U.S. Department of Agriculture
Office of Inspector General
Southwest Region
Audit Report

SECURITY OVER
NATURAL RESOURCES CONSERVATION SERVICE'S
INFORMATION TECHNOLOGY RESOURCES

Report No.
10099-1-Te
JANUARY 2002

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: February 1, 2002

REPLY TO
ATTN OF: 10099-1-Te

SUBJECT: Security Over NRCS' Information Technology Resources

TO: Pearlie Reed
Chief
Natural Resources Conservation Service

This report presents the results of our audit of the security over the NRCS' information technology resources. The NRCS' response to the official draft report, dated January 10, 2002, is included in exhibit A with excerpts and the Office of Inspector General's position incorporated into the relevant sections of the report.

Management decision has been reached for the recommendations in the report. In accordance with Departmental Regulation 1720-1, final action should be taken within 1 year of each management decision. Correspondence concerning final actions should be addressed to the Office of the Chief Financial Officer, Director, Planning and Accountability Division (OCFO/PAD).

We appreciate the courtesies and cooperation extended to us by members of your staff during the audit.

/s/ Robert W. Young, Jr.
for
RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

SECURITY OVER NATURAL RESOURCES CONSERVATION SERVICE'S INFORMATION TECHNOLOGY RESOURCES

REPORT NO. 10099-1-Te

RESULTS IN BRIEF

Improving the overall management of information technology (IT) resources and the transition to electronic business (e-government) have emerged as top priorities within the United States Department of Agriculture (USDA). We conducted this review of the Natural Resources Conservation Service's (NRCS) IT resources as part of our efforts to examine security over USDA IT resources nationwide. The objectives were to assess: (1) the agency's planning and oversight, (2) the threat of penetration of IT systems, and (3) general and application controls established for physical and logical access.

Overall, NRCS had controls and procedures to ensure that a security management structure existed throughout the agency, authorized users and their access were identified, physical access to sensitive areas was controlled, and authorized users had access to system and data resources. However, NRCS needs improvement in the following areas:

- Oversight over security planning was inadequate. The NRCS had not updated their agency security program to reflect the current status of NRCS' security infrastructure, nor did they ascertain that departmental security policies and procedures were disseminated to all NRCS offices responsible for developing site security plans. These conditions exist because NRCS' Information Systems Security Program Manager (ISSPM) has been busy developing computer security policies and procedures.

- Periodic reviews were not conducted to assess risk and to determine if current security policies remained appropriate. Although NRCS had participated in a risk assessment for administrative IT convergence with Rural Development and Farm Service Agency (FSA), NRCS had not conducted a risk assessment of its IT environments, nor had it conducted periodic security reviews to determine if: (1) security policies remained appropriate, and (2) the agency was in compliance with current security guidelines. NRCS

cited reorganizations, operational backlogs, and insufficient IT staffing as the reasons why periodic reviews were not conducted.

- More emphasis on contingency planning was needed. Three of the four sites we visited [NRCS Information Technology Center (ITC), National Business Management Center (NBMC), and the National Soil Survey Center/National Soil Mechanics Center (NSSC/NSMC)] had not identified their mission-critical components or the resources needed to support operations, nor had they developed contingency plans. NRCS cited insufficient IT staffing as the underlying reason why contingency plans were not developed.

- Periodic assessments of IT platforms to identify and remedy vulnerable conditions were needed. NRCS had not updated their UNIX and Windows NT platforms with the latest security updates, and the security policies established for their Novell IT platforms were not in compliance with governmental and industry standards. NRCS cited insufficient IT staffing as the cause of why systems were not upgraded or reconfigured with the latest security updates and policies.

- Intrusion detection capability was needed. By relying on the department's intrusion detection system, NRCS' security officers do not know that a hacker (through one of its public access servers) is attempting to breach or has breached their systems until they receive notification from the agency's ISSPM. Sometimes these notifications are received several days after the incident. Without intrusion detection capability, for its public access servers, and commercial security tools to combat system vulnerabilities, NRCS networks are vulnerable to intruders.

- Formal access authorization procedures were needed. Managers requested system access by sending e-mail messages or by calling network administrators on the phone. This method of authorizing access does not establish or constitute an acceptable method of authorization. Authorizations for access should have been documented on standard forms and maintained in a manner to permit effective reviews.

- Improvement of controls over unauthorized access to critical or sensitive data was needed. Terminal log-off features should have been established or tools acquired that would automatically log off terminals after a predetermined period of inactivity. Implementing this feature would protect systems and data from unauthorized access.

- Physical access controls were needed at the National Water and Climate Center (NWCC). Formal access controls such as key cards, magnetic card locks, security personnel, remote controlled locks, etc., used singly or in combination, are required for this facility. However, an NWCC official said no physical access controls to prevent access to this facility had been implemented because of their limited budget.

We also issued two management alerts to inform NRCS about the condition of their networks. During our review, we conducted security assessments of NRCS networks that identified over 2,500 network vulnerabilities. Of these, 322 were considered high severity, 528 were medium severity, and 1,705 were low severity. Based on our recommendations, NRCS took immediate action to eliminate these vulnerabilities, obtain scanning software, implement a policy to perform periodic assessments, and implement filtering/firewall to prohibit public access to the NRCS networks.

KEY RECOMMENDATIONS

We recommend that NRCS: (1) update the agency's Information Security Program Plan (ISPP) to reflect current conditions and assist facility personnel in establishing site security plans, (2) distribute copies of all departmental regulations and policies to the centers and institutes, (3) conduct annual security reviews to assess risk and determine if current security policies remain appropriate, (4) develop comprehensive contingency plans for all sites/facilities and train staff in preventing, mitigating, and responding to emergency situations, (5) conduct periodic assessments of IT platforms to identify and remedy vulnerable conditions, (6) acquire and install intrusion detection systems between all NRCS networks and public access servers, (7) ensure that all Novell network policies are consistent at all NRCS locations and meet industry-best practices, (8) implement formal access authorization procedures for granting access to the system and data, (9) instruct security representatives to use password-protected screen savers to prevent unauthorized access through inactive terminals, and (10) instruct security representatives at NWCC to establish physical access controls to protect their facility from unauthorized access during business hours.

AGENCY RESPONSE

The agency's proposed corrective actions are summarized in the recommendation sections of this report, and the agency's complete response to the report is attached as exhibit A.

