U.S. Department of Agriculture

Office of Inspector General
Southwest Region

Audit Report

Management and Security of Economic Research Service Information Technology Resources

Report No. 14099-1-Te
March 2004

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington, DC 20250

DATE: March 31, 2004

REPLY TO
ATTN OF: 14099-1-Te

SUBJECT: Management and Security of Economic Research Service Information Technology Resources

TO: Susan Offutt
Administrator
Economic Research Service

ATTN: Paul Chan
Director
Information Services Division

This report presents the results of the subject audit. Your response to the official draft report, dated March 30, 2004, is included in its entirety as exhibit A with excerpts and the Office of Inspector General's position incorporated into the Findings and Recommendations section of the report. Your response contained sufficient justification to reach management decisions on all recommendations contained in the report.

Please follow Departmental and your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer, Director, Planning and Accountability Division. Final action on the management decisions should be completed within 1 year of the date of the management decisions to preclude being listed in the Department's annual Performance and Accountability Report.

We appreciate the courtesies and cooperation extended to us by members of your staff during the audit. If you have any questions, please contact me at 720-6945, or have a member of your staff contact Richard J. Davis, Director, Administration and Finance Division, at 720-1918.

/s/ R. W. Young
ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Management and Security of Economic Research Service Information Technology Resources (Audit Report No. 14099-1-Te)

Results In Brief

Effective management and security of information technology (IT) resources have become increasingly important to the U.S. Department of Agriculture's mission, especially as the Department makes more programs and information available over the Internet. In our continuing effort to examine Information System Security Programs (ISSP) throughout the Department, we audited the management and security of Economic Research Service's (ERS) IT resources.

Specifically, our objectives were to (1) assess the overall management of ERS' ISSP, (2) determine the adequacy of security over agency networks, and (3) determine if adequate logical and physical access controls existed to protect computer resources, including application and system software, against unauthorized modification, disclosure, loss, or impairment.

As the chief source of the Department's economic research and information, ERS manages a large volume of data, some of it sensitive. For example, its computer systems contain social security numbers and farm income and expenditure records belonging to individuals. Protecting such confidential information from cyber intruders must be a top priority for management and staff.

We found that ERS needs to strengthen its ISSP by establishing controls and formal policies for oversight of security planning, periodic review of security controls, administration of IT security tools, and logical and physical access.

Foremost, insufficient security planning and oversight created an unstable foundation for the agency's ISSP. Although the Office of the Chief Information Officer had waived the requirement to submit agency security plans in 2002, agencies still were required to ensure that all weaknesses identified in the 2001 security plan reviews were corrected. However, we found that ERS had not updated its 2001 security plan to incorporate all requirements. Furthermore, the agency had not implemented all of its security plans to comply with Federal regulations. For example, ERS had not implemented a formal computer security training program, obtained security clearances for employees in sensitive positions, established a formal incident response policy, or completed and tested a contingency plan.

If it had routinely reviewed its ISSP, ERS could have discovered and remedied many of the flaws we identified in its security plan and access control procedures. However, ERS had not complied with Federal information resource policies, which require agencies to conduct annual security reviews and perform risk analyses at least every 3 years. ERS had

no formal program for periodically evaluating its security policies and conducting risk assessments to determine the extent of potential risks and threats to its IT resources.

Inadequate administration of IT security tools also left ERS systems open to malicious attacks, a material control weakness that requires additional management oversight. Our vulnerability scan of the agency's computer systems disclosed a large number of risk indicators that could be exploited by cyber attackers. While ERS took immediate action to remedy some of the weaknesses we identified in our audit, it had not responded aggressively to other security vulnerabilities discovered 10 months earlier by its own vulnerability scan.

Finally, ERS' logical and physical access controls did not provide optimum protection against unauthorized modification, disclosure, loss, or impairment of IT resources. We found that computer access lists had not been updated to reflect current users, controls over shared or generic accounts had not been established, users could transmit sensitive data through unsecured remote access methods, settings for password uniqueness and logon attempts did not meet Departmental guidelines, and cleaning staff and other unauthorized individuals had physical access to sensitive areas and equipment.

Recommendations In Brief

We recommend that ERS plan and/or implement a formal training program, background screening of all individuals in sensitive positions, a formal incident response policy, and a contingency plan that is approved by senior management and tested annually. We further recommend that the agency establish formal procedures for periodic review of security controls and risk assessments.

Additionally, we recommend that ERS take immediate corrective action to mitigate all high- and medium-risk vulnerabilities, and that it establish policies to strengthen network security. We recommend that these policies address (1) proper scanning procedures to detect all network vulnerabilities, (2) proper configuration of computer access security settings, (3) a configuration management program, (4) modem security, (5) routine and timely review of firewall configuration, and (6) logical and physical access controls, including controls over computer access lists, accounts, and sensitive areas and equipment.

Agency Response

In a letter dated March 30, 2004, ERS concurred with all of the findings and recommendations and provided proposed actions and completion dates for each recommendation. (See exhibit A.)

OIG Position

We accept the management decisions for all of the recommendations contained in the report. For final action, ERS needs to provide the Director, Planning and Accountability Division, Office of the Chief Financial Officer (OCFO/PAD), documentation as outlined in the Office of Inspector General (OIG) Position sections of the report.

Abbreviations Used In This Report

ADP	Automated Data Processing
DM	Departmental Manual
DR	Departmental Regulations
ERS	Economic Research Service
ISD	Information Services Division
ISSP	Information Systems Security Program
ISSPM	Information Systems Security Program Manager
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCFO/PAD	Office of the Chief Financial Officer, Director, Planning and Accountability Division
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication
USDA	U.S. Department of Agriculture
WAN	Wide Area Network

Table of Contents

Background and Objectives

Background

Information security, improving the overall management of information technology (IT) resources, and the transition to electronic business (e-Government) have emerged as top priorities within the U.S. Department of Agriculture (USDA). As technology enhances our ability to share information instantaneously among computers and networks, it also has made organizations more vulnerable to unlawful and destructive penetration and disruptions. These vulnerabilities pose a threat to the sensitive and critical operations of the Economic Research Service (ERS).

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,[1] and the Paperwork Reduction Act of 1995. Responsibilities regarding information security were reemphasized in the Clinger-Cohen Act of 1997 and Presidential Decision Directive 63, Policy on Critical Infrastructure Protection. Additionally, the Government Information Security Reform Act[1] enacted on October 30, 2000, essentially codifies the existing requirements of the Office of Management and Budget (OMB) Circular A-130.[2]

OMB Circular A-130[2] establishes policy for the management of Federal IT resources. The policy requires security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of information. The policy also requires assignment of security responsibility, security plans, risk assessments, and system certifications to lessen the risk and magnitude of damage to information.

Considerable guidance on information security also has been developed. The National Institute of Standards and Technology (NIST) has issued numerous Federal Information Processing Standards, as well as a comprehensive description of basic concepts and techniques in Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, dated October 1995, and SP 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems, dated September 1996.

Finally, Departmental Manual (DM) 3140-1.1, Management ADP Security Manual, dated July 19, 1984, also provides standards, guidelines, and procedures for the development and administration of automated data processing (ADP) security programs mandated by Departmental regulations (DR).

[1] Federal Information Security Management Act of 2002 replaced Government Information Security Reform Act and Computer Security Act of 1987.
[2] OMB Circular A-130, appendix III, Security of Federal Automated Information Resources, dated November 30, 2000.

