly of a statement that, "Management, Development/Implementation and operational controls are in place." The security plan failed to address the specifics of those controls, or establish responsibility for ensuring that those controls were functioning as intended. Our review of this agency noted substantial security vulnerabilities that may have been mitigated had a comprehensive security plan been in place. At another agency, the security plan did not (1) address personnel controls such as documenting security clearances or screening contract employees, (2) document incident response procedures, or (3) document continuity of support such as a brief description of backup procedures, location of backups, and storage requirements. The OCIO reviewed these agencies' FY 1999 security plans and identified many of these deficiencies; however, OCIO had not communicated these deficiencies to the agencies as a means of bringing about compliance.

¹¹ Security plans were not reviewed at one agency.

¹² The Computer Security Act of 1987 also requires that security plans be developed for all Federal computer systems that contain sensitive information.

¹³ DM 3140-1.1, Part 9, dated July 19, 1984.

Additionally, in a prior audit,¹⁴ we noted that the security plan for one of the Department's major applications had not been completed. That system processed nearly \$470 million in credit and fleet card transactions in one fiscal year, but the department had not documented system operations or ensured that management, operation, and technical controls were functioning effectively.

Further, the guidance that the OCIO issued to agencies for preparing security plans did not fully address all of OMB's requirements. Specifically, OCIO's guidance relating to the security of agencies' major applications did not require agencies to describe (1) the purpose of the system, (2) other systems to which it is interconnected, (3) laws or regulations that affect the system, and (4) the managerial controls in place to ensure the system is functioning properly. These elements are needed to ensure that management has evaluated all aspects of its major applications.

The Department needs to issue adequate guidance in preparing system security plans, establish procedures to ensure that agency security plans meet OMB guidelines, and ensure that security plans are communicated to the system users and administrators at all levels. Until such steps are taken, the Department cannot be assured that agencies have adequately addressed their security needs and that security policies and practices have become an integral part of the agencies' operations.

Contingency Plans and Backup/Recovery Plans

Six of the seven agencies¹⁵ we reviewed had not developed an adequate contingency plan or tested that plan to ensure that they could recover in the event of a disaster or other major disruption in service. Of the six deficient agencies, four did not have written backup and recovery procedures, three did not regularly backup their system files, and none adequately tested their contingency plans. As a result, 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.

The OMB requires that agencies plan for how they will continue to perform their mission or recover from the loss of application support in the event of a system failure. While contingency plans can be written to make a distinction between the recovery from system failure and recovery of business operations, our reliance on information technology and the push toward e-government makes the return to manual processing an unrealistic option to disaster recovery. For this reason, an agency should have procedures in place to protect information resources and minimize the risk of unplanned interruptions, and a plan to recover critical operations should interruptions occur. Although often referred to as disaster recovery plans, controls to ensure service continuity should address the entire range of potential disruptions from minor

¹⁴ Audit Report No. 50099-25-FM, "Security Over the Purchase Card Management System."

¹⁵ Contingency plans were not reviewed at one agency.

interruptions to major natural disasters. Further, OMB A-130 states that contingency plans be tested; as untested or outdated contingency plans create the false sense of the ability to recover in a timely manner.

Generally, the agencies in our review considered their Year 2000 (Y2K) contingency plans as their service continuity plans. However, Y2K plans were not comprehensive, as they did not address all potential service disruptions. For agencies that had prepared separate contingency plans, we found that the plans were outdated and had not been tested. At one agency we found that the contingency plans for several of the agency's mission critical systems had not been updated even though the operating environment had changed since the plans were developed in 1998. At another agency, many of its major applications systems that were listed in its Y2K contingency plan had been replaced or were no longer in use.

We also found that not all agency sites were equipped to perform a routine backup of system files. For example, one agency had not performed a system backup since June 2000, due to problems with its tape backup system. If faced with an emergency, this agency, which processes agricultural economic data, would lose months worth of data. Additionally, one site we visited that processed all of its agency's financial information had not performed a system backup, had no offsite storage, nor did it have a contingency plan in place.

Finally, the Department has only recently completed its contingency plan for the Washington, D.C. metropolitan area network that connects all Washington-based agency offices to the Department backbone. However, that plan is not comprehensive and has not been tested. For instance, the plan states that a 'hot site' can be established in the event of complete system failure; however, the plan does not contain any details on where the site will be located or who has responsibility for establishing and maintaining the site; what equipment will be needed; or, how personnel and other resources will be allocated to operate the facility when needed. Further, the plan states that backups will be performed and kept in a fire-proof safe; however, the plan does not reference any backup procedures or which systems to backup, where the backups will be stored, or how long backup tapes will be kept. Without this detail, the contingency plan cannot be adequately tested and therefore would be of little use in minimizing the disruption of system failure.

