



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

FOOD AND NUTRITION SERVICE
SECURITY OVER INFORMATION
TECHNOLOGY RESOURCES



Report No.
27099-18-Hy
September 2001



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250



DATE: September 5, 2001

REPLY TO
ATTN OF: 27099-18-Hy

SUBJECT: Food and Nutrition Service
Security Over Information Technology Resources

TO: George A. Braley
Acting Administrator
Food and Nutrition Service

ATTN: Sharon Eldred
Acting Director
Grants Management Division

This report presents the results of the subject audit. Your response to the official draft, dated July 24, 2001, is included as exhibit A with excerpts and the Office of Inspector General's position incorporated into the Findings and Recommendations Section of the report.

Based on information provided, we have reached management decision for all recommendations (Nos. 1 through 26) included in the report. Please follow your internal procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

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

/s/

RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

FOOD AND NUTRITION SERVICE SECURITY OF INFORMATION TECHNOLOGY RESOURCES

AUDIT REPORT NO. 27099-18-HY

RESULTS IN BRIEF

The overall objective of this audit was to assess the threat of penetration of Food and Nutrition Service (FNS) mission critical systems and determine the adequacy of the security over the local and wide area networks. FNS utilizes its computer systems to process, analyze, and support more than \$32 billion in financial and program data on an annual basis.

Our audit of FNS' security over information technology (IT) resources has disclosed serious security vulnerabilities and inadequate controls over access to FNS' computer network and systems. These weaknesses occurred because adequate controls have not always been established and/or implemented and agency management has not placed a priority on or budgeted funds to address Office of Management and Budget (OMB) requirements. These weaknesses indicate a need for a stronger IT security program. As technology has enhanced the ability to share information, it also made it more vulnerable to unlawful and destructive penetration and disruptions. We believe unless corrective actions are timely implemented, FNS is at risk that financial and program data may be compromised.

We identified the following material weaknesses during our audit.

- FNS has systems on its network that have potentially serious security vulnerabilities. Agency officials have not effectively ensured that FNS' operating systems are free from known security vulnerabilities. These vulnerabilities, if left uncorrected, could jeopardize the security of FNS' network and its critical and sensitive financial and program data.
- Adequate physical controls have not been implemented at the facilities reviewed. Door lock controls were not always utilized. As a result, computer resources are vulnerable to unauthorized access.

- User ID and password security, as well as FNS' process for reviewing continuing system access to financial and payment systems, are not always effectively managed to ensure individual accountability. Although our audits have not detected unauthorized access, FNS' security processes and controls may not prevent or detect unauthorized individuals from accessing, modifying, or destroying sensitive financial and program information.
- Weaknesses in logical controls¹ exist in two of FNS' systems. Password features have not always been implemented and the user ID password for one system was not encrypted. FNS officials stated they did not activate these features because of compensating controls (for example, only the system administrator had access to the unencrypted file) and cost considerations. However, these compensating controls do not adequately protect passwords from unauthorized users. Additionally, we observed one individual's log-on ID and user password posted within their workstation. As a result, there is a risk that unauthorized individuals could access these systems, alter data, and not be detected.
- FNS' planning for contingencies need improvement. FNS has not always updated or tested its contingency plans in a timely manner nor did they always correct deficiencies identified in its vulnerability assessments. Agency officials advised this occurred because ITD has not placed a priority on or budgeted funds for contingency planning or established a schedule for updating and testing its contingency plans. As a result, FNS' computer facilities are susceptible to damage or unplanned down time in the event of a disaster or unexpected events.
- FNS has not always adhered to OMB requirements that risk assessments and system certifications² be completed at least every 3 years. Five of nine mission critical systems, which contain critical and sensitive information, have not been assessed within the past 3 years. Additionally, certifications have never been obtained for three systems and re-certification for three other systems are past due. As a result, the vulnerability of threats to the confidentiality and integrity of information, the availability of its systems, and the protection of information resources is substantially increased.
- FNS has not validated that all data for one system are encrypted before transmission to the National Information Technology Center (NITC). This

¹ Logical controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input IDs, passwords, or other identifiers that are linked to predetermined access privileges.

² System certification is the method FNS management uses to provide written agency management authorization that major systems are ready for use. These certifications assure management that operational, personnel, and technical controls are functioning effectively.

occurred because FNS has not conducted reviews to determine whether all States have implemented the encryption software provided to them. As a result, sensitive Privacy Act data may be at risk when sent from States because it may not be encrypted.

- Incompatible duties exist within the ITD. The network LAN administrator, who is a super user³ of the LAN, is also the deputy security officer responsible for maintaining the security over the LAN. As a result, there is increased risk that data could be altered and not be detected.

KEY RECOMMENDATIONS

We recommend that FNS take immediate action to eliminate the high and medium risk vulnerabilities found on its systems and implement the following procedures to improve its security vulnerabilities and inadequate controls.