Located in Washington, D.C., and staffed by about 450 employees, ERS is the main source of economic information and research for USDA. The mission of ERS is to inform public and private decision makers on economic and policy issues related to agriculture, food, natural resources, and rural development. Three ERS divisions, Food and Rural Economics, Market and Trade Economics, and Resource Economics, publish a wide variety of research reports and periodicals. To support these activities, the Information Services Division (ISD) manages and directs agencywide IT and communication activities by building and maintaining powerful analytical and communications environments as well as data dissemination systems to deliver agency products.

ERS' IT resources include a local area network (LAN) and two mission business systems, systems A and B. The LAN consists of workstations and servers that provide employees with office software, Internet access, and e-mail. While some sensitive data files reside on the LAN, most of the information is obtained from public sources, such as universities, State governments, other Federal agencies, and foreign governments, and typically pertains to crops, acreage, yield, cost and returns, situation and outlooks, and farm labor. Systems A and B, however, contain more sensitive information, including social security numbers and farm income and expenditures data tied to individuals. To protect the integrity and security of these computer systems, ERS uses logical access controls, such as computer passwords, and physical security measures to prevent incidental or malicious damage to its IT resources.

While the Internet was designed as an open system with no regard for security, new security standards are continually being developed, and safeguards such as encryption, data backup procedures and controls, network intrusion detection systems, and disaster recovery and contingency planning can be employed to afford some degree of security.

Objectives

The objectives of this audit were to (1) assess the overall management of ERS' Information Systems Security Programs (ISSP), (2) determine the adequacy of security over agency networks, and (3) determine if adequate logical and physical access controls exist to protect computer resources, including application and system software, against unauthorized modification, disclosure, loss, or impairment.

Findings and Recommendations

Section 1. ERS Has Not Ensured Compliance With Federally Mandated Security Guidelines and Is Lacking In Its Overall Management of IT Resources

As the foundation of USDA ISSP, security planning and management reflect senior management's commitment to addressing security risks. Without a well-designed program, an agency's security controls may be inadequate or inconsistently applied, and employee responsibilities may be unclear, misunderstood, and improperly implemented.

Through the Computer Security Act of 1987, Congress called for establishing minimum acceptable security practices for Federal computer systems. The Computer Security Act of 1987 requires agencies to identify and protect systems containing sensitive information and calls for a computer standards program and security training. Accordingly, OMB Circular A-130[2] established a minimum set of controls for agencies' automated information security programs, including assignment of security responsibility, security planning, periodic review of security controls, and management authorization of systems to process information.

Based on our review of ERS' security program, we concluded that the agency needs to improve its management of IT resources, and ensure compliance with existing Federal requirements for managing and securing IT resources. Specifically, ERS has not adequately planned for network security and conducted the necessary risk assessments of its network. We attributed these weaknesses to a need for additional management oversight. As a result, ERS' lack of compliance is a material internal control weakness, and its ability to accomplish its mission may be jeopardized if it cannot properly manage its IT infrastructure.

Finding 1 — ERS' Security Plan Was Incomplete and Not Fully Implemented

ERS' security plan did not meet federally mandated security requirements. Although the Office of the Chief Information Officer (OCIO) had waived the requirement to submit agency security plans in 2002, agencies still were required to ensure that all weaknesses identified in the 2001 security plan reviews were corrected. However, at the time of our review, ERS had not updated its 2001 security plan to incorporate all security requirements and had not implemented some of its security plan. These conditions existed because ERS had not assessed its ISSP and not implemented controls to ensure that security planning met requirements. As a result, ERS had no assurance that its security planning adequately protected its IT resources.

OMB Circular A-130[2] states that security plans should establish rules for employee behavior, a training program for computer security, personnel controls, an incident response policy, a contingency program, technical security controls, and system interconnectivity rules.

We reviewed ERS' fiscal year 2001 security plan and found that many of the policies it prescribed had not been implemented. For example, ERS' security plan established policies for security awareness training, screening individuals, incident handling, and contingency planning. At the time of our review, however, ERS had not implemented a formal computer security training program, obtained security clearances for employees in sensitive positions, established a formal incident response capability, or completed and tested a contingency plan.

Training

While the ERS security plan addressed computer security awareness training, ERS had not provided that training to all employees with access to the agency's computer system. ERS also had not implemented a formal training program to include controls to ensure that employees receive specialized training commensurate with their responsibilities.

Consequently, ERS had not complied with the Computer Security Act of 1987, which directs all agencies to provide mandatory periodic training in computer security awareness and accepted computer security practices for all employees who manage, use, or operate Federal computer systems within or under the supervision of that agency. OMB Circular A-130[2] requires that agency security plans establish controls to ensure that all individuals receive appropriate training in how to fulfill their computer security responsibilities before they are allowed to access the system. Such training may vary from a notification at the time of access to formal instruction. Federal regulations[3] require Federal agencies to provide mandatory training as set forth in NIST's guidance.[4] Further, OCIO[5] established guidance that requires all Department agencies and staff offices to develop, organize, implement, and maintain an IT system's security awareness training program to ensure the security of Department information and IT resources. The guidance also requires Department and staff offices to conduct this formal training at least annually.

To determine if agency personnel had received both kinds of required training, we took a judgmental sample of the 12 ERS employee personnel files with significant administrative responsibilities over the agency's

[3] Title 5, Code of Federal Regulations, section 903.301, revised January 1, 2001.
[4] NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, dated April 1998.
[5] OCIO CS-015, Cyber Security Guidance on Computer Security Awareness Training Programs, dated April 3, 2002.

IT resources. We found that none of the 12 files contained evidence to document that computer security awareness training had occurred. While 6 of the 12 employees had not received any kind of training, the other 6 had received some specialized training. However, ERS last provided specialized training to those employees in 1997.

We were told that ERS provides security awareness information to its employees through security brochures, presentations, the Intranet, and mass e-mails. In regard to specialized training, ERS provides job-specific training to its employees when new projects are being implemented and occasionally when employees request training. However, ERS should implement a formal training program to ensure that all employees who use computer systems receive mandatory annual security awareness training and employees who manage computer systems receive appropriate training in how to fulfill their responsibilities.

Screening Individuals

Although the ERS security plan mentioned employee screening, it did not provide any specific guidelines for determining whether a particular individual was suitable for a given position.

OMB Circular A-130[2] requires that agency security plans establish personnel controls for screening individuals who are authorized to bypass significant technical and operational security features of computer systems, commensurate with the risk and magnitude of harm they could cause. Such screening must occur prior to authorizing an individual to bypass controls, and periodically thereafter. According to NIST guidance,[6] background screening helps determine whether an individual is suitable for a given position and that, particularly within the Government, periodic rescreening of personnel can identify signs of possible illegal activity. Federal regulations[7] state individuals receiving an appointment made subject to an investigation must undergo a background investigation initiated before appointment or at most within 14 calendar days of placement in the position. Further, agencies may require employees to undergo periodic reinvestigations.

To assess whether ERS was requiring employee background screening, we took a judgmental sample of the same 12 ERS employee personnel files reviewed for training. Six of those files belonged to employees hired within the last 3 to 4 years. Of the six new hires, two had a security clearance requested by ERS, two received security clearances while employed by another agency, and two were student interns that did not receive security checks. Additionally, 8 of the 12 employees were authorized to bypass

[6] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, dated October 1995.
[7] Title 5, Code of Federal Regulations, section 731.106, revised as of January 1, 2003.

security controls, but 5 of the 8 employees had undergone security clearance investigations between 9 and 30 years ago.