System Certification/Authorization

At four of the agencies in our review, system certifications and authorizations were either non-existent or not timely updated. OCIO officials advised us that they have not fully addressed the area of monitoring agencies' compliance with system certifications and authorization requirements. While the OCIO has begun to develop a database to track agency systems, certifications, and responsible management officials, little else has been done to ensure that system certifications and authorizations are completed and renewed in a timely manner. Without adequate certification and authorization of

the Department's critical systems, the Department cannot be assured that adequate security controls have been established for those systems and that those controls are operating effectively.

The 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. Re-authorization should occur subsequent to a significant change in the system or when there is high risk and potential of harm, but at least every 3 years.

One agency in our review had identified 26 systems that were critical to its mission. Agency officials informed us that they had done some testing of those systems but had not completed their testing, documented the testing they had done, or officially certified any of the 26 systems. Another agency identified 10 systems in its security plan that were determined to be critical, none of which were formally tested, certified, or authorized as required by OMB.

Network Address Tracking

The connection of USDA hosts¹⁶ to the Internet increases the exposure of USDA systems to unauthorized access and other potential exploitations from the Internet. To access the Internet, each host must have an IP address that uniquely identifies it on the network. The OCIO is the IP addressing and domain name registration authority for USDA.

Departmental Regulation 3300-1¹⁷ requires the OCIO to maintain a complete inventory of officially registered USDA IP network and subnetwork addresses in use by agencies and staff offices. In order to properly manage and secure a computer network, it is essential to maintain an accurate accounting of the systems that exist on that network.

The OCIO was not able to provide us with a current or complete list of IP addresses used by the agencies, or the name of a responsible agency official that controlled those addresses. For those addresses where OCIO could provide us an agency contact, we found several instances where the agency contact was inaccurate. Without an accurate listing of IP addresses and agency personnel responsible for administration of those addresses, the OCIO is hindered in its ability to properly secure the Department's network. An accurate accounting of IP addresses, systems, and the agencies responsible for their maintenance would provide OCIO with the information it needs to effectively manage the Department's network, and implement the appropriate level of security.

¹⁶ A host is any type of end-user computer system that connects to a network (e.g., personal computers, Local Area Network servers, UNIX platforms, and mainframes).

¹⁷ DR 3300-1, Appendix I, "Internet," dated March 23, 1999.

RECOMMENDATION NO. 1

Redirect OCIO resources to the security areas noted in this report until funding is obtained to implement a comprehensive security program within USDA.

OCIO Response

The OCIO agrees with the OIG recommendation. We will continue to give consideration, as appropriate, to the Cyber Security areas noted in this report.

OIG Position

We agree with the proposed actions. In order to reach management decision, please provide us the estimated timeframes for carrying out the cited actions.

RECOMMENDATION NO. 2

Monitor agency corrective actions on all security weaknesses identified by our audit to ensure weaknesses have been corrected.

OCIO Response

We concur with this recommendation. Many of the security weaknesses cited in the report were immediately addressed and 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.

OIG Position

We agree with the proposed actions. In order to reach management decision, please provide us the estimated timeframe for developing the process for monitoring corrective action on all security weaknesses identified.

RECOMMENDATION NO. 3

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 Response

We concur with this recommendation. Risk assessment is among the highest priorities in OCIO's Cyber Security strategy. In our early attempt to implement a risk assessment process, it became evident that many agency security technicians and system managers lack the tools and experience necessary to conduct adequate risk assessments.

To correct these deficiencies, the OCIO's Cyber Security Program Office has embarked on a series of contracts that will provide agency personnel with risk assessment tools and training. Our strategy involves developing platform-specific (Windows, UNIX, Telecommunications, etc.) risk assessment guides. Each contract includes a task for conducting a pilot assessment to validate the assessment guide and a training exercise to educate a broad set of users and managers in the art and process of conducting an information system risk assessment.

The first set of contracts, which includes telecommunications, will be awarded in the late March – early April 2001 timeframe. 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.

At the Department level, OCIO's Cyber Security Program Office has engaged a contractor to conduct a risk assessment of the USDA Telecommunications Backbone Network. Contractor technicians have been working on contract tasks since November 2000 and are approaching the end of their analysis. OCIO is expecting a final report from this assessment in early April 2001.

OIG Position

We agree with the proposed actions. In order to reach management decision, please provide us the estimated timeframe for developing the 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.

RECOMMENDATION NO. 4

Revise OCIO instructions on the preparation of Agency Security Plans to include all areas required by OMB A-130.

OCIO Response

We concur. OCIO's guidance to agencies for developing and submitting security plans has been revised.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 5

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.

OCIO Response

The OCIO agrees with this recommendation. A security plan policy that establishes agency timeframes for completing and updating security plans, requires plan submission to OCIO and formalizes OCIO's review and oversight responsibility will be issued by the end of FY 2001.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 6

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.

OCIO Response

We concur with this recommendation. OCIO recognizes that contingency plans, disaster recovery procedures, and business resumption plans are integral aspects of a comprehensive cyber security program. Our Cyber Security Program Implementation Plan acknowledges the need for these devices and outlines their implementation under an Information Survivability Program. However, resource limitations prohibit extensive work in this area.