OIG POSITION

OIG concurs with the management decisions.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The NRCS assists private landowners in protecting their natural resources. The agency emphasizes voluntary, science-based conservation technical assistance, partnerships, incentive-based programs, and cooperative problem solving at the community level. NRCS directs its financial and technical assistance programs to land users through the USDA service centers and through local conservation districts, which are units of State government organized for the purpose of developing and carrying out local conservation programs.

The NRCS relies on computer-based information systems to carry out agency programs, manage its resources, and report program costs and benefits. The advancement of technology has enhanced NRCS' ability to use these systems to share information instantaneously among computers and networks. It also has made the agency more vulnerable to unlawful and destructive penetration and disruptions. Threats range from those posed by insiders and recreational and institutional hackers, to organized crime, espionage, and attacks by intelligence organizations of other countries.

As a result of growing concern over the potential vulnerability of public and private cyber-based information systems, the Administration issued a policy on Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD 63), dated May 22, 1998, to inform the public that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including our cyber systems.

PDD 63 provides guidelines and requires every department and agency of the Federal government to be responsible for protecting its own critical infrastructure, especially its cyber-based information systems. It also states that every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO). The CIAO shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computers and physical systems.

Moreover, the Computer Security Act of 1987 (Public Law 100-235), dated January 8, 1988, and Office of Management and Budget (OMB) Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, dated February 8, 1996, require all Federal agencies (departments) to plan for the security of all sensitive information systems throughout their life cycle.

OBJECTIVES

The overall objectives of this review were to evaluate the adequacy of controls NRCS has established over its IT resources and assess whether the controls function as designed. Specifically, the review was to determine compliance with applicable laws and regulations and to assess: (1) the adequacy of NRCS' security planning and management oversight, (2) the threat of penetration of NRCS' networks, and (3) the adequacy of Federal information system controls established by NRCS.

SCOPE

NRCS was selected as part of a nationwide review of seven agencies with systems that have the greatest impact on USDA's ability to deliver its programs. Our fieldwork was performed during and for the period May 2000 through March 2001.

Audit coverage included NRCS' National Offices in the District of Columbia and Beltsville, Maryland; NRCS ITC in Ft. Collins, Colorado; NBMC in Fort Worth, Texas; NWCC in Portland, Oregon; and NSSC/NSMC in Lincoln, Nebraska. We reviewed controls and procedures established by NRCS for security planning, threat of network penetration, and Federal information systems. We judgmentally selected, for detailed testing, 264 NRCS network components out of the 1,200 Department's network components tested nationwide. The sample was selected based upon location and the request of the agency being tested.

This audit was conducted in accordance with generally accepted government auditing standards.

METHODOLOGY

To accomplish the audit objectives, we relied on documentary, analytical, and testimonial evidence. We compared the controls NRCS had established to protect its IT resources with the requirements of the Computer Security Act of 1987 (Public Law 100-235), dated January 8, 1988, OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, dated February 8, 1996, and various departmental regulations and manuals related to IT security. We also referred to government policies such as

PDD 63. We used commercial, off-the-shelf software products to test NRCS' networks for vulnerable security features in Netware platforms and IT systems operating Transmission Control Protocol/Internet Protocol (TCP/IP).

FINDINGS AND RECOMMENDATIONS

CHAPTER 1 – AGENCY SECURITY PLANNING AND MANAGEMENT OVERSIGHT NEED STRENGTHENING

We found that NRCS' security program was not current and management's oversight over compliance with departmental security policies and procedures was inadequate. We also found that periodic reviews of security controls needed improvement, and more emphasis on contingency planning was needed.

FINDING NO. 1 - OVERSIGHT OVER SECURITY PLANNING WAS INADEQUATE

The NRCS' oversight over security planning, to ensure that departmental guidelines were followed for establishing and implementing security plans, was inadequate. The NRCS had not updated its agency security program to reflect the current status of NRCS' security infrastructure since July 1, 1999, nor did it ensure that departmental security policies and procedures were disseminated to all NRCS offices responsible for developing site security plans. These conditions exist because NRCS' ISSPM had been busy developing computer security policies and procedures. As a result, NRCS had no assurance that the agency security program and site security plans were adequate in defining the degree of protection needed for automated systems supporting their mission.

The Computer Security Act of 1987 (Public Law 100-235), dated January 8, 1988, and Departmental Manual 3140-1, Management ADP Security Manual, dated July 19, 1984, require agencies to establish a plan for the security and privacy of each Federal computer system that contains sensitive information[1]. The security plan is to address employee behavior, training, personnel controls, incident response capability, continuity of support, technical security, and system interconnection.

[1] Sensitive information is any information, the loss, misuse, unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy.

Our review of security program planning at the NRCS National Office disclosed that the agency's information security program plan had not been revised since July 1, 1999. In addition, three of the four sites we visited (NRCS ITC, NBMC, and NSSC/NSMC) had not established site security plans. NRCS cited various reorganizations, operational backlogs, and insufficient staffing of IT personnel as the reasons for lack of compliance oversight.

The NBMC officials said they do not receive any guidance in security or receive any policies and procedures from the National office. NBMC officials said, since 1994, the centers and institutes have been left off the distribution list for departmental regulations and procedures. Although officials said it is getting better, there is still a problem. We validated their statements by reviewing the distribution list and verifying if other centers were not receiving policies and procedures from the National office. For example, two of the four centers we visited did not have a copy of NRCS' National Information Security Handbook, issued January 1, 2000, or a copy of National Bulletin No. 270-0-01, Computer Security Awareness Training Information, issued March 10, 2000.

RECOMMENDATION NO. 1

The NRCS should revise their 1999 ISPP to reflect current conditions. The updated plan should be approved by management and distributed to all IT security coordinators including those at centers and institutes.

NRCS Response

NRCS updated their ISSP in July 2000 to comply with Departmental Regulation and the FY 2000 call letter. A copy of the security plan was distributed to all offices and provided to OIG under separate correspondence.

OIG Position

We agree with the management decision for Recommendation No. 1.

RECOMMENDATION NO. 2

The NRCS should assist facility personnel in establishing site security plans that cover topics prescribed by OMB Circular A-130 and require facilities to conduct periodic assessments of the plans to determine compliance and appropriateness of current policies.

NRCS Response

NRCS is finalizing a Security Handbook that contains specific requirements for site security reviews, risk assessments, and business continuity plans. The handbook contains examples and checklists that all personnel can use to complete these documents. The handbook should be completed in March 2002.

OIG Position

We agree with the management decision for Recommendation No. 2.