We were told that, although background screening was not regularly performed until a few years ago, ERS had started an informal process to conduct background screening for all new hires. ERS' human resources staff was also verifying that employees hired within the last 3 to 4 years had background checks, but that effort did not include employees hired prior to the past 4 years. Without proper background checks on its trusted users, ERS does not have assurance that those users can be entrusted with network resources and data under its control.

Incident Handling

The ERS security plan addressed incident handling, but ERS had not established a formal incident response policy to ensure that events were documented and shared with OCIO.

OMB Circular A-130[2] requires that agency security plans include an incident response policy to ensure that system users receive help when a security incident occurs and that information concerning common vulnerabilities and threats is shared with other organizations. NIST guidance[8] states, when faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. Further, NIST guidance[9] states firewall administrators should examine the logs daily. Departmental guidance[10] states all USDA agencies and staff offices shall establish and implement an internal incident response capability. Further, each agency will develop internal reporting procedures that define the actions that must be taken in responding to and reporting security incidents. At a minimum, internal procedures will include the agency reporting chain and require the involvement of the agency personnel and Departmental Information Systems Security Program Manager (ISSPM).

We learned that all ERS employees are provided with a brochure that describes the agency's incident response policy. According to the brochure, ERS uses a team concept in handling security incidents — that is, each team decides what constitutes an incident and how to handle it. However, ERS had not issued specific written instructions to teams for handling and reporting security incidents.

[8] NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, dated December 1998.
[9] NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, dated January 2002.
[10] DM 3500-001, USDA Computer Incident Response Procedures, dated October 25, 2001.

ERS also had not documented several recent security incidents. Apart from receiving notification from OCIO of an attempted outside breach against its firewall, ERS had never experienced a major security incident according to ERS' ISSPM. However, OCIO had notified ERS of three minor security incidents within the last year, and ERS' ISSPM reviewed the incidents and took corrective action as deemed necessary. Those incidents included an attempted buffer overflow, in which an intruder tried to gain control of an ERS computer system by loading more data into a temporary storage unit than it was intended to hold, and Internet Protocol addresses attempting to penetrate the system. When we tried to validate how many security incidents were reported by OCIO, ERS' ISSPM could not supply any documentation on the incidents and did not know how many incidents had been reported.

Additionally, the ISSPM is responsible for reviewing the agency's firewall logs on a daily basis to monitor security incidents and sending the review results to OCIO at least 3 times a week. However, we learned that these reviews are not conducted if the ISSPM is not at work. The ISSPM will also scan from outside the firewall using a commercially available software product once a month and send the scan results to OCIO.

We concluded that, without a formal written incident response policy to ensure that incidents are documented and shared with OCIO, ERS may not be ready to protect its IT resources and assist in the protection of other Federal computer systems in the event of a major security incident.

Contingency Planning

Our review further disclosed that ERS' contingency plan, intended to ensure adequate recovery of computer resources in the event of a disaster or other major disruption in service, was incomplete and not properly applied.

OMB Circular A-130[2] requires that agency security plans establish controls to create and periodically test the agency's ability to continue providing service within a system based on the needs and priorities of system users. According to NIST,[6] contingency plans should be developed for restoring critical applications, including arrangements for alternate processing facilities in case the usual facilities are significantly damaged or cannot be accessed. The plans should also include (1) an assessment of critical data and operations to determine the importance and sensitivity of data and other organizational assets, (2) an identification of minimum computer resources needed to support critical operations, such as computer hardware, software, and data files, (3) a policy on data and software backup procedures, and (4) guidelines for mandatory training on employee responsibilities in preventing, mitigating, and responding to emergency situations.

Additionally, contingency plans should be kept up to date, approved by senior management, and tested periodically to discover inevitable flaws.

First, we found that ERS had not identified and prioritized all of its critical resources. For example, the agency's security plan described the sensitivity of information handled on system A, but it did not rate or describe the data maintained on system B, which also contained confidential information. However, ERS' security plan did describe the computer hardware and software used on the LAN to support these IT resources.

Further, we found that ERS' contingency plan had not been updated, approved by senior management, or tested. ERS' ISSPM stated that the contingency plan could not be tested until the agency secured and approved a backup site for continuity support.

In addition to flaws with the contingency plan itself, our assessment disclosed that ERS had not implemented appropriate data and program backup procedures. Specifically, we found that ERS was not keeping its wide area network (WAN) backup diskettes offsite. The ISSPM assumed the backup diskettes were kept offsite. This assumption was corroborated by an ERS WAN team member who stated that he took the backup diskettes home in case a disaster prevented access to the bank vault across the street. However, we found 12 weekly backup diskettes stored onsite in a fireproof safe. We also validated that the team member did not take LAN backup tapes home but only took a backup copy of the WAN software settings home. After further discussion of the importance of storing backup data offsite, ERS representatives agreed to keep the backup diskettes in an offsite bank vault.

ERS also had not implemented adequate continuity controls over its physical environment. Although the agency had a sophisticated electronic fire protection system, including sprinkler heads, smoke detectors, heat detectors, manual pull stations, security door override, remote monitor alarm, tamper detection systems, and a building-wide alarm system, ERS had inadequate controls in place to fully recover in the event of natural disasters, such as floods or earthquakes. We noticed that water could leak into or flood the LAN room because it contained a wet-pipe sprinkler system. An ERS representative stated the LAN room has a water detector that will sound an alert for leaks or floods. We requested, but ERS did not provide, a floor plan showing the location of the water detectors.

We concluded that ERS had not fulfilled all contingency planning requirements or taken steps to minimize and prevent potential damage and interruption of its system by implementing adequate backup procedures and environmental controls.

Recommendation No. 1

Establish and implement controls to periodically assess the IT security program to ensure that security planning meets USDA, OMB, NIST, and other Federal requirements.

Agency Response. ERS concurs with this recommendation. ERS will create a formal process to assess the IT security program through an annual review of the current security plan before it is submitted to OCIO, USDA. ERS plans to apply this review process to the 2004 submission of the security plan. This review will be performed by agency Data Coordinators and the Chief Information Officer.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of the documentation detailing the formal process created for assessing the IT security program.

Recommendation No. 2

Establish and implement a formal training program, to include controls to ensure that all employees who use computer systems receive mandatory annual security awareness training and employees who manage computer systems receive appropriate training in how to fulfill their responsibilities.

Agency Response. ERS concurs with this recommendation. USDA's OCIO has implemented an e-Government system that provides all USDA employees with a number of basic training classes through the Government-wide GoLearn program. ERS has begun to use this resource, as directed by OCIO, to provide each employee with security training classes. To improve tracking of employee training, USDA is in the process of integrating a Learning Management System into the GoLearn system. The Learning Management System will be operational in 2004 and integrated into human resource systems to improve management of training. ERS plans to utilize this system to track and document employee participation and completion of training classes.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with documentation supporting ERS' utilization of the Learning Management System for tracking and documenting employee training.

Recommendation No. 3

Establish a formal screening policy to include controls to ensure that individuals with significant security responsibilities are screened prior to appointment or within 14 calendar days of placement in the position and periodically rescreened.