- Establish procedures for conducting periodic scans at FNS National, regional, and field offices where servers are maintained.
- Establish controls that ensure computer rooms are locked at all times and combinations to locks are changed periodically and after all personnel changes.
- Implement controls to remove log-on IDs and passwords from all FNS systems upon an individual's separation from employment, identify and remove inactive system users from authorization lists, and require supervisory approval for all FNS users of Treasury systems.
- Establish controls to ensure that passwords have a maximum life of 90 days, a minimum length of 6 to 8 characters, and be periodically changed; and require password files be encrypted and personnel protect passwords from disclosure.
- Establish controls to ensure all contingency plans are updated at least annually, to include all operating environment changes and system improvements, and establish a schedule for testing all contingency plans.
- Establish procedures to ensure that risk assessments of all computer systems are conducted every 3 years or whenever a significant modification is made, establish controls for ensuring that system certifications and re-certifications are timely completed, and establish a

³ Super users have access to all data and programs on the LAN.

schedule and expedite the completion of all system certifications and re-certifications.

- Perform reviews of all States to ensure encryption software has been implemented and is being utilized for the transmission of Privacy Act data.
- Delegate the responsibility for data security over the LAN to either the information systems security officer or the deputy information systems security officer.

AGENCY RESPONSE

FNS agreed with the audit recommendations and will implement applicable procedures and controls to improve security over information technology resources.

OIG POSITION

We concur with the proposed management decisions.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
RESULTS IN BRIEF	i
KEY RECOMMENDATIONS	iii
AGENCY RESPONSE	iv
OIG POSITION	iv
INTRODUCTION	1
BACKGROUND	1
OBJECTIVES	4
SCOPE	4
METHODOLOGY	4
FINDINGS AND RECOMMENDATIONS	5
CHAPTER 1	5
VULNERABILITY TESTS DISCLOSED NUMEROUS SECURITY WEAKNESSES ON SYSTEMS IN FNS' NETWORK	5
FINDING NO. 1	5
RECOMMENDATION NO. 1	7
RECOMMENDATION NO. 2	7
RECOMMENDATION NO. 3	8
CHAPTER 2	9
PHYSICAL SECURITY OF COMPUTER FACILITIES NEEDS IMPROVEMENT	9
FINDING NO. 2	9
RECOMMENDATION NO. 4	10
RECOMMENDATION NO. 5	11
CHAPTER 3	12
SYSTEM ACCESS CONTROLS NEED STRENGTHENING	12
FINDING NO. 3	12
RECOMMENDATION NO. 6	15
RECOMMENDATION NO. 7	15
RECOMMENDATION NO. 8	16
FINDING NO. 4	16
RECOMMENDATION NO. 9	18
RECOMMENDATION NO. 10	19
RECOMMENDATION NO. 11	19
RECOMMENDATION NO. 12	19
RECOMMENDATION NO. 13	20
RECOMMENDATION NO. 14	20
FINDING NO. 5	20
RECOMMENDATION NO. 15	22
RECOMMENDATION NO. 16	22

CHAPTER 4	24
CONTINGENCY PLANNING NEEDS IMPROVEMENT	24
FINDING NO. 6	24
RECOMMENDATION NO. 17	26
RECOMMENDATION NO. 18	26
RECOMMENDATION NO. 19	27
FINDING NO. 7	27
FINDING NO. 8	28
RECOMMENDATION NO. 20	30
CHAPTER 5	31
OMB CIRCULAR A-130 REQUIREMENTS NOT ALWAYS MET	31
FINDING NO. 9	31
RECOMMENDATION NO. 21	32
RECOMMENDATION NO. 22	33
FINDING NO. 10	33
RECOMMENDATION NO. 23	35
RECOMMENDATION NO. 24	35
CHAPTER 6	36
PRIVACY ACT DATA NEEDS TO BE ENCRYPTED	36
FINDING NO. 11	36
RECOMMENDATION NO. 25	37
CHAPTER 7	38
INADEQUATE SEPARATION OF DUTIES EXIST WITHIN ITD	38
FINDING NO. 12	38
RECOMMENDATION NO. 26	39
EXHIBIT A – FNS RESPONSE TO DRAFT REPORT	40
ABBREVIATIONS	47

INTRODUCTION

BACKGROUND

The mission of FNS is to provide children and needy families access to a more healthful diet through its food assistance programs and comprehensive nutrition education efforts.

FNS' food assistance programs account for almost half of the U.S. Department of Agriculture's (USDA) budget. Taken together, FNS' programs provide a nutritional safety net for America's low-income families.

FNS is responsible for administering 15 domestic food assistance programs. These include the Food Stamp Program (FSP); Special Nutrition Programs which include the Child Nutrition Programs (CNP) and Special Supplemental Nutrition Program for Women, Infants, and Children; Food Donations Programs; and Nutrition Assistance for Puerto Rico. FNS expended program funds totaling more than \$32 billion in fiscal year (FY) 2000.