In the meantime, a current Cyber Security Program Office staff member has been receiving extensive training in the art of contingency planning and disaster recovery. A limited attempt to counsel agencies on contingency and recovery procedures will begin this fiscal year, but extensive work in this area requires additional funding.

OIG Position

While we recognize the limited resources of the OCIO, until additional funding can be obtained for extensive work in this area, we believe an attempt should be made by 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. In order to reach management decision, please provide us with how OCIO intends to require the agencies to submit their comprehensive and system-specific contingency plans, and the timeframes for implementing those requirements.

RECOMMENDATION NO. 7

Require agencies to perform annual testing of their contingency plans, adjust their plans based on the results, and report their test results to OCIO.

OCIO Response

We concur with this recommendation. OCIO acknowledges that annual contingency plan testing is required to ensure plans are adequate and that test results should be shared with OCIO. However, due to resource limitations, our Information Survivability Program, which includes contingency planning has not yet been initiated.

OIG Position

In order to reach management decision, the OCIO needs to advise us how it intends to require that agencies test their contingency plans annually, adjust their plans accordingly, and provide the test results to the OCIO. Further, OCIO needs to provide us with timeframes for implementing the proposed requirement.

RECOMMENDATION NO. 8

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.

OCIO Response

We concur with this recommendation. OCIO recognizes that certification (and accreditation) of systems, particularly those that process, handle, or store sensitive and classified data, to verify confirmation to prescribed high-level security standards and practices commensurate with the sensitivity of the assets, as determined by the business owners, is required. The Department's goal is to achieve a C2¹⁸ level of certification for all sensitive but unclassified systems. Facilities that house critical infrastructures will be required to meet a Department of Justice level 4 physical security standard.

The OCIO Cyber Security Implementation Plan schedules the initiation of a Sensitive Certification Program in FY 2002, provided additional funding is obtained.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 9

Establish controls to ensure that an accurate and timely updated database is maintained of IP addresses and responsible agency contacts.

OCIO Response

We concur with this recommendation. OCIO is in the process of collecting this data.

OIG Position

In order to reach management decision, the OCIO needs to provide us with a timeframe for establishing controls that will ensure the database of IP addresses and agency contacts will be maintained and updated timely.

¹⁸ C2 certification is a set of criteria used by the U.S. Government National Security Agency for evaluating the security features of a computer system.

FINDING NO. 2

Our vulnerability scans disclosed severe and systemic weaknesses in system security administration. Specifically, we found that scans of selected departmental systems

disclosed a large number of risk indicators that could be exploited from both inside the department's networks and from the Internet, and that system policy settings unnecessarily increased the risk and were not uniform throughout the Department. Agencies have not taken self-initiated action to eliminate security vulnerabilities with their systems' operating software, nor has OCIO provided guidance to agencies on proper and consistent system policy settings. As a result, the Department's systems and networks are vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of the Department's critical financial and economic data.

We conducted an assessment of selected USDA agencies' networks between June and December 2000. We used two commercially available software products - one designed to identify over 800 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP),¹⁹ and the other, which tests system policy settings in Novell networks.

TCP/IP System Vulnerabilities

We conducted our vulnerability scans at 29 specific locations within 7 USDA agencies. These scans included over 1,200 systems within the Department. Our assessments revealed nearly 3,300 high and medium-risk vulnerabilities. We reported the weaknesses found at agency locations directly to agency management. Agency officials agreed with our results and took immediate action to correct the problems. In addition, we identified over 6,300 low-risk vulnerabilities, many of which, while not critical to system security, can be an indication of poor systems administration. Three agencies in our review had already acquired similar scanning tools but were not using them to aggressively eliminate vulnerabilities on their systems.

Detailed below are examples of the high-risk²⁰ vulnerabilities disclosed during our scans of the various agency systems:

¹⁹ Transmission Control Protocol/Internet Protocol (TCP/IP) is a series of protocols originally developed for use by the US Military and now used on the Internet as the primary standard for the movement of data on multiple, diverse platforms.

²⁰ 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.

- An export directory was found to be configured to allow anyone to write to the directory. As a result, an attacker could modify any files on this system. For instance, essential data could be erased or modified.
- An error in the system's log could allow an attacker to run programs, including malicious code, 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 the system.
- A Windows NT machine was configured to allow anyone to sign on as the Administrator by using a blank password. The Administrator is the most trusted user on a Windows NT system; therefore, the Administrator has complete control over the computer and can perform any function.
- Administrator accounts on three other Windows NT systems were set to allow access by using a password that was the same as the Administrator's Login 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.

Our testing also identified instances that demonstrate the need to continually assess the vulnerabilities on agency networks and mitigate the possibility of attack. At one agency, we found that the File Transfer Protocol,²¹ which the agency used within its network to transfer files between its field offices, was accessible by users of the Internet. Agency officials believed that they had sufficiently blocked the use of this protocol from Internet users by filtering such access at their routers and firewall; however, our tests confirmed to agency officials that the routers and firewall were not adequately protecting their files from Internet access. Agency officials immediately corrected the vulnerability.