Agency Response. ERS concurs with the recommendation. In January 2003, ERS identified positions with significant security responsibilities and submitted applications for security clearances for all ISD personnel with major security responsibilities. Many of these applications are still pending for final approval. Additionally, position descriptions for the covered positions have been revised to include the requirement for security clearances, the level of clearance required, and the reauthorization timeframe.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its formal screening policy outlining the controls to ensure employees with significant security responsibilities are screened prior to appointment and periodically. In addition, ERS needs to provide OCFO/PAD with a copy of the revised position descriptions.

Recommendation No. 4

Establish a formal written incident response policy to include controls to ensure that all security incidents are documented and shared with OCIO.

Agency Response. ERS concurs with this recommendation. By October 1, 2004, ERS will create a policy for the review and documentation of all security incidents. The log will record the incident and the date it is forwarded to OCIO. ERS will only document significant incidents that are unique or cause a serious threat to security.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its formal incident response policy outlining the controls to ensure that all security incidents are documented and shared with OCIO.

Recommendation No. 5

Establish and implement procedures, to include control measures, that govern the preparation of a contingency plan to (1) identify and prioritize critical operations and the resources supporting them, (2) contain backup procedures and environmental controls, and (3) develop emergency priorities to support the continuity of these operations. The contingency plan should also be approved by senior management and tested annually.

Agency Response. ERS concurs with the recommendation. By October 2004, ERS will review its existing Continuity of Operation Plan to identify additional needs for contingency planning. ERS will modify the Continuity of Operation Plan to include contingency plans for identifying critical operations and necessary resources and current LAN backup procedures for logging the movement of tapes from the central backup system to offsite location. ERS also is making progress in preparing a disaster recovery plan for critical systems by installing and testing recovery systems onsite and at a remote location. ERS plans on conducting disaster recovery tests twice each year and performing ongoing operations to keep systems current.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of the revised Continuity of Operation Plan and disaster recovery plan that has been tested and approved by senior management.

Finding 2 **ERS Needs a Formal Program to Periodically Review Security Controls**

ERS had no formal program for periodically evaluating its security policies and conducting risk assessments to determine the extent of potential threats and risks associated with its IT resources. Management had not established controls to evaluate the security program for compliance with Federal information resource policies and failed to hire skilled personnel to conduct risk assessments. Therefore, the agency had no assurance that its current IT security measures were adequate to protect its computer system and the information it processes.

OMB Circular A-130[2] requires agencies to conduct annual security reviews and perform a risk analysis at each ADP site every 3 years, or when systems undergo significant modification. In addition to OMB requirements,

Departmental guidance[11] requires agencies to perform formal risk analyses. Further, Presidential Decision Directive 63 requires agencies to assess the risks to their networks and establish a plan to mitigate the identified risks.

In addition, NIST guidance[8] states that, because the security of a system may degrade as technology evolves or people and procedures change, periodic reviews provide assurance that security controls are functioning effectively and providing adequate levels of protection. Further, technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software patches), and penetration testing can assist in the ongoing review of system security measures. These tools, however, are no substitute for a formal management review at least every 3 years. OCIO guidance[12] mandates requirements for regular risk assessments using checklists designed to determine vulnerabilities on most common IT platforms and environments.

ERS senior management has ultimate responsibility for security of the agency's computer systems. However, ERS' ISD Branch Chief stated that the agency had no official program for reviewing security policies and that no other audits or security reviews had occurred. He also stated that ERS had not budgeted for hiring a skilled person solely to conduct risk assessments. By implementing formal procedures for periodic reviews and conducting risk assessments, ERS would be able to determine if appropriate security measures have been implemented and if the level of risk associated with its IT resources is acceptable.

Additionally, since it had not evaluated its security policies or conducted a risk assessment, ERS could not officially authorize its systems for operations and processing. We noted that the agency had not formally authorized its general support and application systems. NIST guidance[8] states that a management official must authorize a system to operate and process information based on an assessment of management, operational, and technical controls.

Recommendation No. 6

Establish and implement formal procedures for annual periodic reviews of management, technical, and operational controls, and conduct risk assessments every 3 years or when systems undergo significant modification.

[11] Departmental Manual 3140-1.1, Management of ADP Security Manual, dated July 19, 1984.
[12] OCIO CS-016, Cyber Security Guidance Regarding Risk Assessments and Security Checklists, dated July 19, 2002.

Agency Response. ERS concurs with the recommendation. ERS will conduct its first annual review of management, technical, and operational controls of its security systems in May 2004 during the security plan review process. It will include the necessary procedures for establishing and reviewing risks. ERS also has completed a preliminary risk assessment of its WAN/LAN systems. A risk evaluation of the WAN/LAN systems, which are the foundations of all systems and applications, will serve as an essential part of any other critical system evaluations.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its formal procedures for annual periodic reviews of IT security controls and for conducting risk assessments.

Recommendation No. 7

Establish and implement a process for managers to formally authorize the adequacy of existing security for the computer systems they operate or applications they develop. Computer systems and applications should be reauthorized every 3 years or when systems undergo significant modification.

Agency Response. ERS concurs with this recommendation. ERS will create a process for managers to formally authorize the security of systems or applications that are under their responsibility. The review will be part of the preparation and review of the annual security plan. The policy describing the process will be completed by the end of 2004.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with documentation detailing the process for managers to formally authorize the adequacy of existing security.

Coupled with a strong security plan and management oversight, proper use of technical tools and resources can contribute to the overall security of an agency's ISSP. To evaluate ERS' systems, we used three commercially available software products that (1) tested for over 1,100 known vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol,[13] (2) tested system policy settings in network operating systems, and (3) searched for modems within a set of telephone numbers to identify potentially unsecured carrier lines.

Finding 3 Vulnerabilities Expose ERS Systems to the Risk of Attacks

Our vulnerability scans of selected ERS systems disclosed risk indicators that could be exploited. We also found that system policy settings did not provide for optimum security and were not uniform throughout the agency. Many of these vulnerabilities occurred because ERS had not developed a configuration management program to ensure routine maintenance of all systems with recent security patches and other software updates. As a result, ERS systems and networks were vulnerable to cyber attacks. We consider the number of vulnerabilities identified to be a material internal control weakness that requires additional management oversight.

OMB Circular A-130[2] requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce threats and potential losses.

Transmission Control Protocol/Internet Protocol System Vulnerabilities

Our vulnerability assessments of 103 network components disclosed 203 high-risk, 636 medium-risk, and 1,456 low-risk vulnerabilities. The high- and medium-risk vulnerabilities, if left uncorrected, could allow unauthorized users to access critical and sensitive ERS data. Additionally, the large number of low-risk vulnerabilities we identified can be an indication that ERS needs to strengthen its system administration.

[13] Transmission Control Protocol/Internet Protocol is a series of protocols originally developed for use by the U.S. military and now used on the Internet as the primary standard for the movement of data on multiple, diverse platforms.

Detailed below are examples of the high-risk vulnerabilities we identified.

- Of the 203 high-risk vulnerabilities, 79 related to inadequate or nonexistent passwords. For example, seven accounts were set to allow access using a password that was the same as the administrator user name. As the most trusted user on a system, the administrator has complete control over the system and can perform any function. Additionally, we detected 25 accounts with a blank password or no required password. Depending on the accounts' access privileges, an attacker could use them to access other computers on the network, including the data stored in those computers.