RECOMMENDATION NO. 3

The NRCS should distribute copies of all its departmental ADP regulations and policies to the centers and institutes and ensure that all future mail distributions include these facilities.

NRCS Response

NRCS is developing a web site for its security officers. The web site will contain copies of all USDA and NRCS security documents. However, until completion, distribution lists will be updated to ensure that all security officers receive copies of these documents. The web site should be online in March 2002.

OIG Position

We agree with the management decision for Recommendation No. 3.

FINDING NO. 2 - PERIODIC REVIEWS OF SECURITY CONTROLS NEED IMPROVEMENT

Our review disclosed that although NRCS participated in a risk assessment in January 1999 of the administrative IT convergence with the Local Area Network/Wide Area Network/VOICE (LAN/WAN/VOICE) partnership agencies (NRCS, Rural Development, and FSA), it had not conducted a risk assessment of its own IT environments. In addition, NRCS had not conducted an annual security assessment to determine if: (1) security policies remained appropriate, and (2) the agency was in compliance with current security guidelines. NRCS stated that these conditions exist because of reorganizations, operational backlogs, and insufficient IT staffing. Consequently, NRCS had no assurance that its current IT security policies and procedures were functioning at a level acceptable to management.

Departmental Manual 3140-1, Management ADP Security Manual, dated July 19, 1984, and OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, dated February 8, 1996, require agencies to conduct annual security assessments at each Automatic Data Processing (ADP) site. Although Appendix III to OMB Circular No. A-130 no longer requires the preparation of formal risk analyses, the need to determine adequate security will require that a risk-based approach be used.

The NRCS' ISSPM said they have not conducted a security review since his appointment in January 2000 because they have been busy developing computer security policies and procedures. We requested a copy of the latest security review documented at the NRCS National Office. The date on the document indicated that the review was conducted in June 1998.

Moreover, we found that three of the four centers we visited (NRCS ITC, NBMC, and NSSC/NSMC) had not conducted any security assessments to determine if site security was adequate to prevent or detect and recover from security failure. However, we found that since the NWCC was identified as a Departmental Priority System for the Y2K (Year 2000) preparation, NRCS conducted a risk assessment to mitigate risks related to the century date change and power failures of their Climate and Snowpack Telemetry data collection systems.

RECOMMENDATION NO. 4

The NRCS should conduct annual security reviews to assure that management, operational, personnel, and technical controls are functioning effectively.

NRCS Response

NRCS performs security reviews on six to eight field organizations annually. NRCS will continue these reviews for testing security over equipment location, fire, environmental, and administrative controls. All offices are required to report any deficiencies found during this review, and provide updates on corrective action taken. Beginning in FY 2002, NRCS plans to begin annual security reviews at the five major IT organizations that were the subject of this report.

OIG Position

We agree with the management decision for Recommendation No. 4.

FINDING NO. 3 - MORE EMPHASIS ON CONTINGENCY PLANNING NEEDED

Our assessment of service continuity disclosed that NRCS should place more emphasis on contingency planning. For example, three of the four sites we visited (NRCS ITC, NBMC, and NSSC/NSMC) had not identified their mission-critical components or the resources needed to support operations, nor had they developed contingency plans. Consequently, their inability to restore and recover automated services puts the functions of the organizations at risk.

Contingency plans should be developed for restoring critical applications that include arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. The plan 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 the 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.

OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, dated February 8, 1996, requires that agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system.

We also found that two of the sites (NRCS ITC and NBMC) had not taken steps to prevent and minimize potential damage to system applications and data by implementing adequate data backup procedures. For example, at NRCS ITC, backup tapes were not properly safeguarded; they were kept onsite in a locked, non-fireproof cabinet. NRCS ITC officials stated that they did not have funding for off-site storage. At NBMC, logs were not maintained to track backup tapes nor were backup tapes created and stored off-site. An NBMC official stated that their backup system was not working. He said that when their backup system was working, they sent their backup tapes to the National Cartographic and Geospatial Center (NCGC) for off-site storage. However, when we contacted an NCGC official to determine if they were handling off-site storage for NBMC, he told us that they did not maintain any backup tapes for NBMC.

Without contingency planning, NRCS has no assurance that their facilities could continue essential functions if IT support was interrupted.

RECOMMENDATION NO. 5

Comprehensive contingency plans should be developed for all NRCS ADP facilities. Require all facilities to identify their mission-critical operations, data, and supporting resources. The plan should also have provisions for periodic updating and testing.

NRCS Response

NRCS has started the contingency planning process for the major IT centers covered by this report. A meeting for these centers has been scheduled in January 2002, to discuss the requirements for contingency plans and define schedules for their development. For field sites, the NRCS security handbook will provide assistance and guidance on contingency planning. Contingency plans should be completed by August 2002.

OIG Position

We agree with the management decision for Recommendation No. 5.

RECOMMENDATION NO. 6

Provide training to all employees in their roles and responsibilities relative to the emergency, disaster, and contingency plans.

NRCS Response

NRCS is currently revamping all contingency plans. Employees will be briefed once the plans are complete.

OIG Position

We agree with the management decision for Recommendation No. 6.

RECOMMENDATION NO. 7

Instruct all ADP facilities to repair all nonfunctional data backup units, request funding for off-site data storage, and maintain logs to track backup tape location.

NRCS Response

NRCS has resolved this issue with the NBMC.

OIG Position

We agree with the management decision for Recommendation No. 7.

CHAPTER 2– CONTROLS OVER INTERNET/INTRANET SECURITY NEED IMPROVEMENT

We found that NRCS had not conducted periodic security assessments of their IT platforms and had not established an intrusion detection program.

FINDING NO. 4 - PERIODIC SECURITY ASSESSMENT OF INFORMATION TECHNOLOGY PLATFORMS NEEDED

The NRCS had not conducted periodic security assessments of their IT platforms to identify and remedy vulnerable conditions that make their systems susceptible to attack. We conducted a security assessment of NRCS IT platforms and found that NRCS had not upgraded their UNIX and Windows NT platforms with the latest security updates, and the system security policies established for their Novell environments were not in compliance with governmental and industry standards. NRCS cited insufficient IT staffing as the cause of why systems were not upgraded or reconfigured with the latest security updates and policies. Consequently, these conditions increased the exposure of NRCS' networks to unauthorized access and abuse from the Internet.

PDD 63 states that every department and agency of the Federal government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. PDD 63 also requires each sector of the government, which might be a target of infrastructure attack, to conduct an initial vulnerability assessment followed by periodic updates.