At another agency, we conducted vulnerability scans from both inside the agency's network and from outside its firewall. We conducted this test to ensure the agency's firewall was adequately blocking Internet users from successfully accessing the network. Our tests disclosed that the firewall was not properly configured to protect the agency's network, thereby exposing its network to the risk of attack from Internet users. Agency officials took prompt action to correct this vulnerability.

²¹ File Transfer Protocol, a commonly used protocol used to transfer files from one system to another.

During our audit testing at one agency, we noted that the agency had developed a configuration program for its systems. This process ensures that all systems are configured alike by attempting to update all systems with recently released security patches and other software updates. However, this agency was the only departmental agency included in our testing that employed this type of system configuration policy. We believe this corporate level approach to system configuration, along with regularly scheduled vulnerability assessments and mitigation of the risks discovered, would not greatly enhance the security of agency computer systems.²²

We also noted that the OCIO, which operates the USDA telecommunications backbone, has recently implemented a policy for firewall implementation. However, this policy does not require agencies to place a firewall between their networks and the OCIO backbone. Consequently, agencies are not only at risk from vulnerabilities on their own systems, but also from vulnerabilities residing on other agencies' systems in the Department. We found that one agency's internal network, which is used by its employees, was not adequately separated from its public access network (i.e., web servers). There is no protection in place that would prevent public users of that agency's web servers from accessing the internal network and obtaining sensitive information not intended for public access. Without firewall protection between agencies and the backbone, weaknesses in one agency's network could put all other agencies on the Department's backbone at risk.

Novell System Policies

We also conducted a detailed assessment of the security of the Novell networks at 10 sites in 5 agencies. Our assessment software allowed us to compare the agencies' security practices to the actual settings on the Novell systems. We were also able to compare each system's security settings to the software product's "best practices," which are based on standard practices from a wide variety of government and private institutions. The software product reports weaknesses that may leave the system open to potential threats in the following areas (1) account restrictions, (2) password strength, (3) access control, (4) system monitoring, (5) data integrity, and (6) data confidentiality.

Our assessments disclosed that the majority of weaknesses were in the account restrictions, password strength, and access control areas, the areas that define a user's ability to access the system. Further, we found that these security settings were not consistently applied within an agency, varying from one site to another.

²² The corporate level approach to system security configuration provides a uniform basis for system security updates, however, it is critical that an aggressive approach is taken to identify new vulnerabilities, and that updates to the system to correct those new vulnerabilities be performed in a timely manner.

Examples of where some agencies did not meet best practices:

- Seven of the 10 sites had minimal account lockout time set. This setting defines how long a user's account is locked after attempting to log into the system with a bad password. If this setting is too short it can adversely affect the security of the system by allowing an attacker to try numerous passwords on that account in an attempt to gain access.
- Eight of the 10 sites allowed the number of grace logins, which varied from site to site, to exceed best practices. This setting defines how many times a user can attempt to log-in after their password has expired before the system locks that users' account. This setting helps strengthen system security by limiting the number of times a user can login using an expired password before the system requires the user to change their password.
- Eight of the 10 sites had not defined user access times. This setting allows system administrators to limit a user's ability to access they system only during a user's work hours, reducing the risk that the user's account would be used for a system attack during non-work hours.

In addition to the above policy settings, we found instances that were unique to specific sites that indicated a lack of adequate system administration. For instance, at one site we found that the agency had failed to remove old user accounts after it no longer shared its Novell network with another agency. Some of these user accounts were administrator equivalents that would have allowed those users unrestricted access to the system. At another agency, we discovered that one of its mission critical systems required a minimum length password of only one character, did not require users to periodically change their passwords, or encrypt passwords sent over the network. All of these policies make it easier for an unauthorized user to potentially gain access to the systems.

These weaknesses existed because of a lack of adequate system administration within the agencies, and the lack of a Department-wide policy of configuration management defining minimum requirements for system security settings.

RECOMMENDATION NO. 10

Establish Departmental policy requiring agencies to scan their systems on a routine basis and take prompt action to eliminate noted vulnerabilities.

OCIO Response

We concur with this recommendation. Many agency security technicians lack the expertise and tools to perform adequate analysis of the networks they manage. To address these deficiencies, the Cyber Security Program Office is currently negotiating 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.

OIG Position

We agree with the proposed actions. In order to reach management decision, OCIO needs to provide us with proposed procedures for ensuring that all agencies routinely scan their systems. Include timeframes for establishing and implementing this requirement.

RECOMMENDATION NO. 11

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 Response

We concur with this recommendation. Please see our response to Recommendation No. 2.

OIG Position

In order to reach management decision, please provide us the estimated timeframe for developing the process for monitoring corrective action on all vulnerabilities identified.