- Three hosts had accessible default accounts that could be detected through a remote administration program. When software applications used to manage computer networks are left configured with their original default settings, which are well known, intruders are able to easily obtain or change system data and to gain information about open connections with other systems. Under an effective security policy, these accounts would be removed, renamed, or, at minimum, have a difficult-to-guess password.

ERS officials stated that they scanned selected network servers on a monthly basis using a scanning tool similar to ours. However, we discovered that the agency was not using all of the scanning software's functions. Depending on the purpose of the scan, users of the software can select various scanning policies to perform a range of tasks. Instead of using policies to detect systems that were improperly configured or compromised by highly skilled attackers, ERS used only the scan policy that identifies services running on the machines connected to its network. While this policy did identify some vulnerabilities, other significant risk indicators went undetected.

We also determined that ERS was not aggressively following up to eliminate security vulnerabilities that had already been discovered on its systems. We compared the results of scans conducted by ERS to the scans we performed. On one system, we found that a high-risk vulnerability identified by ERS in February 2002 still existed on that host 10 months later. Additionally, when we followed up with ERS 3 months after conducting our scans in December 2002, the agency had not begun mitigating the weaknesses we identified because the ISSPM was busy with other priorities.

Network Operating System Policies

Our detailed assessment of security over the ERS network operating system identified many access control weaknesses. To make our assessment, we used software that produced reports of access control lists, user account characteristics, password controls, and many other security features.

Some of the weaknesses we identified in this area are detailed below.

- Of the accounts, 73 had passwords that never expired. According to NIST guidance,[14] passwords should be changed periodically. Similarly, OCIO guidance[15] requires passwords for all systems, applications, and processes to be changed every 60 days for general users. Passwords issued to system administrators, system managers, and software engineers or those used for dial-in access are to be changed every 30 to 45 days.

- All 11 administrator-equivalent accounts had passwords that never expired, and the passwords for only 2 of those accounts had been changed within the last 30 to 45 days. Further, 1 of the 11 accounts had not been logged on in over a year.

- Of the 25 users, 7 with remote access settings enabled had passwords that never expired, and those passwords had not been changed within the last 30 to 45 days.

- Of the 595 user accounts on the system, 58 users had not logged in within the last 90 days. Of these 58 accounts, 26 included the word "Delete" in the full-name identifier, but the account remained on the system. Further, 19 of the 58 accounts were enabled, even though 8 of them had not logged into the system in over a year.

- Of the accounts that existed on the ERS LAN, 39 were shared or generic user accounts. Of the 39 accounts, 7 were still active even though they had not logged into the system within the last 90 days. Furthermore, NIST guidance[6] states that these kinds of accounts make it impossible for system administrators to track the actions of users in the event that inappropriate or malicious activity occurs. Likewise, OCIO guidance[15] prohibits shared accounts by requiring that each access, whether a user ID or process, be traceable to an individual.

[14] NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dated September 1996.
[15] OCIO CS-013, Cyber Security Guidance Regarding Controlled Access Protection, dated March 6, 2002.

We immediately communicated the results of our review of the network operating system to ERS management. Based on our findings, ERS took action to correct the weaknesses we identified. Specifically, ERS changed all nonexpiring passwords to expire every 35 days, eliminated dial-up access for the 25 users identified in our review, deleted 35 unused accounts, and disabled another 5 unused accounts from the ERS network.

Modem Security

ERS lacked a comprehensive modem listing, indicating lack of control over network gateways and noncompliance with regulations.

The presence of unauthorized modems attached to network computers can undermine a well-thought-out security plan. For example, if a computer with an unauthorized modem is connected to an agency's network, anyone with minimal computer skills and malicious intent can use the unsecured modem as a back door into the network. Thus, regulations[16] require agencies to evaluate security measures in place on network gateways. Regulations[17] also mandate that agencies conduct vulnerability and risk assessments of existing gateways at annual intervals.

Although ERS officials recognized that some of the agency's desktop computers had modems that connected to an Internet service provider instead of accessing the Internet through the Departmental network, they were unable to provide a complete inventory of modems within ERS' network. ERS officials added that they had never scanned their system for these modems. We conducted a detailed assessment of over 1,000 ERS telephone numbers to identify active modems and areas of inadequate security over modems on the network. Our assessment identified a total of 38 lines that could potentially have been modems. ERS officials noted that these were probably part of their dial-in modem bank but were still researching them at the end of our fieldwork. ERS should maintain an accurate list of all the modems on its network to ensure that they are properly configured and ensure that they are not used inappropriately to circumvent firewall and other network security measures it has in place.

Configuration Management

Our scans further revealed that ERS had not developed a configuration management program for its systems. Significant variations appeared in the high-risk vulnerabilities we identified, indicating that security patches were

[16] DR 3140-001, USDA Information Systems Security Policy, dated May 15, 1996.
[17] DR 3140-002, USDA Internet Security Policy, dated March 7, 1995.

not consistently applied.[18] Likewise, 100 of the 203 high-risk vulnerabilities we identified existed because the agency had not applied security patches and other software updates to its systems in a timely manner. Patches for 36 of the 100 vulnerabilities had been available for over a year.

Today more than ever, timely response to vulnerabilities is critical to maintain the operational availability, confidentiality, and integrity of IT systems. A configuration management program ensures that all systems are routinely maintained with recent security patches and other software updates. We concluded that a system configuration management program, including regularly scheduled and properly conducted vulnerability assessments and timely remediation of the risks discovered, would substantially enhance the security of ERS' network operating systems.

Firewall Configuration

Finally, we reviewed ERS' firewall configuration to determine if it was adequately protecting the network. Overall, we found that ERS had maintained its firewall adequately. However, we found several firewall rules that were either no longer needed or were not configured in the best interest of ERS network security. ERS had not established controls to conduct routine and timely reviews of firewall configuration. Therefore, ERS' network was exposed to risk of attack from Internet users.

NIST guidance[19] states firewall and security policies should be audited and verified at least quarterly. At a minimum, firewall policy can be verified by obtaining hardcopies of the firewall configurations and comparing these hardcopies against the expected configuration based on defined policy.

ERS officials took immediate action on most of our concerns by either deleting or modifying firewall rules to improve security. However, the network officials accepted the risks posed by two of our concerns. Additionally, ERS officials informed us that they routinely reviewed the access logs generated by the firewall, but they only infrequently reviewed the firewall rules that protect the network.

[18] According to NIST guidance, security-related programming flaws are generally discovered only after a large number of users start using the software and hackers and independent testers start attempting to compromise it. Once a programming flaw is discovered, the software manufacturer often releases a piece of software to correct the flaw. This software is often called a patch, hot fix, or service pack.
[19] NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, dated January 2002.

Recommendation No. 8

Ensure that corrective actions have been taken on all high- and medium-risk vulnerabilities identified during our audit, track the vulnerabilities, and certify that actions have been taken to remedy these vulnerabilities.

Agency Response. ERS concurs with this recommendation. By June 2004, ERS will have completed the procedures to identify and track all security vulnerabilities of its systems. OIG Recommendations Nos. 9 through 13 provide more specific coverage of actions to be taken in this regard. Under these specific recommendations, ERS will take corrective actions as it judges necessary. Some vulnerabilities identified in the audit cannot be corrected due to changes in IP address assignments. If a particular vulnerability cannot be traced to a specific workstation or device, the agency will not be able to make a correction. As with other issues, the agency will evaluate the risk associated with a particular vulnerability and will take appropriate actions based on the findings.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with documentation certifying that appropriate corrective actions have been taken to remedy these vulnerabilities.