We used a commercial, off-the-shelf software product to scan NRCS' Novell Netware platforms located in the District of Columbia; Beltsville, Maryland; and Lincoln, Nebraska, for inconsistencies with security policies used in Netware operating systems. We found over 30 percent of NRCS Netware security standards were not in compliance with industry-best practices.

We also used another commercial, off-the-shelf software product to conduct internal (private access) and external (public access) scans to assess the security of NRCS networks located in Fort Collins, Colorado; Fort Worth, Texas; Portland, Oregon; and Lincoln, Nebraska. The software tests networks for vulnerable security features involving IT platforms operating TCP/IP. The following table lists the total vulnerabilities revealed at each location.

Total Network Vulnerabilities

NETWORK LOCATION	High[2] Risk	Medium Risk	Low Risk	TOTAL
Fort Collins, Colorado	27	122	331	480
Fort Worth, Texas (External Scan)	0	4	26	30
Fort Worth, Texas (Internal Scan)	265	278	905	1,448
Portland, Oregon	5	10	45	60
Lincoln, Nebraska	25	114	398	537
TOTAL	**322**	**528**	**1,705**	**2,555**

Prior to the completion of our review, we alerted NRCS management of the conditions of their networks and recommended immediate action to eliminate the reported vulnerabilities. These vulnerabilities, if left uncorrected, could allow unauthorized users access to critical and sensitive NRCS program and financial data. We met with NRCS officials at these locations to discuss the results of our assessment and the procedures necessary to mitigate the vulnerabilities. They concurred with our findings and reported that many of the vulnerabilities had been corrected.

The following are examples of high-risk vulnerabilities and Novell security features with failed compliant status that were revealed during the scanning process:

- A vulnerability in a file transfer protocol existed which could allow an attacker to execute system commands, modify files, and replace them with virus programs.

[2] High-risk vulnerabilities are those which 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 network data that might be sensitive, but is less likely to lead to a higher-risk exploit.

- A vulnerability in the network security software existed which could allow an intruder to remove or create any file on the computer. This could allow an intruder to gain access to critical/sensitive data.

- A vulnerability existed that could allow local and remote hackers to gain access to systems and execute commands to perform denial-of-service attacks.

- Eighty percent of user objects[3] established for Novell IT platforms did not have intruder detection turned on. Intrusion detection is a critical Novell security feature. Without intrusion detection turned on, critical and sensitive data stored on the file server are exposed to unnecessary risk.

- Twenty percent of user objects allowed more than three bad logins prior to lockout. Allowing an excessive number of bad login attempts could put NRCS' system at risk to hackers attempting to gain access to the network by guessing access codes.

- Twenty-five percent of user objects failed the password requirement test. Password requirement controls are critical. Without this security feature turned on, NRCS networks are vulnerable to intruders who use networks as a means of attacking systems and causing various forms of threat.

In addition, we noted that NRCS' internal network, used by its employees, was not adequately separated from its public access network (i.e., web servers). There was no protection (filtering/firewall) in place that would prevent Internet users accessing NRCS' web servers from accessing NRCS' internal network and obtaining sensitive NRCS information not intended for public access.

RECOMMENDATION NO. 8

Take immediate action to eliminate the vulnerabilities identified in the network assessment report.

NRCS Response

The written response to the first management alert states that the ITC has corrected all vulnerabilities of high and medium severity. ITC will correct low-severity vulnerabilities by upgrading system software. NRCS' response to the second management alert states that all the vulnerabilities for NBMC, South Central Regional Office, NSSC/NSMC have been

[3] User objects are directories in a file system that group related information together; each object represents a user that has access to NRCS' network.

corrected. It also stated that the vulnerabilities at the NCGC would be corrected by November 17, 2000. We contacted NCGC officials and confirmed that all vulnerabilities have been corrected.

OIG Position

We agree with the management decision for Recommendation No. 8.

RECOMMENDATION NO. 9

Obtain scanning software and provide adequate training to personnel related to the operation of the software and correction of vulnerabilities found and implement a policy to perform assessments on a regular basis.

NRCS Response

The written responses to the management alerts stated that NRCS is a partner of the Electronic Access Initiative project. Through this initiative, FSA, NRCS, and Rural Development are purchasing intrusion detection software. Intrusion detection software training is being provided as part of the procurement. We contacted NRCS' ISSPM and confirmed that the intrusion detection software has been purchased. He said they purchased approximately 22,000 licenses for scanning all NRCS sites.

OIG Position

We agree with the management decision for Recommendation No. 9.

RECOMMENDATION NO. 10

Implement a means of filtering/firewall to prohibit public/USDA access to the internal ITC network.

NRCS Response

The written response to the first management alert states that access to the internal ITC network is protected by USDA/Office of the Chief Information Officer (OCIO) firewall. It states that an additional filtering switch/router will be used to protect the internal ITC network against unauthorized traffic. It also states the target switch/router implementation date was to be October 31, 2000. If the switch/router cannot be implemented, a firewall may need to be procured at $35,000 to $50,000. We contacted NRCS' ISSPM to determine if the switch/router was implemented as stated. He said a firewall was installed to protect the internal ITC network.

OIG Position

We agree with the management decision for Recommendation No. 10.

RECOMMENDATION NO. 11

Implement a policy to perform assessments on a regular basis to prevent recurrence of the vulnerabilities identified in the report.

NRCS Response

The written response to the second management alert states that NRCS has formed a partnership with FSA and Rural Development in developing a common policy for scanning systems. It anticipated that the policy would be completed by January 1, 2001. We contacted NRCS' ISSP and confirmed that a common policy has been developed for scanning systems.

OIG Position

We agree with the management decision for Recommendation No. 11.

RECOMMENDATION NO. 12

The NRCS should ensure that all Novell network policies are consistent at all NRCS locations and they meet the National Institute of Standards and Technology requirements.

NRCS Response

NRCS will correct deficiencies noted in their Novell network policies and scan the Novell system in Washington, D.C., to ensure corrections have been made. This process should be completed by March 2002. In long term, this system will be replaced with Windows 2000 – a system compliant with the Common Computing Environment[4] standard.

OIG Position

We agree with the management decision for Recommendation No. 12.

[4]A goal of the USDA Service Center modernization project to provide a Common Computing Environment for Farm Service Agency, Rural Development, and Natural Resource Conservation Service personnel.