FNS programs are administered through its national office and seven regional offices. FNS issues program regulations and provides training and assistance to States. Program benefits are delivered under agreements with State agencies who determine program eligibility and distribute benefits. FNS pays the benefit costs and part of the State administrative expenses for most of its food assistance programs.

Within FNS, the Information Technology Division (ITD) administers the IT program. The five branches of ITD and their responsibilities follow.

- The Systems Administration Branch is responsible for State systems throughout the system's life cycle. Additional responsibilities include operation of the (1) Anti-Fraud Locator Using Electronic Benefits Transfer Retailer Transactions (ALERT) system, (2) systems quality assurance and configuration management program, and (3) database administration.
- The Application Support Branch is responsible for FNS' automated systems and the FNS Internet system.
- The Desktop Services Branch is responsible for FNS infrastructure that includes computer equipment, telecommunications, networks, etc. In addition, Desktop Services Branch responsibilities include assisting users in developing small desktop systems, operating a user help desk, and providing office automation support.

- The Information Services Branch is responsible for the clearance of all agency records and is the FNS Freedom of Information Act point-of-contact.
- The Benefit Redemption Systems Branch (BRSB) is responsible for supporting the food coupon redemption-process of the FSP. This is accomplished through the Store Tracking and Redemption Subsystem (STARS).

FNS has nine information systems that are critical to FNS' mission.

Food Stamp Program Integrated Information System – is a combination of four mainframe sub-systems used to support the administration and monitoring of the FSP, which handles over \$18 billion in appropriated funds on an annual basis. These subsystems are either located at USDA's National Information Technology Center (NITC) in Kansas City, Missouri or at FNS' BRSB in Minneapolis, Minnesota.

- Grantee Reporting Subsystem – uses data gathered through other subsystems to review the performance of each grantee.
- Coupon Requisition and Inventory Management Subsystem - tracks information on the inventory of food coupons and associated accounting activities.
- Disqualified Recipient Subsystem – tracks disqualified food stamp recipients through a nationwide database and conducts computer-matching activities with State agencies.
- STARS - records and monitors FSP food coupon redemption activities, records proven regulatory violations by retailers, and monitors administrative actions associated with enforcement of related penalties.

Special Nutrition Programs Integrated Information System – is a system used to support the administration and monitoring of Special Nutrition Programs' food and administrative funds, which were almost \$13 billion in FY 2000; and to track program participation statistics. This system is located at USDA's NITC.

Food Stamp Quality Control System – is a system used to store case information about a sample of households that participate in the FSP. This system has two components: the mainframe located at NITC which is used for processing all data submitted by States and the PC-based data input/data collection system resident at each State office.

Agency Financial Management System – this system provides accountability for expenditures of Federal funds; and administration of program grants,

operating expenses, and personnel compensation and benefits for FNS staff. This system is located at USDA's NITC.

FNS Regional Office Administered Programs (ROAP) – is a modified version of the Florida CNP payment system that is used to interface with other FNS payment and information systems when FNS performs the role of the State agency. FNS directly administers CNPs where State law prohibits a State from administering an FNS program for certain types of sponsors. There are ROAPs for the National School Lunch, Breakfast and Milk Programs in six States; the Summer Food Service Program in three States; and the Child and Adult Care Food Program in one State. ROAP expenditures totaled more than \$52 million in FY 2000. This system is located at the FNS Mid-Atlantic Regional Office (MARO) in Robbinsville, New Jersey.

ALERT – is a fraud detection decision support system designed to monitor and track authorized electronic retailer transactions between FSP retailers and recipients. The system facilitates management of the retailer portion of the FSP by providing transaction-level information to Federal personnel charged with the responsibility of FSP retailer management and compliance activities. This system is located at the FNS National Office in Alexandria, Virginia.

These systems and subsystems are considered to contain sensitive data as defined by Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, dated February 1996. There are three factors to be used in considering sensitivity level: integrity, availability, and confidentiality. Integrity is a property of a system that permits effective and reliable development and use. Availability requires that information must be available on a timely basis to meet mission requirements. Confidential information requires protection from unauthorized disclosure.

OMB Circular A-123, Management Accountability and Control, dated June 1995, provides guidance on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls. OMB Circular A-130, Security of Federal Automated Information Resources, Appendix III, dated February 9, 1996, provides government-wide direction on information resources management. The National Institute of Standards and Technology (NIST) manual, dated September 1996, addresses generally accepted principles and practices for securing IT systems. NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, dated December 1998, assists agencies in improving protection of information technology resources. USDA

Departmental Manual 3140-1, Automated Data Processing (ADP) Security Policy, dated July 1984, provides standards, guidelines, and procedures for the development and administration of ADP security programs.