RECOMMENDATION NO. 12

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.

OCIO Response

We concur with this recommendation. OCIO recognizes the need for sound Configuration Management (CM). A security expert who specializes in CM has been hired to the Cyber Security Program Office staff, has developed and delivered CM training to agency technicians, and is developing interim CM guidance. For the long term, OCIO plans to implement Department-wide configuration management within its Sensitive System Certification and Accreditation Program, scheduled to begin in FY 2002.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 13

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 Response

Before implementing this recommendation, OCIO's Cyber Security Program Office will review the impact and benefits of the strategy.

OIG Position

In order to reach management decision, please provide us your time-phased corrective action plan to fulfill this recommendation.

FINDING NO. 3

Six of the seven agencies²³ in our review had not ensured that only authorized users had access to their networks. Agencies have been lax in ensuring that their 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 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. As a result, the Department's critical data are at risk of unauthorized disclosure, modification, or deletion.

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

Limiting physical access to network systems and equipment should be the first step in securing any network. Physical access controls guard against theft, disablement, or other modification of network hardware that could lead to the loss of the critical data that resides on that hardware. The OCIO has not provided agencies with the necessary guidance on physically securing their network hardware, or ensuring that physical access controls are in place to limit access to only authorized individuals.

During our review of two co-located agencies, we noted that they, and other agencies located at that facility, shared the same computer room. Employees from all agencies had access to the other agencies' systems, many of which contain critical and sensitive agency data. Further, at several agencies, critical network devices were housed in the same rooms with the facilities' shared telephone network hardware. Telephone

²³ Access controls were not reviewed at one agency.

contractor personnel were allowed full access to this room and the network equipment closets, thereby giving them unrestricted physical access to the mission-critical router and network switches. At three locations in two agencies, we witnessed contractor personnel leaving those network equipment closets open and unattended, giving anyone unauthorized access to critical network switching hardware.

At several state and county offices servers were not secure. At one state office, the server was in an open area; while in another state office the server was in a separate room that could not be locked. At a third state office, a contractor, who had been left unsupervised after normal office hours, used a computer in the office to access unauthorized Internet websites.²⁴

Testing at another agency showed that the computer room was vulnerable to unauthorized access because the office's key card system had not been activated. Further, entrance to the computer room could be gained through two doors that opened to a hallway that was highly used by non-agency personnel. These doors were prominently marked as the computer room doors for this agency. At another location of this agency, we noted that the combination lock controlling one of the computer room entrances was not changed after a contractor had separated from employment. The agency changed the combination during our audit.

Finally, at two sites we found that numerous maintenance personnel, 30 in one location and 17 in the other, had access to rooms that housed critical network equipment and server systems. These rooms were secured using electronic key cards. While this system was able to record which cards had been used to access those rooms, the agency had not periodically reviewed access levels to ensure that only authorized users were allowed into these rooms. Further, the agency could not be assured that only authorized personnel possessed the access cards. At one location, the agency had difficulty finding someone that was able to provide a current list of users with access to the computer room. Many of these personnel were not Department employees and the agency could not provide us assurance that these maintenance people were still employed or still required access.

Logical Access Controls

While physical access controls protect network hardware, logical access controls protect network applications and data against theft or unauthorized modification. Network administrators should provide only authorized users access to network applications and data, and ensure that such access is limited to what is needed to perform the user's job functions. Without strong logical access controls, privacy and financial data is subject to loss and unauthorized modification.

²⁴ Websites contained gambling and pornographic materials.

Throughout our review, we found that weaknesses in logical access controls were prevalent in agencies' systems. Nearly all agencies' systems contained inactive or expired user accounts, accounts that belonged to users no longer employed, and 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 agencies used several 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. With this type of procedure, an agency could identify and eliminate unnecessary user accounts from its system. An agency's inability to enforce its logical access controls exposes that agency's system settings and data to unauthorized modification or deletion.

Shared user accounts make it impossible for system administrators to track the actions of users in the event that an inappropriate or malicious action was taken. At one agency, generic user accounts were allowed to exist on a mission critical database. Several people knew the password for these accounts and could modify database records without being detected. Further, this agency routinely established temporary accounts that were set up with excessive access rights and were not changed according to the users' needs. Those rights included the ability to create, modify, and even erase files. At another agency, system administrators were using shared accounts to make changes to the systems' operating software, rather than requiring each administrator to have their own account with administrative privileges.

User accounts that become inactive, but not disabled, provide additional opportunities for unauthorized users to gain access to the network. Once that access is gained, unauthorized activity cannot be traced to the responsible person. At one agency, we found that over 14 percent of current personnel and 45 percent of the guest accounts had not accessed the systems in at least a year. At another agency, we identified 143 out of 630, or 23 percent, of its accounts that were inactive and left on its system.