Recommendation No. 9

Establish and implement a policy to use the proper scanning policy to detect all network vulnerabilities and ensure that prompt action is taken to eliminate noted vulnerabilities.

Agency Response. ERS concurs with the recommendation. ERS has created a scanning policy that will be implemented in March 2004. The policy specifies the types of scans to be conducted; scans will be conducted monthly and activities to correct vulnerabilities will be tracked in a log.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its scanning policy for detecting and eliminating all network vulnerabilities.

Recommendation No. 10

Establish and implement a policy outlining minimum computer access security settings to include controls to ensure that settings have not been misapplied.

Agency Response. ERS concurs with this recommendation. There are various policies in place, but they are not comprehensive. ERS will document existing policies for access security settings and will create a process to review compliance with these policies. The process will provide for timely review and correction of deficiencies and will be in place by the end of 2004.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with documentation of computer access security setting policies and process for timely reviewing compliance with these policies.

Recommendation No. 11

Establish and implement a configuration management program to include controls to ensure that the program is functioning as planned.

Agency Response. ERS concurs with this recommendation. ERS has implemented a configuration management program that includes controls to ensure that the program is functioning as planned. ERS participates in the USDA program to license a system that provides centralized configuration management and reporting. ERS has been utilizing the system to keep all operating systems patched to avoid critical security vulnerabilities since December 2003.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with documentation identifying the configuration management program, including controls to ensure that the program is functioning as planned.

Recommendation No. 12

Establish and implement a remote access policy to include controls to establish an accurate list of all modems on its network, ensure that they are properly configured, make sure that they are not used inappropriately to circumvent firewall and other network security measures it has in place, and update the listing on a periodic basis.

Agency Response. ERS concurs with this recommendation. By June 1, 2004, ERS plans to complete the inventory of all modems on its network and will develop a policy to specify how and when modems are authorized for connection to the network. There will be an annual review of the configuration and usage of the modems. ERS has been incrementally eliminating the use of modems from its network and will continue with this effort.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its remote access policy, including controls to ensure that modems are not used inappropriately to bypass network security.

Recommendation No. 13

Establish and implement a policy to include controls to conduct routine and timely reviews of firewall configuration.

Agency Response. ERS concurs with this recommendation. ERS has created a policy for quarterly reviews of the firewall configuration. The review will focus on the adequacy of rules incorporated into the configuration and the elimination of unnecessary rules. The first review was completed during February 2004. The policy includes documenting all of the existing rules and any actions taken during the review.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its firewall review policy, including controls to ensure that firewall rules are adequate and documented.

We assessed ERS' logical and physical access controls to determine if they adequately detected and prevented unauthorized entry to agency automated information and computer systems. We found a significant number of logical control weaknesses in the systems we tested, as well as problems related to physical access.

OMB Circular A-130[2] stresses management controls affecting IT users. These controls help to protect operating systems and other software from unauthorized modification and to protect the integrity, availability, and confidentiality of information by restricting the number of users, and provide protection from disclosure of information to unauthorized individuals. NIST guidance[6] defines access controls as physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.

Finding 4 ERS Needs to Strengthen Its Access Controls

Although ERS had established procedures for requesting computer access and reviewed user access lists, the agency had not reviewed its computer access procedures to determine if they were adequate. ERS also had not conducted a security assessment of logical and physical access controls to determine if they met departmental guidelines. ERS had not established controls to ensure compliance with Federal information resource policies and failed to hire skilled personnel to conduct risk assessment. Therefore, ERS had no assurance that its computer resources are protected against unauthorized access.

OMB Circular A-130[2] and Departmental guidance[11] contain standards, guidelines, and procedures for the development and administration of agencies' automated information security programs. Agencies are required to establish controls to assure adequate security for all information they process, transmit, or store. Further, agencies must review the security controls in each system at least every 3 years, or when significant modifications are made to the system; the scope and frequency of these reviews must be commensurate with the acceptable level of risk for the system. NIST guidance[8] advises that periodic reviews provide assurance that controls are functioning effectively and providing adequate levels of protection. Further, NIST guidance[14] states organizations should base access control policies on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their

official functions, and organizations should carefully administer access controls.

Logical Access

We found a significant number of material logical access control weaknesses in the ERS systems we tested. We also found that ERS had not conducted periodic reviews to determine if its logical access controls were adequate to protect sensitive data. ERS' ISD Branch Chief stated that there had been no other audits or security reviews at ERS, and that the agency had no official program for reviewing security policies.

Our review disclosed that ERS' lists of users authorized to access the LAN, the National Finance Center, and the National Information Technology Center are not being regularly reviewed and had not been updated to reflect current users. Specifically, we found that ERS' computer access lists contained enabled user IDs for separated personnel, disabled user IDs, duplicate IDs, user names that had not been changed, and inaccurate and incomplete information maintained for non-Federal employees.

Departmental guidance[20] requires security staff to remove employee user IDs and passwords when the employee is no longer with the agency. A formal procedure should be established for notification of the security officers by the agency personnel office of all retirements or other personnel separations. When there is a change of a contractor that uses the system, all user IDs and passwords on the system must be changed as soon as the contractor's services are terminated. Security staff must maintain files of users, including names, office addresses, and telephone numbers.

ERS' representative for ISD explained that it was difficult to maintain computer access lists since ISD was not always informed and did not always receive the separating employee's checklist. ERS' procedure for separating employees instructs supervisors to circulate a separating employee's checklist to ISD for removal of the employee's access to agency computer systems. Furthermore, ISD also did not receive the list of current and separated contractors and non-Federal employees. ERS should strengthen its internal controls to ensure that all computer access lists are updated and routed to ISD, and ISD is notified and receives the separating employees' checklists when employees terminate their employment.

We also reviewed ERS user profiles and identified 65 users that had shared or generic accounts. Of these accounts, 4 permitted users to access sensitive data, and the remaining 61 accounts allowed access only to standard software packages. Departmental guidance[20] states issuance of group user IDs and passwords and the sharing of the same are not permitted.

[20] DM 3140-1.6, Management ADP Security Manual, dated July 19, 1984.

When we inquired into the use of these accounts, ERS staff stated that they were needed for a special project related to homeland security. ERS LAN staff also stated that they were in the process of reviewing shared and generic accounts and disabling or deleting them. We concluded that ERS should establish formal access authorization procedures for periodic review and maintenance of computer access accounts, including review of access logs by management, independent of the security function.

In regard to remote access, our review disclosed that ERS had not reviewed its security controls in that area to determine if they were adequate. Although ERS justified, documented, and approved requests according to NIST guidance,[14] it had not periodically reviewed controls over remote access. At the time of our review, remote users could access ERS' network through three methods, but only one of those methods was approved by ERS for users handling the agency's sensitive data. Data transmitted through the other two methods is either not encrypted or secure and could permit unauthorized access. However, we found that some users who handled sensitive data could use unapproved methods for remote access. For example, some users who are authorized to handle sensitive data on one of its systems, such as farm income and social security numbers, also had the capability to access this data through unapproved methods. We concluded that ERS should periodically review its list of remote access users to ensure that it grants them only the appropriate access.