FNS has developed two handbooks to assist them in developing an IT security program. FNS Handbook 701, FNS Information Systems Security Policy Handbook, dated October 1996, provides management guidance necessary for maintaining an information systems security program; and FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, dated November 1997, provides step-by-step procedures for implementing an information systems security program.

OBJECTIVES

Our objectives were to: 1) Assess the threat of penetration of FNS payment/data systems, and 2) determine the adequacy of security over the local and wide area networks (LAN/WAN).

SCOPE

The audit was conducted in accordance with generally accepted Government auditing standards. Fieldwork was performed at the FNS National Office in Alexandria, Virginia; MARO, in Robbinsville, New Jersey; and BRSB in Minneapolis, Minnesota. FNS' web servers, in Washington D.C., were evaluated as a part of Office of Inspector General (OIG) audit, Security Over USDA IT Resources Need Improvement, Audit No. 50099-27-FM, dated March 2001. We selected locations to ensure all nine of FNS' mission critical systems were reviewed.

This audit is part of a department-wide audit of IT security. In addition to selected program agencies within USDA, audit work was also conducted at the National Finance Center, NITC, and the Office of Chief Information Officer (OCIO). We reviewed controls over FNS systems located at USDA's NITC as a part of OIG audit, NITC General Controls Review, FY 2000, Audit No. 88099-03-FM.

METHODOLOGY

We conducted our review by gaining an understanding of the computing environment at FNS, assessing agency planning and oversight over Internet/Intranet security, reviewing security over the LANs/WAN, assessing the threat of penetration into FNS sensitive systems and the LANs/WAN, and evaluating Federal information system controls at three computer facilities. We conducted our review through interviews, review of FNS records, and observations. We also applied a software-scanning tool to assess the threat of penetration into FNS' systems.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	VULNERABILITY TESTS DISCLOSED NUMEROUS SECURITY WEAKNESSES ON SYSTEMS IN FNS' NETWORK
------------------	--

FINDING NO. 1

FNS has systems on its network that have potentially serious security vulnerabilities. Agency officials have not effectively ensured that the FNS operating systems⁴ are free from known security vulnerabilities. These vulnerabilities, if left uncorrected, could jeopardize the security of FNS' network and its critical and sensitive financial and program data. FNS systems process, analyze, and support more than \$32 billion in financial and program data on an annual basis.

OMB Circular A-130⁵ requires agencies to implement and maintain an automated information security program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

To conduct our assessment of FNS' network and systems at three FNS locations, we used a commercial off-the-shelf software product which is designed to identify vulnerabilities associated with various operating systems. The software is able to perform over 800⁶ tests for security vulnerabilities on systems that use Transmission Control Protocol/Internet Protocol (TCP/IP).

We conducted our scans on 2 UNIX systems, 84 Windows NT systems, and 23 routers/switches between June 2000 and January 2001. The assessments, which were conducted from both within the FNS network and from a location outside its network, revealed 982 vulnerabilities⁷: 27 high, 243 medium, and 712 low. This included 15 vulnerabilities, 9 medium and 6 low, that could be exploited from outside the FNS network.

⁴ (e.g. UNIX and Windows NT).

⁵ OMB Circular A-130, Security of Federal Automated Information Resources, Appendix III, dated February 9, 1996.

⁶ During our vulnerability scans, we periodically updated our software to include additional discovered vulnerabilities. Not all scans conducted may have checked for the more than 800 vulnerabilities that were known at the time of this audit.

⁷ High-risk vulnerabilities are those that provide unauthorized 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 higher-risk exploitation.

The high and medium risk vulnerabilities, if left uncorrected, could allow unauthorized users access to FNS' network and possibly FNS' critical and sensitive data. The significant number of low vulnerabilities can also be an indicator of poor system administration.

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

- One system was accessible using the inherently insecure file transfer protocol. On this system, a default account name could be used to gain access to the system using this protocol. An attacker could use this vulnerability to fill up the system's hard disk, making it unusable by authorized users, or place a virus or other malicious software that could be executed by a more privileged user.
- A user account on one system had no password assigned to it, leaving it accessible by anyone. Depending on the access privileges on this user account, an attacker could use this vulnerability to access this and other computers on the network.
- One server that was found to have website capabilities was found to have one or more potentially vulnerable scripts. These scripts could be exploited to allow an attacker to execute malicious commands on that server.

During our scan of FNS' systems in its national office, a component of its firewall was not functioning and was down for three weeks, leaving only router filtering to protect its network. FNS officials took immediate action to correct the firewall problem. FNS has advised us that they are taking aggressive actions to correct the vulnerabilities we identified during our scans. FNS officials also stated new servers were installed as of April 2001. FNS recently purchased scanning software and will begin performing periodic scans of its systems and network to determine whether identified vulnerabilities have been corrected and whether any additional vulnerabilities are present.