RECOMMENDATION NO. 13

NRCS should study the possibility of providing funding for additional IT staffing to address all areas where shortages in IT staffing have a negative impact on security planning and implementation.

NRCS Response

NRCS has received an IT assessment report in which many of their IT components including staff shortages were addressed. Implementing the recommendations of this report should resolve IT staffing issues.

OIG Position

We agree with the management decision for Recommendation No. 13.

FINDING NO. 5 - INTRUSION DETECTION CAPABILITY WAS INADEQUATE

The NRCS had not established an intrusion detection program because they relied on the department's intrusion detection system to protect their network. Furthermore, NRCS' officials said they needed commercial security tools to upgrade their computer systems. Consequently, without adequate security systems, NRCS' network was vulnerable to intruders who use networks as a means of attacking systems and causing various forms of threat.

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, dated February 8, 1996, requires that agencies establish controls to respond to security incidents in a manner that protects their own information and the information of others who might be affected by the incident.

The OCIO at Ft. Collins, Colorado, monitors data traffic over the USDA Intranet backbone to identify any alleged intrusions against the department's IT systems. The OCIO uses monitoring software that prints a list of alleged intrusions each morning. This information is forwarded to the Department's IT security officer who in turn notifies the appropriate agency ISSPM that an intrusion was attempted against one of their IT systems. The agency's ISSPM then notifies the local security officer where the incident occurred. However, NRCS has several public access web servers connected to their network in which data is not transmitted over OCIO's system.

Therefore, without intrusion detection capability, NRCS security officers do not know that a hacker (through one of its public access servers) is attempting to breach or has breached their systems until they receive notification from the agency's ISSPM. If an intrusion occurs on a Friday evening, the security officer of the breached system will be notified Monday – 3 days after the incident.

OCIO notified NSSC that their IT system had been attacked. However, NRCS security representatives at NSSC/NSMC said they had no prior knowledge that their system had been breached. The first incident occurred on March 13, 2000, and a second intrusion incident occurred on April 3, 2000. These incidents disabled NSMC's Internet and e-mail system for over a month.

The monitoring program used by NBMC to detect and subsequently take remedial actions on intrusions or attempted intrusions was inadequate. The NBMC representatives said they downloaded a monitoring utility that detects file placement after the system has been breached. The utility is effective in mounting attacks against files that potentially can damage their systems; however, it does not detect attempted intrusions or set off alarms to notify security personnel that an attempt to breach their system is in progress.

Further, in our review to determine if NRCS' remedial actions for actual intrusions were adequate, we found that on two occasions when NRCS reported intrusion incidents, it did not report taking any actions to prevent repeated intrusions against its networks. The only recourse NRCS' security representatives took was to disconnect their system from the network, recreate and reload critical data, and bring the system back online. The representatives located at the NRCS site where one breach occurred stated on the incident-handling management report that they needed commercial security tools to combat the inherent security weaknesses of Windows NT.

RECOMMENDATION NO. 14

Acquire and install intrusion detection systems between all NRCS networks and public access servers and between all NRCS networks and the USDA Intranet. The intrusion detection system should be capable of detecting, logging, and preventing network intrusions as well as being capable of setting off alarms to notify security personnel that an intruder is attempting to breach the system.

NRCS Response

NRCS is working with security officers to improve the timeliness of reporting incidents that need immediate attention. Steps have also been taken to improve data security by implementing a web farm[5] to control public access and by distributing data to sites that are protected by firewalls, intrusion detection systems, or public key infrastructure. Currently, NRCS is transferring more State web sites to the web farm. All State to web farm transfers should be completed by April 2002.

OIG Position

We agree with the management decision for Recommendation No. 14.

[5] Web farm is a secured web site containing centralized web-based data and applications accessible to employees, customers, and partners.

CHAPTER 3 – LOGICAL AND PHYSICAL ACCESS CONTROLS NEED IMPROVEMENT

We found that logical and physical access controls and controls to prevent unauthorized access to critical/sensitive data were inadequate. Logical and physical access controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment. Logical controls, such as security software programs, prevent or detect unauthorized access to sensitive files. Physical controls limit physical access to computers by securing these resources in locked rooms.

FINDING NO. 6 - LOGICAL ACCESS CONTROLS NEED IMPROVEMENT

Access authorizations were not documented on standard forms and periodically reviewed to determine if they remain appropriate. The NRCS managers used e-mail and verbal communication to request system access for their employees. This method of requesting system access will increase the risk of mishandling, alterations, and misunderstandings. As a result, NRCS had no assurance that the level of access authorizations granted to their users was appropriate for their assigned responsibilities.

The Computer Security Act of 1987 (Public Law 100-235), dated January 8, 1988, and OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, dated February 8 1996, require all Federal agencies (departments) to plan for the security of all sensitive information systems throughout their life cycle.

The system administrator at the NRCS National Office said they log all access authorizations in their Magic Help Desk database. She said supervisors use the e-mail system to request access and her program assistant creates a help ticket in Magic to track the request. However, when we asked the system administrator for a list of access authorizations to determine if access authorizations were appropriate and periodically reviewed, she could not retrieve the authorization data because the Magic Help Desk database was not designed to retrieve data based on predetermined selection criteria.

Computer specialists at NSSC said supervisors discuss a new employee's need for system access with a member of the IT staff. Based on this discussion, a new account is established. Verbal communication is used to request access; no formal documentation is maintained for review.

We also reviewed NRCS' access controls to determine if user access is removed after termination of employment. To conduct this review, we obtained from NRCS' administrative office, information on current employees with network access and information on employees and contractors that were separated in the past 2 years. We compared the current employee information against the separated employee data to determine if user access was removed after termination of employment. Our review identified 10 separated employees and 2 separated contractors listed as having current access to NRCS' network. Six of the separated employees had active logon ID's at NRCS' National Office, two had active accounts at NRCS ITC, one at NWCC, and one at NSSC. The two separated contractors had active logon ID's at NRCS ITC. Formal procedures should be established for notifying the security officer by the agency personnel office of all retirements or other personnel separations.

RECOMMENDATION NO. 15

Implement formal access authorization procedures for granting access to systems and data. A standard form should be used that requires management approval prior to the IT staff granting the request.

NRCS Response

NRCS is finalizing a security handbook that contains specific requirements for logon access. It includes examples of forms to use for documenting access that has been granted or terminated, requirements for management approval when adding or deleting user IDs, and requirements for personnel to follow when requesting and/or acknowledging receipt of their user IDs.