Finally, we reviewed ERS' network account policy settings and found that the parameters established for password uniqueness and logon attempts did not meet established guidelines. According to OCIO guidance,[15] systems shall not allow reuse of a previously used password until after five different passwords have been used. Departmental guidelines[20] require that access to the system be rejected after three bad logon attempts.

Although the LAN staff told us that they met regularly to discuss security and had agreed to set password history to 3, and bad logon attempts to 5, our review of ERS network account policy settings found the parameter for password history set to 3 and bad logon attempts set to 10. The LAN staff did not know when the parameter for bad logon attempts was set at 10.

We concluded that ERS should establish guidelines to periodically review its network account policy settings, as well as user access and user profiles.

Physical Access

Our assessment of ERS' physical access controls disclosed improper procedures, which posed a threat to security of the LAN room and backup tapes.

We found that ERS controls access to the LAN room by issuing electronic security keys to employees and contractors. OCIO guidance[21] states that only Department personnel and authorized contractors having an ongoing recurring business need will be given unescorted access to the IT restricted space. Further, cleaning staff, maintenance personnel, and visitors shall be escorted at all times by Department or permanent contractors. ERS provided us a list containing the names of individuals who had been issued electronic security keys for access to the LAN room and assisted us in reviewing it. The list included multiple individuals from the cleaning staff and one other employee who should not have had access. We concluded that ERS should not issue electronic security keys to cleaning staff, maintenance personnel, and visitors for physical access to sensitive areas.

Furthermore, ERS did not maintain logs for documenting visitors to sensitive areas or for recording the transfer of LAN backup tapes to and from offsite storage. NIST[6] and OCIO[21] guidance state that logs can include the times and dates of transfers, names and signatures of individuals involved, and other relevant information. By maintaining physical access control logs for sensitive areas and backup tapes, ERS can protect its computer resources from unauthorized access and hold authorized individuals accountable for their actions.

We tested ERS' physical access controls by requesting entry to the LAN room and by accompanying an ERS employee to deposit LAN backup tapes at the offsite storage facility. We did not have to sign a log when we toured the LAN room, nor did the ERS employee sign a log to track the movement of the LAN backup tapes. We concluded that ERS should escort all visitors to the LAN room and other sensitive areas and require visitors to sign a log upon entering and exiting the facility.

Logical controls alone cannot protect the integrity and confidentiality of sensitive files. For this reason, it is important that ERS establish formal procedures to ensure that physical access to the LAN room and backup tapes are controlled. ERS should also conduct periodic physical access reviews to determine if controls are effective in preventing unauthorized access to computer resources.

[21] OCIO CS-05, Cyber Security Guidance on Physical Security in USDA IT Restricted Space, dated November 28, 2001.

Recommendation No. 14

Establish and implement formal procedures and controls for periodic reviews of logical and physical access controls to determine if controls are up to date and functioning as designed.

Agency Response. ERS concurs with this recommendation. By January 1, 2005, ERS will conduct quarterly reviews of its logical and physical access controls to include enforcing existing procedures in notifying security staff when employees or contractors no longer require system access. The procedure will include a review process by the Chief Information Officer and agency Data Coordinators to judge the adequacy of the process. The review will use the agency's e-mail address book to provide information on current status of employees, their room numbers, and phone numbers.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its written formal procedures developed for the quarterly review process of logical and physical access controls.

Recommendation No. 15

Establish and implement internal control procedures to ensure that all computer access lists are updated and routed to ISD, and that ISD is notified and receives a separating employees' checklist when employees terminate their employment.

Agency Response. ERS concurs with this recommendation. By July 1, 2004, ERS will review the existing procedure for clearing employees as they depart the agency. The review will add requirements for non-Federal employees and contractors. The review will focus on creating assurances that policy is being followed and that ISD is receiving proper notification.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its written procedures including controls to ensure that access lists are updated and routed to ISD, and that ISD is notified when employees terminate their employment.

Recommendation No. 16

Establish and implement formal access authorization procedures to include controls for periodic review and maintenance of computer access accounts, including review of computer access lists, LAN account policy settings, and access logs.

Agency Response. ERS concurs with this recommendation. This is similar in nature to Recommendation No. 10. The agency response there should cover this recommendation as well.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD with a copy of its written procedure, including controls detailing the steps security personnel are to follow in authorizing access and in performing periodic reviews of access accounts to ensure that access granted to employees is appropriate for their assigned duties.

Recommendation No. 17

Establish and implement formal physical access control procedures for logging visitor access to the LAN room and tracking the location of backup tapes.

Agency Response. ERS concurs with this recommendation. ERS has created a logbook to document physical access to the LAN room and has created logs to track the location and movement of backup tapes.

OIG Position. We accept the ERS management decision. For final action, ERS needs to provide OCFO/PAD a copy of the logbooks created to document physical access to the LAN room and to document the movement of backup tapes.

Scope and Methodology

We selected ERS as part of a nationwide review of eight USDA agencies with major computer systems. Audit work was performed at the ERS National Office located in Washington, D.C. We reviewed controls over the agency's computer systems to ensure the integrity of its information security program. Our fieldwork was performed during and for the period October 2002 through June 2003.

To accomplish the audit objectives, we performed the following steps.

- Tested ERS' security programs, including both physical and logical access controls, by analyzing records and controls established by the agency to protect its computer systems.

- Reviewed and compared the controls ERS had established to protect its IT resources with the requirements of the Computer Security Act of 1987, Federal regulations, departmental regulations and manuals, and other sources.

- Interviewed ERS officials responsible for managing the agency's computer systems.

- Referred to Government policies such as Presidential Decision Directive 63 and used commercial, off-the-shelf software products to scan 103 ERS critical network components for vulnerabilities.

This audit was conducted in accordance with generally accepted Government auditing standards. Therefore, the audit included tests of program and accounting records considered necessary to meet the audit objectives.

USDA

United States Department of Agriculture

MAR 3 0 2004

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

FROM: Susan Offutt
Administrator
Economic Research Service

SUBJECT: Management and Security of Economic Research Service
Information Technology Resources Audit 140099-1-Te

Below is the ERS response to your recommendations made as a result of the audit of the management and security of the Agency's Information Technology Resources. This response represents our commitment to resolve the identified deficiencies.

Recommendation No. 1 Establish and implement controls to periodically assess the IT security program to ensure that security planning meets USDA, OMB, NIST, and other Federal requirements.

Agency Response ERS will create a formal process to assess the IT security program through an annual review of the current Security Plan before it is submitted to the OCIO, USDA. We plan to apply this review process to the 2004 submission of the security plan. This review will be performed by the Agency Data Coordinators and the CIO.

Recommendation No. 2 Establish and implement a formal training program to include controls to ensure that all employees who use computer systems receive mandatory annual security awareness training and employees who manage computer systems receive appropriate training in how to fulfill their responsibilities.

Agency Response USDA's OCIO has implemented an eGovernment system that provides all USDA employees with a number of basic training classes through the government-wide GoLearn program. ERS has begun to use this resource, as directed by the OCIO, to have each employee take the security training classes. However there was no good methodology to track employee completion of the training available at this time. USDA is continuing to build on this eGov system and is in the process of integrating a Learning Management System (LMS) into the GoLearn system. The LMS will be operational in 2004 and will be integrated into Human Resource Systems to improve management of training. ERS plans to utilize this system to track and document employee participation and completion of training classes.