Periodically, systems need to be updated to incorporate recently released security patches and other software updates. During our visit to the three FNS locations, we noticed that each office was responsible for implementing security patches and configurations for their servers. Under a corporate approach, all servers in all offices would be updated and configured alike. FNS should implement a corporate approach to system configuration. Similar configurations will reduce the amount of individual attention needed when updates or upgrades are needed. At the exit

conference on May 30, 2001, FNS agreed to establish appropriate controls for identifying and eliminating vulnerabilities in its network.

RECOMMENDATION NO. 1

Take immediate action to eliminate the high and medium risk vulnerabilities found on FNS' systems.

Agency Response

All FNS workstations will be upgraded to Microsoft Workstation 2000 Professional by December 31, 2001. This will eliminate the ability of a person without proper credentials from accessing FNS systems. This accounts for the majority of the high and medium risk vulnerabilities discovered. Once Internet Security Systems (ISS) penetration and monitoring software is installed, new penetration studies will be run on all servers and workstations, and any deficiencies will be corrected immediately. Scans will be completed by January 15, 2002 and identified deficiencies will be corrected within 30 days thereafter.

OIG Position

Upgrading to Windows 2002, which requires a password to log onto the workstation, would not correct the weaknesses identified by OIG scans or prohibit someone from accessing FNS systems. However, we concur with management decision because the high and medium risk vulnerabilities identified during OIG scans relate to servers that FNS subsequently replaced. Additionally, FNS plans to conduct scans on its new servers and correct identified deficiencies on all servers and critical devices by February 15, 2002.

RECOMMENDATION NO. 2

Establish procedures for conducting periodic scans at all FNS national, regional and field offices where servers are maintained.

Agency Response

FNS is participating in the Department's global contract for ISS software. By September 30, 2001, ISS will be installed and penetration studies will be made on all devices that are licensed under FNS. An operational Handbook will be published by September 30, 2001, which will include procedures for conducting scans of all devices on a quarterly basis. Additionally, scans of servers and more critical devices will be conducted on a weekly basis beginning by October 31, 2001. Initial scanning will be completed by

January 15, 2002 and identified deficiencies will be corrected on all servers and critical devices by February 15, 2002.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 3

Implement a policy to use a corporate level approach to configuration management.

Agency Response

Desktop Services Branch of the Information Technology Division of FNS established a Configuration Management Team on January 1, 2001. The team's charge is to provide design standards for information technology, such as servers, workstations, software products, and printers. These standards will establish a policy and ensure consistent system configuration agency-wide. All standards are documented in the Desktop Services Branch Handbook. The standards will be completed by October 1, 2001.

OIG Position

We concur with FNS' proposed management decision.

FINDING NO. 2

Adequate physical controls have not been implemented at two of the locations reviewed. This occurred because door lock controls were not always utilized. As a result, computer Resources are vulnerable to unauthorized access.

USDA⁸ defines computer facilities by type. Type I facilities are major computer facilities which are operated by non-agency personnel, service multiple USDA agencies, and have their own specific security policies. The NITC is considered a Type I facility. Type II computer facilities are agency specific facilities, including those that have a LAN or other mission critical system. FNS Handbook 701⁹ defines the FNS National Office, BRSB, and its regional offices as Type II facilities. Type III facilities are office spaces where multifunction workstations and network devices are located.

FNS Handbook 701¹⁰ requires that access to FNS computer systems and data be limited to personnel who have clearance. The handbook also requires that Type II computer facilities be controlled spaces. Only authorized personnel should enter the computer room unescorted and doors should be locked to control access. OMB Circular A-123¹¹ requires that access to resources and records be limited to authorized individuals.

Physical security is a vital part of an information systems security program. Physical security protects computer resources from unauthorized use, damage, theft, or unauthorized access to computer systems. To ensure that controls are in place, we interviewed FNS security and computer room personnel, and observed physical controls to prevent unauthorized access at three locations: FNS National Office, MARO, and BRSB. The computer room at FNS National Office contains the ALERT server, LAN server, and associated hardware and software. The computer room at MARO contains the ROAP server, LAN server, and associated hardware and software. The computer room at BRSB contains the mainframe subsystem STARS, LAN server, and associated hardware and software.

⁸ USDA Departmental Manual 3140-1, ADP Security Policy, dated July 1984.

⁹ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Section 310, dated October 1996.

¹⁰ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Section 300 and Section 312, dated October 1996.

¹¹ OMB Circular A-123, Management Accountability and Control, revised June 21, 1995.

Two of the computer rooms were vulnerable to unauthorized access during the audit. At one location, a door to the computer room was left unlocked, at least once, during our audit. During the initial weeks of our audit we attempted to enter FNS' computer rooms. At one location, no one questioned our presence in the computer room for more than five minutes. We were also able to access, within the office suite, a computer and examine files located on the hard drive without a user ID or password. At another location, the combination to the cipher lock for the computer room's rear entrance was not changed after a contract employee separated from employment in June 2000. FNS does not have procedures for periodically changing the combination of the computer room door lock. After we discussed this issue with FNS personnel in October 2000, the combination was changed. These conditions provide an opportunity for unauthorized personnel to gain access to FNS' computer facilities.