OIG Position

We agree with the management decision for Recommendation No. 15.

RECOMMENDATION NO. 16

To improve access controls, maintain a file containing access authorizations documented on standard forms and approved by senior managers. Periodically reconcile the list of active login ID's against the current, separated, and temporary personnel rosters. Remove active login ID's assigned to separated employees and contractors.

NRCS Response

NRCS is finalizing a security handbook that contains specific requirements for requesting access to local and National computer systems. It also contains example forms to be used for documenting access and removal requests, and requirements for periodic reviews to ensure that only current federal employees and contractors are authorized to access these computer systems.

OIG Position

We agree with the management decision for Recommendation No. 16.

RECOMMENDATION NO. 17

The NRCS should establish a formal procedure requiring: (1) the agency personnel office to notify the security officer of all retirements or other personnel separations, and (2) prior to separation, employees are to check with the systems administrator to have their login accounts removed.

NRCS Response

NRCS is finalizing a security handbook that contains procedures and specific requirements that employees and personnel offices must follow when employee(s) or contractor(s) leave the agency or transfer to another office. Examples of forms were also included for use in documenting this process.

OIG Position

We agree with the management decision for Recommendation No. 17.

FINDING NO. 7 – CONTROLS TO PREVENT UNAUTHORIZED ACCESS TO CRITICAL/SENSITIVE DATA NEED IMPROVEMENT

We found that some of the operating systems used by NRCS were not capable of logging off terminals after a period of inactivity. We also observed that users violated security by displaying access codes. These conditions exist because: (1) NRCS did not enable security features to prevent unauthorized access through inactive terminals, and (2) there were too many access codes for employees to remember. As a result, the risk of unauthorized access was increased.

OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, dated February 8, 1996, requires agencies to plan security controls to assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from National Institute of Standards and Technology.

During our review of logical access controls at NBMC, NSSC/NSMC, and NWCC, we found that NBMC and NWCC computer terminals did not automatically log off after a predetermined period of inactivity, password restrictions at NSSC/NSMC and NWCC were not set to prevent users from reusing any of their last six passwords, NBMC security parameter for maximum password age was set to never expire, and NSSC/NSMC UNIX operating system did not disable login accounts after a predetermined number of failed login attempts. The NBMC IT representative said they would have to purchase some special software to implement automatic terminal log-off controls, and the NWCC representative said their terminals were not set to log off after any period of inactivity.

We also observed employee work areas to determine if logon ID's and passwords were displayed. While conducting a security review at an NRCS office located in Beltsville, Maryland, we identified TCP/IP addresses written on post-it notes and displayed next to terminals at NRCS' Service Center Inter-Operative Lab. Moreover, we identified TCP/IP addresses and system administrator passwords displayed on a marker board located in the NBMC's computer room and identified logon ID's and passwords displayed in three out of the eight work areas we visited at NSSC.

RECOMMENDATION NO. 18

To prevent unauthorized access, NRCS should: (1) practice security measures, such as locking Windows NT workstations or requiring users to use password-protected screen savers, and (2) establish password security policies in compliance with Departmental Manual 3140-1 guidelines.

NRCS Response

NRCS is finalizing a security handbook that contains policies for password security, such as, using password protected screen savers and establishing methods to force users to change their passwords periodically. Beginning in January 2002, NRCS will start replacing all their Windows 9x computers with Windows NT, Windows 2000, and Windows XP systems. These computers support password protected screen savers. All systems should be replaced by September 2002.

OIG Position

We agree with the management decision for Recommendation No. 18.

RECOMMENDATION NO. 19

The NRCS should warn all employees and contractors against the danger of displaying written access codes (logon ID's, passwords, and IP addresses) in the work place.

NRCS Response

NRCS continues to place emphasis on the dangers of posted passwords by sending all employees quarterly security newsletters which address password protection, and by providing this information during security awareness training.

OIG Position

We agree with the management decision for Recommendation No. 19.

FINDING NO. 8 - ADHERENCE TO PHYSICAL ACCESS CONTROLS NEEDS IMPROVEMENT

Our review disclosed that the physical controls established at NWCC and NSSC/NSMC were inadequate. There were no physical controls in place at NWCC to detect or prevent unauthorized access during business hours nor were physical controls adequate at NSSC/NSMC to protect computer equipment from unauthorized access. Further, NWCC has not changed its computer room combination lock since 1995. NWCC official said with their limited budget, they could not afford to implement these controls. Consequently, NWCC and NSSC/NSMC computer facilities and resources are vulnerable to unauthorized access and theft.

NWCC operates a Type II facility. A Type II facility has general-purpose computer(s) which service multiple users concurrently as end processors, i.e., support self-contained processing using resident operating systems, compilers, peripheral devices, etc. Departmental Manual 3140-1.2, Management Agency Security Manual, dated July 19, 1984, requires facilities designated as Type II to establish formal access controls, such as key cards, magnetic card locks, remote controlled locks, security personnel, and closed-circuit television, used singly or in combination, to assure that only authorized personnel enter the facility.

We also identified some additional areas that need improvement during our review of physical access controls at NSSC and NSMC. We observed that NSSC has two servers that are not physically secure. They are located at individuals' desks and not in the computer room. Also, NSMC has a server, used primarily for e-mail and printing, that is not physically secure. It is located in a common area where several lab technicians share desk space.

Moreover, we identified that a janitorial service contracted by GSA cleans NSSC's computer room after office hours when no staff members are present. The NSSC has requested that the janitors clean during office hours; however, since GSA administers the janitorial contract, NSSC has not been able to control the cleaning schedule.

RECOMMENDATION NO. 20

Instruct the NWCC security representatives to develop formalized policies and controls to: (1) detect and prevent unauthorized access to their facilities and resources, and (2) change the combination of the computer room's cipher lock at regular intervals, at least semi-annually or when an employee is terminated or retires.

NRCS Response

NWCC has budgeted funds and held meetings to address facility security. NWCC has also revised their procedure on changing lock combinations to every 90 days and when employees leave. Further, NRCS is strengthening access security by replacing all Windows 9x computers with Windows NT/2000 systems. Employees will be required to use the password protected screen savers provided with these systems to prevent unauthorized access.

OIG Position

We agree with the management decision for Recommendation No. 20.

RECOMMENDATION NO. 21

Instruct NSSC/NSMC to develop a formalized agreement with GSA to have the janitorial service clean their computer room during office hours, and relocate the servers located in common areas to the computer room.