Economic Research Service
1800 M Street, NW, Washington, DC 20036-5831
www.ers.usda.gov

Recommendation No. 3 Establish a formal screening policy to include controls to ensure that individuals with significant security responsibilities are screened prior to appointment or within 14 calendar days of placement in the position and periodically rescreened.

Agency Response In January 2003, ERS identified the positions with significant security responsibilities. Additionally, Position Descriptions for the covered positions have been revised to include the requirement for security clearances, the level of the clearance required, and the reauthorization timeframe.

In January 2003, ERS submitted applications for Secret or Top-Secret security clearances for all ISD personnel with significant security responsibilities. Many of these clearance applications are still pending for final approval.

Recommendation No. 4 Establish a formal written incident response policy to include controls to ensure that all security incidents are documented and shared with the OCIO.

Agency Response By October 1, 2004, ERS will create a policy for the review and documentation of all security incidents. Under this policy, a log will record the incident and the date it is forwarded to the OCIO. However, ERS cannot possibly document and report every attempt to penetrate ERS systems. Each day there are hundreds of attempts to probe and attack agency operations that are automatically repelled by the various security systems in place. ERS will only document significant incidents that are unique or cause a serious threat to security.

Recommendation No. 5 Establish procedures to include control measure that govern the preparation of a contingency plan to (1) identify and prioritize critical operations and the resources supporting them, (2) contain backup procedures and environmental controls, and (3) develop emergency priorities to support the continuity of these operations. The contingency plan should also be approved by senior management and tested annually.

Agency Response By October 2004, ERS will review existing policy for the creation and operation of the agency's Continuity Of Operation Plan to identify the additional needs for a contingency plan. Changes to the COOP will include the contingency plans for critical operations and the resources necessary for their operations. ERS currently has procedures for backups of all LAN servers and the data stored on them. This will be reviewed and modified to include logging the movement of tapes from the central backup system to the offsite location. Additionally, ERS has completed the first step in providing a disaster recovery plan for the most critical systems. The servers have been installed in the LAN room for testing and actions are underway to have the recovery system installed at a remote location. Through this scenario, the disaster recovery will be tested at least twice each year and ongoing operations will be conducted to keep the systems current.

Recommendation No. 6 Establish and implement formal procedures for annual periodic reviews of management, technical, and operational controls, and conduct risk assessments every 3 years or when systems undergo significant modification.

Agency Response ERS will conduct annual review of management, technical, and operational controls of its security systems. The first review will be conducted in May 2004 during the annual review of the agency security plan. It will include the necessary procedures for establishing and reviewing risks. ERS has completed a preliminary risk assessment of its WAN/LAN systems. The WAN/LAN systems are the foundation of all systems and applications within the agency and the risk evaluation will be the core of any other critical system evaluations. ERS will continue with this review and proceed through certification and accreditation by October 2004.

Recommendation No. 7 Establish and implement a process for managers to formally authorize the adequacy of existing security for the computer systems they operate or applications they develop. Computer systems and applications should be reauthorized every 3 years or when systems undergo significant modification.

Agency Response ERS will create a process for managers to formally authorize the security of systems or applications that are under their responsibility. The review will be part of the preparation and review of the annual security plan. The policy describing the process will be completed by the end of 2004.

Recommendation No. 8 Ensure that corrective actions have been taken on all high and medium risk vulnerabilities identified during our audit, track the vulnerabilities, and certify that actins have been taken to remedy these vulnerabilities.

Agency Response By June 2004, ERS will have completed the procedures to identify and track all security vulnerabilities of its systems. The OIG recommendations 9 through 13 provide more specific coverage of actions to be taken in this regard. Under these specific recommendations, ERS will take corrective actions as it judges necessary. Some vulnerabilities identified in the audit can not be corrected due to changes in IP address assignments. If a particular vulnerability can not be traced to a specific workstation or device, the agency will not be able to make a correction. As with other issues, the agency will evaluate the risk associated with a particular vulnerability and will take appropriate actions based on the findings.

Recommendation No. 9 Establish and implement a policy to use the proper scanning policy to detect all network vulnerabilities and ensure that prompt action is taken to eliminate noted vulnerabilities.

Agency Response ERS has created a policy to improve scanning following the OIG recommendation to implement to prevent compromise by highly skilled attackers. The policy specifies the types of scans to be conducted starting in March 2004. The scans will be conducted monthly and activities to correct vulnerabilities will be tracked in a log.

Recommendation No. 10 Establish and implement a policy outlining minimum access security settings to include controls to ensure that settings have not been misapplied.

Agency Response There are various policies in place but they are not comprehensive. ERS will document existing policies for access-security settings and will create a process to review

compliance with these policies. The process will provide for timely review and correction of deficiencies and will be in place by the end of 2004. As noted in the audit, ERS have made many corrections as they were identified by the auditors.

Recommendation No. 11 Establish and implement a configuration management program to include controls to ensure that the program is functioning as planned.

Agency Response ERS has implemented a configuration management program that includes controls to ensure that the program is functioning as planned. ERS participates in the USDA program to license the [redacted] system that provides centralized configuration management and reporting. ERS has been utilizing the [redacted] system to keep all operating systems patched to avoid critical security vulnerabilities since December of 2003.

Recommendation No. 12 Establish and implement a remote access policy to include controls to establish an accurate list of all modems on its network, ensure that they are properly configured, make sure that they are not used inappropriately to circumvent firewall and other network security measures in place, and update the listing on a periodic basis.

Agency Response By June 1, 2004 ERS plans to complete the inventory of all modems on its network and will develop a policy to specify how and when modems are authorized for connection to the network. There will be an annual review of the configuration and usage of the modems. ERS has been incrementally eliminating the use of modems from its network and will continue with this effort.

Recommendation No. 13 Establish and implement a policy to include controls to conduct routine and timely reviews of firewall configuration.

Agency Response ERS has created a policy for quarterly reviews of the firewall configuration. The review will focus on the adequacy of rules incorporated into the configuration and the elimination of unnecessary rules. The first review was completed during February 2004. The policy includes documenting all of the existing rules and any actions taken during the review.

Recommendation No. 14 Establish and implement formal procedures and controls for periodic reviews of logical and physical access controls to determine if controls are up to date and functioning as designed.

Agency Response By January 1, 2005, ERS will conduct quarterly reviews of its logical and physical access controls to include enforcing existing procedures in notifying security staff when employees or contractors no longer require system access. The procedure will include a review process by the CIO and agency Data Coordinators to judge the adequacy of the process. The review will use the agency's email address book to provide information on current status of employees, their room numbers, and phone numbers.

Recommendation No. 15 Establish and implement internal control procedures to ensure that all computer access lists are updated and routed to ISD, and that ISD is notified and receives a separating employee's checklist when employees terminate their employment.

Agency Response By July 1, 2004, ERS will review the existing procedure for clearing employees as they depart the agency. The review will add requirements for non-federal employees and contractors. The review will focus on creating assurances that policy is being followed and that ISD is receiving proper notification.

Recommendation No. 16 Establish and implement formal access authorization procedures to include controls for periodic review and maintenance of computer access accounts, including review of computer access lists, LAN account policy settings, and access logs.

Agency Response This is similar in nature to Recommendation No. 10. The agency response there should cover this recommendation as well.

Recommendation No. 17 Establish and implement formal physical access control procedures for logging visitor access to the LAN room and tracking the location of backup tapes.

Agency Response ERS has created a logbook to document physical access to the LAN room and has created logs to track the location and movement of backup tapes.