An independent contractor conducted a security review of one of FNS' facilities in April 2000. The independent contractor also reported a lack of security to the office suite. FNS responded that a key card system was being implemented. In May 2001 the building key card system was installed and activated.

FNS needs to establish adequate physical controls to ensure that computer rooms are secured at all times and combination locks are periodically changed. At the exit conference on May 30, 2001, FNS officials stated that they had sent a notice to all employees to keep doors locked in the computer room and agreed to implement other necessary procedures to ensure that adequate physical security controls are implemented, including changing combinations to locks at least quarterly and after an employee leaves the agency.

RECOMMENDATION NO. 4

Establish controls that ensure security officers and computer room personnel keep computer rooms locked at all times.

Agency Response

Established policy already covers this area (See FNS Information Systems Security Policy Handbook 701, section 310 and 312) and in the revised FNS Information Systems Security Policy Handbook 701 (see section 110 Policy). Computer room personnel have been briefed to challenge unescorted visitors to FNS controlled office space. In addition, computer security reminders will be issued at least quarterly, beginning in August 2001, regarding keeping computer rooms doors locked.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 5

Establish procedures to ensure that security officers periodically change combinations to locks and after personnel are separated from employment.

Agency Response

FNS Headquarters and regional facilities are required by FNS Handbook 702 (see section 621) to establish their own procedures regarding physical access. For instance, FNS Headquarters does not utilize combination door locks to secure its computer room. To ensure regional facilities have such procedures, annual facility plans will be reviewed by August 6, 2001, and any shortcomings will be followed up within 60 days. Additionally, site reviews are performed by FNS security staff on a periodic basis to ensure compliance with the annual facility plan.

OIG Position

We concur with FNS' proposed management decision.

FNS has not established adequate controls over access to FNS' computer network and systems or the U.S. Department of the Treasury (Treasury) systems. Active management of system access is critical to ensure that access is limited to authorized users. FNS did not (1) timely remove user access for separated employees, (2) adequately evaluate users to determine continuing need for system access, (3) maintain an updated list of all users by system, (4) implement adequate logical controls to restrict access to data and files, or (5) implement adequate compensating controls for accessing Treasury systems.

We reviewed the management of user access and software parameters for four mission critical systems. We also reviewed the access controls over Treasury systems used by FNS. Our audit did not detect any unauthorized access.

FINDING NO. 3

USER ACCESS CONTROLS WERE NOT ADEQUATE

FNS has not implemented adequate user access controls. FNS did not timely remove mainframe access for separated employees, maintain a list of systems each individual is authorized to access, or adequately review users for continued system access. Agency officials advised this occurred because: (1) ITD

was not always promptly notified when an employee with mainframe access separated from the agency; (2) FNS' databases of LAN and mainframe users were not linked increasing the risk that when LAN access was deleted mainframe access may not be removed; and (3) managers were not always identifying all users with a continued need for access in their annual review. As a result, computer resources are vulnerable to unauthorized access.

OMB Circular A-123¹² requires that policies and procedures used by agencies reasonably ensure reliable and timely information is obtained, maintained, reported and used for decision making. Active management control of log-on IDs is critical to ensure that inactive and unauthorized users are removed. Management controls should provide reasonable assurance that assets are safeguarded against unauthorized use.

FNS Handbook 701¹³ requires the information systems security officer to maintain a master list of all log-on IDs and what systems each individual

¹² OMB Circular A-123, Management Accountability and Control, revised June 21, 1995.

¹³ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Section 302, dated October 1996.

log-on ID is authorized to access. In addition, individual log-on IDs and passwords are to be deleted from all FNS systems when individual users depart FNS.

NIST principles and practices¹⁴ provide a baseline that organizations can use to establish and review their information technology programs. Specifically that user IDs that are inactive on the system for a period of 3 months or another specified period of time should be disabled.

Mainframe Access

We identified five instances where user access was not timely removed from an FNS system after an employee separated from the agency. Although ITD removes LAN access at separation, ITD does not always delete the employee's mainframe access. This occurs because ITD is not always notified of this access and they do not maintain a current listing of users, by system, with mainframe access. In addition, FNS systems are not linked to allow one deletion for all systems, LAN and any mainframe system. Therefore, the user's specific system access would still be accessible by someone using the separated employee's log-on ID and password. Also, there is a risk that the separated employee could log onto a current employee's unattended workstation.