NRCS Response

NSMC/NSSC have secured one server in a rack-mounted locked cabinet and relocated the others to the computer room. Further, to improve security, NSMC/NSSC have changed the lock to their computer room and reached an agreement with janitorial staff for cleaning the computer room during office hours.

OIG Position

We agree with the management decision for Recommendation No. 21.

Response to Inspector General Recommendations
Security over NRCS' Information Technology Resources
October 17, 2001

Finding No. 1 – Oversight over security Planning was Inadequate

Recommendation No. 1 – The NRCS should revise their 1999 ISSP to reflect current conditions. The updated plan should be approved by management and distributed to all IT security coordinators including those at centers and institutes.

NRCS Response:

The NRCS ISSP was updated in July 2000 in accordance with Departmental Regulation and FY 2000 call letter. The document was distributed in sufficient quantity to provide one copy per office. A copy of this document is being provided under separate correspondence.

Recommendation No. 2 – The NRCS should assist facility personnel in establishing site security plans that cover topics prescribed in OMB Circular A-130 and require facilities to conduct periodic assessments of plans to determine compliance and appropriateness of current policies.

NRCS Response:

NRCS is finalizing a Security Handbook. This handbook contains specific requirements for site security reviews as well as risk assessments and business continuity plans that are used to develop the site security plan. The handbook contains examples and checklists that will assist personnel at all levels of the organization in completing these documents. The key elements of the security and risk assessment checklist are administrative controls, security awareness and training, personnel controls, physical protection, telephone key system, software and application protection, and security planning. These documents will be completed on an annual basis and forwarded to the next higher reporting level for review. The key elements of the Business Continuity Plan are responsibilities, backup and recovery actions, and disaster recovery. The handbook should be completed in March 2002. A draft copy will be provided in January 2002 when the final edits are complete.

Recommendation No 3. – The NRCS should distribute copies of all its departmental ADP regulations and policies to the centers and institutes and ensure that all future mail distributions include these facilities.

NRCS Response:

NRCS is in the process of developing a Web site for NRCS security officers. This site will contain copies of all USDA and NRCS security documents. The Information Technology Division is currently working with the Management Services Division to update distribution lists. This site will be completed as part of the NRCS Web modernization and should be online in March 2002.

Finding No. 2 – Periodic Reviews of Security Controls need improvement

Recommendation No. 4 – The NRCS should conduct annual security reviews to assure that management, operational, personnel, and technical controls are functioning effectively.

NRCS Response:

NRCS performs security reviews as part of the ongoing IRM reviews that are performed on six to eight states annually. NRCS plans to continue this process for the field organization. Specific security areas covered during these reviews are location of equipment, fire, environmental, and administrative controls. Any deficiencies found during these reviews are noted in a report, and offices are required to provide updates of actions taken to correct the deficiencies. Beginning in FY 2002, NRCS plans to begin annual reviews on the five major IT organizations that were the subject of this audit report.

Finding No. 3 – More emphasis on Contingency Planning is needed

Recommendation No. 5 – Comprehensive contingency plans should be developed for all NRCS ADP facilities. Require all facilities to identify their mission-critical operations, data, and supporting resources. The plan should also have provisions for periodic updating and testing.

NRCS Response:

NRCS has already begun the process of working on plans for development of contingency plans and continuation of operations plans for the major IT centers covered by this report. In January 2002, NRCS will host a meeting for the five centers to discuss the requirements for the plans and to define schedules for their development. For field sites, the NRCS Security Handbook provides assistance and guidance on contingency planning. Plans should be completed by August 2002.

Recommendation No. 6 – Provide training to all employees in their roles and responsibilities relative to the emergency, disaster, and contingency plans.

NRCS Response:

NRCS is currently revamping all contingency plans, IT continuity of operations plans, and disaster recovery plans. Employees will be briefed once the plans are complete.

Recommendation No. 7 – Instruct all ADP facilities to repair all non-functional data backup units, request funding for off-site data storage, and maintain logs to track backup tape locations.

NRCS Response:

The NRCS security officer has worked with the National Business Management Center staff in Ft. Worth, TX to resolve this issue.

Finding No. 4 – Periodic security assessment of information technology platforms is needed.

Recommendation No. 8 - Take immediate action to eliminate the vulnerabilities identified in the network assessment report:

NRCS Response: (Previously provided and agreed to)

Recommendation No. 9 – Obtain scanning software and provide adequate training to personnel in the use of the software and correction of vulnerabilities found, and implement a policy to perform assessments on a regular basis.

NRCS Response: (Previously provided and agreed to)

Recommendation No. 10 – Implement a means of filtering/firewall to prohibit public/USDA access to internal ITC network.

NRCS Response: (Previously provided and agreed to)

Recommendation No. 11 – Implement a policy to perform assessments on a regular basis to prevent recurrences of the vulnerabilities identified in the report.

NRCS Response: (Previously provided and agreed to)

Recommendation No. 12 – The NRCS should ensure that all Novel network policies are consistent at all NRCS locations and that they meet the National Institute of Standards and Technology requirements.

NRCS Response:

NRCS will correct the stated deficiencies in the Novell system in Washington, D.C. by March 2002. The NRCS security staff will scan the system to ensure corrections have been made. The long-term response to this issue will be to replace the Novell system with a Windows 2000 system compliant with the Common Computing Environment (CCE) standard, however this may not be completed during FY 2002.

Recommendation No. 13 – NRCS should study the possibility of providing funding for additional IT staff to address all areas where shortages in IT staffing have a negative impact on security planning and implementation.

NRCS Response:

NRCS has received the final draft of an Information Technology Assessment that assessed many IT components throughout the agency; IT staffing being one of those. Based upon the implementation of recommendations in this report, staffing issues should be resolved.

Finding No. 5 – Intrusion detection capability was inadequate

Recommendation No. 14 – Acquire and install intrusion detection systems between all NRCS networks and public access servers and between all NRCS networks and the USDA Intranet. The intrusion detection system should be capable of detecting, logging, and preventing network intrusions as well as being capable of setting off alarms to notify security personnel that an intruder is attempting to breach the system.

NRCS Response:

NRCS has been working with the Associate Chief Information Officer for Cyber Security and the National Information Technology Center to ensure timely reporting of incidents needing immediate action. Timeliness of these reports has improved.