Agencies need to ensure that the user accounts of separated employees and contractors are removed immediately to ensure those users do not gain access to agency data after they leave. At two agencies, we identified active network accounts, 53 at one agency and 20 at another, that belonged to separated employees and contractors. At another agency, we found that a system administrator with complete network administrative control retired from the agency. The agency subsequently contracted with that employee to work from his home on a test database, but did not remove his administrative access rights, which included complete modification ability over data that impacts agricultural commodity markets.

RECOMMENDATION NO. 14

Monitor agencies corrective actions on the cited access controls until the weaknesses identified have been corrected.

OCIO Response

We concur with this recommendation. Please see our response to Recommendation No. 2.

OIG Position

In order to reach management decision, please provide us the estimated timeframe for developing the process for monitoring corrective action on the cited access controls.

RECOMMENDATION NO. 15

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 Response

OCIO concurs with this recommendation. Policy will be issued to require access rules that prevent unauthorized access, including terminated employees.

OIG Position

We agree with the proposed action. In order to reach management decision, please provide us the estimated timeframe for issuing the policy.

RECOMMENDATION NO. 16

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 Response

The OCIO concurs with this recommendation. OCIO recognizes the importance of physical security. Our risk assessment guidance will provide for analysis of physical security within the checklists and assessment tools being developed. Furthermore, the Cyber Security Program Office has hired a physical security expert who is currently developing this guidance.

OIG Position

We agree with the proposed action. In order to reach management decision, please provide us the estimated timeframe for issuing the guidance on physical security.

EXHIBIT A – Status of Recommendations in the Action Plan to Strengthen USDA Information Security

Action Plan Recommendations	OCIO Actions to Date	Status
Security Program Management		
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.	Completed February 2000
Establish structures to provide the central group and agency IT staffs ready and independent access to senior executives	OCIO is drafting a letter to the Under Secretary of Agriculture to set up an Advisory Council. The council would be comprised of the agency CIO's and one business manger from each agency.	Council should be established by the 4 th quarter FY 01
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.	Completed February 2000
Personnel		
Assess Cyber-Security staffing needs	The Associate CIO for Cyber-Security is currently seeking to add staff. The first two positions have already opened, and additional announcements are pending.	Personnel are expected to be on board by the end of the 2 nd quarter FY 01.
Implement systematic training to enhance IT staff professionalism and technical skills	A cyber-core team is being developed. This core of security specialists will be specially trained to address security issues as they arise. A contractor provided training in the 1st quarter 2001 for 15 individuals, and an additional training session is scheduled for 2nd quarter 2001 and will be continuous thereafter.	Completed November 2000 and will be on-going.
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.	Contractor requirements will be completed by end of FY 01. All assessments are expected to be completed by mid FY 03.
Establish a close link between human resources processes and information security	OCIO has been working closely with Human Resources on developing new position descriptions for the Cyber-Security Office. In addition, they are monitoring the new pilot to attract security expertise and retain IT staff.	On-going

EXHIBIT A – Status of Recommendations in the Action Plan to Strengthen USDA Information Security (Continued)

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.	Training on risk assessment will be completed by 2 nd quarter FY 01.
Implement appropriate policies and related controls that are linked to the Department's business risks.	Three new policies have been issued in final, with one additional policy still in draft.	Completed December 2000 and on going.
Immediately clarify management's support for security policies and guidelines.	The risk assessment training includes business managers. Management involvement will educate managers on security concerns and facilitate cooperation between them and the IT staff. Also, the Advisory Council to be established will include the CIO and one representative from agency.	Training on risk assessment will be completed by 2 nd quarter FY 01. The Advisory Council will be established by the 4 th quarter FY 01.
Establish procedures to monitor and evaluate policy and control effectiveness; use the results to direct future activities.	One of the positions due to be announced will be for a policy person. This individual will be responsible for monitoring and evaluating policies and their subsequent effectiveness.	Personnel will be on board by the end of the 2 nd quarter FY 01.
Be alert to and implement new monitoring tools and techniques.	New firewalls were installed across the backbone in the Fall of 2000. Logs from the firewalls are monitored daily by OCIO staff. These are used to identify possible intrusion or scanning activity.	Completed December 2000
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 contract is finalizing its analysis of the backbone network security needs. Funding has been set-aside in the FY 01 and FY 02 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.	2 nd Quarter FY 01 for contractor analysis 4 th Quarter FY 02 for procurement
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 is currently being sought.	Completed, but will be an on-going project.
Centrally coordinate current USDA cyber security initiatives.	Security initiatives have been developed and centralize in the office of the Associate CIO for Cyber-Security.	Completed February 2000

EXHIBIT B – Status of Recommendations in 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	Lack of adequate funding has set back OCIO’s plans for PDD-63 compliance. Funding has now been obtained and OCIO has begun the process of compiling with PDD-63.	OCIO’s 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 fiscal year 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.	Funding has already been acquired. The risk assessment checklists should be procured and set into action by the third quarter 2001.
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.	Training provided to technician and functional managers will be completed by fourth quarter 2001.