When an employee/contractor separates from FNS the individual's supervisor completes a computer system access document requesting deletion of the individual's access, a final salary report, or an exit interview form. The employee/contractor is debriefed, and the form(s) is provided to the FNS security officer who then suspends the individual's LAN access on the day of separation and deletes the LAN access the next business day. However, if ITD is not notified that the employee has mainframe access to several systems, this access may not be deleted.

Program managers use a system-generated report (e.g. Security2 report) of all users and their functional access to review current system access. We reviewed this report, for one system, as of September 26, 2000, and identified 98 users, including employees and contractors. We compared the report to the available personnel rosters and reports of separation from the agency. We compared the report to the security officer's list of mainframe log-on IDs and a NITC list of inactive mainframe users as of July 10, 2000. We identified one employee who had separated from FNS in May 1998 and four other employees who separated from FNS prior to January 2000, whose mainframe log-on IDs were not deleted until July 2000.

¹⁴ NIST Generally Accepted Principles and Practices for Securing Information Technology Systems manual, Common Security Practice, 3.11, Identification and Authentication, dated September 1996.

Review of Authorized Users

In the analysis of one system's authorized users (98) we identified that managers were not adequately reviewing the list of users for continuing system need. We identified the following:

- 51 users (52 percent) did not have a current mainframe log-on ID, of which 34 were removed by NITC for inactivity;
- 15 users were granted access to this system during the period August 1996 through September 1999 but never accessed the system; and
- 12 users were no longer FNS employees.

As a result of a recent report, OIG Audit No. 88099-01-FM, NITC General Controls Review, FY 1998, dated December 1999, NITC implemented a control to identify and remove mainframe users at NITC who have been inactive after 180 days. FNS is notified of NITC's actions to remove mainframe access, however, FNS has not taken actions to remove inactive users from its systems.

Program managers identify system users and their security levels through a review of the Security2 report or similar report. FNS officials stated that they use this list at least once a year to evaluate the appropriateness of user access. FNS Handbook 701¹⁵ states that managers and supervisors are responsible for determining the need for employees to access a system, but it does not require a periodic review of authorized users. Our analysis shows that the Security2 report is not effectively screened for separated employees or users who no longer have a need for system access, including inactive users.

Recognizing the need to improve system access controls, FNS is interested in developing a centralized database that maintains and utilizes a master list of all current users by system. This system will need to work on both mainframe and client server applications. FNS is evaluating either purchasing a commercial off-the-shelf product or developing a prototype to accomplish this task.

FNS needs to strengthen system access controls by requiring that log-on IDs and passwords be removed for terminated employees and inactive users, and ensure the security officer maintains a master list of all current mainframe users by system. At the exit conference on May 30, 2001, FNS

¹⁵ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Section 270, Non-Information Systems Security Personnel Responsibilities, and Section 309 System Access Security Responsibilities, dated October 1996.

officials agreed to implement necessary procedures to ensure that adequate access controls are implemented.

RECOMMENDATION NO. 6

Implement controls to remove log-on IDs and passwords from all FNS systems when employment terminates.

Agency Response

Human Resources has agreed to issue monthly gains and losses reports to the Security Office beginning in August 2001. The Security Office will use this information to remove log-on IDs and passwords from all FNS systems when employment terminates. The Security Office will send out lists of contractor employees to the Contracting Officer's Representative (COR) in the Agency on a quarterly schedule beginning in September 2001 to verify a current list of contractors.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 7

Establish controls to ensure the security officer maintains and utilizes a master list of current users by system.

Agency Response

FNS will approach this recommendation in two steps. Initially, we are developing a system to capture FNS-674 information in a database. This will provide the capability to track who has access to specific systems. Reports will be available by system and by individual. The information will be updated and maintained by using the monthly gains and losses list from Human Resources and by the quarterly list of active contractors from the CORs. The users will be able to complete an FNS-674 on-line and the data will be captured into the database. We are currently testing the system. We anticipate implementation by December 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 8

Implement procedures that require managers to perform a critical review of system-generated reports of all users and identify and remove log-on IDs and passwords for all users who no longer have a need for access or who have been identified as inactive.

Agency Response

FNS will develop and implement a system to ensure that each System Manager reviews the list of approved users of their system. Log-on IDs and passwords for all users who no longer have a need for access or who have been identified as inactive will then be removed. The lists will be provided to each System Manager semi-annually. We will begin the cycle by October 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

FINDING NO. 4
WEAKNESSES EXIST IN LOGICAL CONTROLS

Weaknesses exist in the logical controls of FNS systems. This occurred because adequate security password features have not been implemented in two systems and the user ID password file for one system was not encrypted. FNS officials stated they did not activate these features because of

compensating controls (for example, only the system administrator had access to the unencrypted file) and cost considerations. However, these compensating controls do not adequately protect passwords from unauthorized users. As a result, there is a risk that unauthorized individuals could access these systems, alter data, and not be detected.