NRCS has also taken steps to improve security of NRCS data by implementing a Web Farm and data distribution sites that are protected either by traditional firewall/IDS systems or Public Key Infrastructure (PKI). Public access to NRCS information is being focused at three sites, Fort Collins, Colorado, Fort Worth, Texas, and Portland, Oregon. Fort Collins houses the public Web presence of NRCS and NRCS data. Portland and Fort Worth house specialized data; i.e., climate and geospatial data respectively. Fort Collins and Fort Worth have traditional firewall/IDS systems in place. Portland is piloting a PKI system that should be installed by February 2002.

NRCS has moved 31 state Web sites to the Web Farm, and many more state Web sites will have been moved by December 31, 2001, the end date for the work being accomplished under a Web Modernization contract. All state Web sites should be moved to the Web Farm by April 2002.

Finding No. 6 – Logical assess controls need improvement

Recommendation No. 15 – Implement formal access authorization procedures for granting access to systems and data. A standard form should be used that requires management approval prior to the IT staff granting the request.

NRCS Response:

NRCS is finalizing a Security Handbook. This handbook contains specific requirements for site logon access. The handbook contains example forms to be used for the purpose of documenting the new access and removal actions. Management is required to approve the addition or deletion of any user IDs. The person requesting the action must provide user name and access requirements. In addition, after the user ID is assigned, the employee must acknowledge receipt of the ID and password. The forms are retained consistent with current records management procedures and Departmental Regulations.

Recommendation No. 16 – To improve access controls, maintain a file containing access authorizations documented on standard forms and approved by senior managers. Periodically reconcile the list of active login ID's against the current, separated, and temporary personnel roster. Remove active login ID's assigned to separated employees and contractors.

NRCS Response:

NRCS is finalizing a Security Handbook. This handbook contains specific requirements for requesting access to local, National Finance Center, and National Information Technology Center computers. There is also a requirement for periodic review to ensure that only current federal employees and contractors have this access. The handbook contains example forms to be used for the purpose of documenting access and removal requests. The forms are retained based on current record management procedures.

Recommendation No. 17 – The NRCS should establish a formal procedure requiring: (1) the agency personnel office to notify the security officer of all retirements or other personnel separations and (2) prior to separation, employees are to check with the systems administrator to have their login accounts removed.

NRCS Response:

Item 1 – NRCS has personnel offices in all 50 states that work closely with their appropriate IT staffs to ensure that all user ID's for retired or separated employees are

removed from computer systems. The NRCS Security Handbook contains procedures and forms that offices can adapt to fit their respective needs for these situations.

Item 2 - NRCS is finalizing a Security Handbook. This handbook contains specific requirements for informing IT personnel when a user ID is to be deleted. A form that managers will complete when an employee or contractor leaves the agency or transfers to another office is included in the handbook.

Finding No. 7 – Controls to prevent unauthorized access to critical/sensitive data need improvement

Recommendation No. 18 – To prevent unauthorized access, NRCS should: (1) practice security measures, such as locking Windows NT Workstations or require users to use password-protected screen savers, and (2) establish password security policies in compliance with Departmental Manual 3140-1 guidelines.

NRCS Response:

With the replacement of all Windows 9x computers, NRCS will be using Windows NT, Windows 2000 and Windows XP all of which support password-protected screen savers. The final allotment of CCE computers, which was needed to provide a CCE computer to all NRCS employees, was purchased in September 2001 with delivery scheduled to begin in January 2002. All systems should be delivered by February 2002 and installed by September 2002.

The NRCS Security Handbook, as well as policy from the Common Computing Environment, requires use of these password-protected screen savers. With the implementation Windows 2000 Servers agency-wide, NRCS will require strong passwords (using the 3 of 4 method) which expire every 90 days. Deployment of these servers should be completed by the end of the second quarter of calendar year 2002.

Recommendation No. 19 – The NRCS should warn all employees and contractors against the danger of displaying access codes (logon ID's, passwords and IP addresses) in the work place.

NRCS Response:

NRCS continues to place emphasis on the dangers of posted passwords. The May 2001 quarterly security update, which is sent to all NRCS employees, addressed the specific problem of password protection and included a poster warning against the practice. This information is provided during Security Awareness Training and is required in the Security Handbook. NRCS will continue to place emphasis on this issue in training.

Finding No. 8 – Adherence to physical access controls needs improvement

Recommendation No. 20 – Instruct the NWCC security representative to develop formalized policies and controls to: (1) detect and prevent unauthorized access to their facilities and resources, and (2) change the combination of the computer room's cipher lock at regular intervals, at least semi-annually or when an employee terminates or retires.

NRCS Response:

The National Water and Climate Center (NWCC) has changed the procedures for changing lock combinations. The lock combination is changed every 90 days and when employees leave. The NWCC has budgeted funds to improve building access, and has held discussions with the building manager on possible building alterations. These discussions are ongoing.

Additionally, the CCE program has purchased replacement for all non-WIN NT/2000 systems. With the replacement of all Win 95/98 computers, all users will be required to use password protected screen savers; thus preventing unauthorized users access to a system. These computers were purchased in September 2001 with delivery scheduled to begin in January 2002. All systems should be delivered by February 2002 and installed by March 2002.

Recommendation No. 21 – Instruct NSSC/NSMC to develop a formalized agreement with GSA to have the janitorial service clean their computer rooms during office hours, and relocate the servers located in common areas to the computer room.

NRCS Response:

The NSSC servers have been relocated to the computer room. NSSC has re-keyed the lock to the computer room to ensure access is restricted to authorized personnel. Janitorial staff now cleans the computer room during normal working hours, and they are escorted. The NSMC server is being repositioned as a rack-mounted Windows 2000 server in a locked cabinet. This server will be installed as part of the CCE server deployment that should be completed by July 2002.

ABBREVIATIONS

ADP	Automatic Data Processing
CCE	Common Computing Environment
CIAO	Chief Information Assurance Officer
CIO	Chief Information Officer
FSA	Farm Service Agency
GSA	General Services Administration
ISPP	Information Security Program Plan
ISSPM	Information Systems Security Program Manager
IT	Information Technology
ITC	Information Technology Center
LAN/WAN	Local Area Network/Wide Area Network
NBMC	National Business Management Center
NCGC	National Cartographic Geospatial Center
NRCS	Natural Resources Conservation Service
NSSC/NSMC	National Soil Survey Center/National Soil Mechanics Center
NWCC	National Water and Climate Center
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PDD 63	Presidential Decision Directive 63
TCP/IP	Transmission Control Protocol/Internet Protocol
USDA	United States Department of Agriculture