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 has contracted to conduct a risk assessment and analysis of the Department backbone security needs. OCIO should have the results of this assessment by March 2001.	OCIO intends to begin procuring encryption equipment to encrypt backbone traffic by the end of fiscal year 2001 and will continue to procure such equipment in fiscal year 2002.
Implement appropriate safeguards to secure the link between National Technology Information Center (NTIC) and the National Finance Center (NFC).	OCIO has contracted a study of backbone security and has implemented VPN encryption.	Once backbone encryption equipment is implemented, all backbone traffic, including traffic between NITC and NFC will be encrypted. Estimated completion of fiscal year 2002.

EXHIBIT B – Status of Recommendations in From Prior Audits (Continued)

Recommendation	Actions to Date	Estimated Completion Date
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 intends to begin procuring encryption equipment to encrypt backbone traffic by the end of fiscal year 2001 and will continue to procure such equipment in fiscal year 2002.
Take immediate action to eliminate the vulnerabilities identified by the Office of Inspector General's (OIG) vulnerability scans.	OCIO took immediate action to eliminate the vulnerabilities identified by OIG's vulnerability assessment.	Completed third 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 purchased the same vulnerability assessment tool used by OIG. OCIO intends to use this tool on a regular basis once it has hired sufficient personnel to conduct the assessments.	OCIO has begun to hire additional personnel resources. The assessment of network servers, routers, and other hardware is ongoing.
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.	Completed third quarter 2000.

EXHIBIT C – Auditee Response To Draft Report



United States
Department of
Agriculture

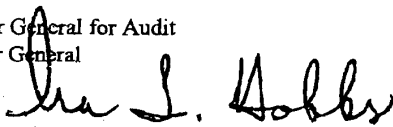
Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

March 29, 2001

TO: James R. Ebbitt
Assistant Inspector General for Audit
Office of Inspector General

FROM: Ira L. Hobbs 
Acting Chief Information Officer

SUBJECT: Response to Audit Report "Security over USDA Information Technology
Resources Needs Improvement" No. 50099-27-FM

Following are our responses to your memorandum of March 5, 2001, regarding the subject report:

Office of the Chief Information Officer (OCIO) takes its responsibility for overall security of USDA's information assets seriously. As you are aware, the Secretary has directed our office to develop and implement a plan to improve information security throughout the Department. Our Action Plan to Strengthen USDA Information Security, issued in August 1999, addresses Federal computer security requirements, as well as the broader security issues that must be considered in order to implement a comprehensive and effective information computer security program.

We are aggressively implementing our security action plan. Already we have established our Cyber Security Program office, have hired an Associate CIO to manage it, have assigned staff to the office, are prioritizing and planning specific security-related activities, and are analyzing the Department's existing security controls. Where appropriate, we are changing security policies and procedures and implementing mitigation actions when vulnerabilities are discovered.

As you note in your report, OCIO is committed to protecting the Department's IT infrastructure.

In regards to the recommendations contained within your memorandum, we offer the following comments:

OIG Recommendation No. 1: Redirect OCIO resources to the security areas noted in this report...

EXHIBIT C – Auditee Response To Draft Report

OCIO Response: The OCIO agrees with the OIG recommendation. We will continue to give consideration, as appropriate, to the Cyber Security areas noted in this report.

OIG Recommendation No. 2: Monitor agency corrective actions on all security weaknesses identified by our audit...

OCIO Response: We concur with this recommendation. Many of the security weaknesses cited in the report were immediately addressed and 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.

OIG Recommendation No. 3: Establish a risk assessment policy that requires agencies to keep network documentation updated...

OCIO Response: We concur with this recommendation. Risk assessment is among the highest of priorities in OCIO's Cyber Security strategy. In our early attempt to implement a risk assessment process, it became evident that many agency security technicians and system managers lack the tools and experience necessary to conduct adequate risk assessments.

To correct these deficiencies, the OCIO's Cyber Security Program Office has embarked on a series of contracts that will provide agency personnel with risk assessment tools and training. Our strategy involves developing platform-specific (Windows, UNIX, Telecommunications, etc.) risk assessment guides. Each contract includes a task for conducting a pilot assessment to validate the assessment guide and a training exercise to educate a broad set of users and managers in the art and process of conducting an information system risk assessment.

The first set of contracts, which includes telecommunications, will be awarded in the late March – early April, 2001 time frame. 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.

At the Department level, OCIO's Cyber Security Program Office has engaged a contractor to conduct a risk assessment of the USDA Telecommunications Backbone Network. Contractor technicians have been working on contract tasks since November 2000 and are approaching the end of their analysis. OCIO is expecting a final report from this assessment in early April 2001.

EXHIBIT C – Auditee Response To Draft Report

OIG Recommendation No. 4: Revise OCIO instructions on the preparation of Agency Security Plans...

OCIO Response: We concur. OCIO's guidance to agencies for developing and submitting security plans has been revised.

OIG Recommendation No. 5: Establish a security plan policy...

OCIO Response: OCIO agrees with this recommendation. A security plan policy that establishes agency timeframes for completing and updating security plans, requires plan submission to OCIO and formalizes OCIO's review and oversight responsibility will be issued by the end of FY2001.

OIG Recommendation No. 6: Require agencies to prepare and submit OCIO comprehensive and system-specific contingency plans that address protection of information resources and recovery procedures...

OCIO Response: We concur with this recommendation. OCIO recognizes that contingency plans, disaster recovery procedures, and business resumption plans are integral aspects of a comprehensive cyber security program. Our Cyber Security Program Implementation Plan acknowledges the need for these devices and outlines their implementation under an Information Survivability Program. However, resource limitations prohibit extensive work in this area.

In the meantime, a current Cyber Security Program Office staff member has been receiving extensive training in the art of contingency planning and disaster recovery. A limited attempt to counsel agencies on contingency and recovery procedures will begin this fiscal year, but extensive work in this area requires additional funding.

OIG Recommendation No. 7: Require agencies to perform annual testing of their contingency plans...

OCIO Response: We concur with this recommendation. OCIO acknowledges that annual contingency plan testing is required to ensure plans are adequate and that test results should be shared with OCIO. However, due to resource limitations, our Information Survivability Program, which includes contingency planning, has not yet been initiated.

OIG Recommendation No. 8: Ensure agency compliance with OMB A-130 requirements for system certification/authorization...

OCIO Response: We concur with this recommendation. OCIO recognizes that certification (and accreditation) of systems, particularly those that process, handle, or store sensitive and classified data, to verify confirmation to prescribed high-level

Page 3 of 5

EXHIBIT C – Auditee Response To Draft Report

security standards and practices commensurate with the sensitivity of the assets, as determined by the business owners, is required. The Department's goal is to achieve a C2 level of certification for all sensitive but unclassified systems. Facilities that house critical infrastructures will be required to meet a Department of Justice level 4 physical security standard.

The OCIO Cyber Security Implementation Plan schedules the initiation of a Sensitive System Certification Program in FY2002, provided additional funding is obtained.

OIG Recommendation No. 9: Establish controls to ensure that an accurate and timely updated database is maintained of IP addresses and responsible agency contacts...

OCIO Response: We concur with this recommendation. OCIO is in the process of collecting this data.

OIG Recommendation No. 10: Establish Departmental policy requiring agencies to scan systems on a routine basis...

OCIO Response: We concur with this recommendation. Many agency security technicians lack the expertise and tools to perform adequate analysis of the networks they manage. To address these deficiencies, the Cyber Security Program Office is currently negotiating 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.

OIG Recommendation No. 11: Ensure that the agencies in our review have taken the necessary corrective action on all high and medium risk vulnerabilities identified during our audits...

OCIO Response: We concur with this recommendation. Please see our response to Recommendation No. 2.

OIG Recommendation No. 12: Require agencies to adopt a corporate level approach to configuration management...

OCIO Response: We concur with this recommendation. OCIO recognizes the need for sound Configuration Management (CM). A security expert who specializes in CM has been hired to the Cyber Security Program Office staff, has developed and delivered CM training to agency technicians, and is developing interim CM guidance. For the longer term, OCIO plans to implement Department-wide configuration management within its Sensitive System Certification and Accreditation Program, scheduled to begin in FY2002.

EXHIBIT C – Auditee Response To Draft Report

OIG Recommendation No. 13: Update the firewall policy to require that agencies implement firewalls between their networks and the Department's backbone...

OCIO Response: Before implementing this recommendation, OCIO's Cyber Security Program Office will review the impact and benefits of the strategy.

OIG Recommendation No. 14: Monitor agencies corrective action on the cited access controls until the weaknesses have been corrected...

OCIO Response: We concur with this recommendation. Please see our response to Recommendation No. 2.

OIG Recommendation No. 15: Establish a policy requiring agencies to routinely review system accesses to ensure that terminated employees no longer have access to agency systems...

OCIO Response: OCIO concurs with this recommendation. Policy will be issued to require access rules that prevent unauthorized access, including terminated employees.

OIG Recommendation No. 16: Provide guidance to agencies on how to physically secure all network critical hardware...

OCIO Response: OCIO concurs with this recommendation. OCIO recognizes the importance of physical security. Our risk assessment guidance will provide for analysis of physical security within the checklists and assessment tools being developed. Furthermore the Cyber Security Program Office has hired a physical security expert who is currently developing this guidance.

We shall continue to keep you posted of our progress on these recommendations.

cc: Bill Hadesty, CS/OCIO.
[] OIG
Sherry Linkins, OCIO
Greg Montgomery, CS/OCIO

ABBREVIATIONS

CIO	Chief Information Officer
CM	Configuration Management
FY	Fiscal Year
GAO	U.S. General Accounting Office
ID	Identification
IP	Internet Protocol
IT	Information Technology
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OCIO	Office of the Chief Information Officer
OIG	Office of the 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
Y2K	Year 2000