Logical controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user IDs, passwords, or other identifiers that are linked to predetermined access privileges. Logical controls should be designed to restrict legitimate users to the specific systems, programs, and files that they need and prevent others, such as hackers, from entering the system at all.¹⁶

¹⁶ U.S. General Accounting Office, Federal Information System Controls Audit Manual, dated December 1996.

FNS Handbook 701¹⁷ requires users to change passwords at periodic intervals. For Type II facilities, passwords should be changed every 90 days. Paragraph B requires that when passwords are issued, the user should immediately change the password to one known only to the user. FNS Handbook 702¹⁸ requires that passwords be 6 to 8 characters in length and be changed by the user at least every 90 days, except when following requirements of other agency computer centers, such as NITC. FNS Handbook 702 also requires all personnel using FNS information systems to use a password that is known only to them and not divulge or share their password with anyone. NIST principles and practices¹⁹ provide a baseline that organizations can use to establish and review their information technology programs. Specifically, organizations should limit the number of log-on attempts and configure operating systems to lock out a user ID after a set number of failed log-on attempts. NIST principles and practices also state that authentication data (e.g. passwords) should be protected with access controls and one-way encryption to prevent unauthorized individuals, including system administrators, or hackers from obtaining data. Current FNS handbooks do not address encryption. However, FNS is the process of revising FNS Handbook 701, to incorporate encryption requirements that are in accordance with NIST standards.

The most commonly used means of restricting access to data files and software programs is through security software. Security software provides a means of specifying who has access to a system, what types of access are granted, what standards are in place for passwords, and other limitations on access to files and programs.

We tested the logical controls for four mission critical systems and identified the following weaknesses in the security password parameters in two systems.

- One system does not require passwords to be: composed of more than one character, changed after initial log-on, and periodically changed thereafter. Additionally, system password files were not all encrypted. The system software that is used to gain access consists of vendor-supplied and contractor developed software. The password file for the contractor-developed portion is in clear text, which increases the risk that unauthorized internal or external users may access this data and use it for unauthorized purposes.

¹⁷ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Section 302, Log-on and Passwords, paragraph F, dated October 1996.

¹⁸ FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Section 104, Password Standard, dated November 1997.

¹⁹ NIST Generally Accepted Principles and Practices for Securing Information Technology Systems manual, Common Security Practice, 3.11.2, Authentication, dated September 1996.

- Two systems do not have a feature that limits the number of log-on attempts without a valid password. One system allows an unlimited number of password attempts. Another system will allow three invalid passwords before a user is locked out. However, a user can immediately return to the log-on menu and again attempt three passwords before being locked out. A user from this system could attempt to log-on indefinitely.
- Two systems do not have time-out features. As a result, there is a risk that unauthorized personnel can review, modify, or delete system information if a workstation is left unattended.

We also observed computer workstations at all locations reviewed to determine if passwords were displayed. At one location we observed 25 workstations and noted that in one workstation a log-on ID and password was posted next to the employee's computer. In prior fiscal years, except for FY 2000, FNS conducted security awareness training and distributed notices to remind personnel to protect passwords and log-on IDs from disclosure.

FNS needs to implement additional logical controls to ensure that passwords have a minimum length, a maximum life, and are immediately changed during the initial log-on. All password files need to be encrypted to prevent unauthorized access to system files or data and during periodic security awareness training all personnel need to be reminded to protect log-on IDs and passwords from disclosure. Subsequent to the audit fieldwork, FNS implemented controls to require minimum password length, maximum password life, change an initially assigned password, and encrypt password files. At the exit conference on May 30, 2001, FNS officials also agreed to implement other necessary logical controls to correct identified weaknesses.

RECOMMENDATION NO. 9

Modify system controls to require password length of 6 to 8 characters.

Agency Response

The Agency policy requires passwords on all systems, and that the passwords be at least 6 to 8 characters in length. The systems not currently compliant will be compliant by December 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 10

Modify system controls to require a maximum password life of 90 days.

Agency Response

All of our systems are required to have a password that expires every 90 days, except for NFC which requires users to change their passwords every 45, or every 18 days, depending on their access. The systems not currently compliant will be compliant by December 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 11

Modify system controls to require that a user immediately change an assigned password during the initial log-on.

Agency Response

The systems not currently compliant will be compliant by December 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 12

Establish procedures that require password files for all systems be encrypted.

Agency Response

The systems not currently compliant will be compliant by December 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 13

Implement a time-out feature for all critical systems.

Agency Response

All mainframe systems currently have a time-out feature. LAN based systems and client server systems will be protected by the workstation security. All FNS workstations will be upgraded to Microsoft Workstation 2000 Professional by December 31, 2001. All FNS workstations will have implemented screen savers. After a period of inactivity, the workstation will be locked, and only the logged-on user or an administrator can unlock the workstation.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 14

Conduct periodic security awareness training during which personnel are reminded to protect passwords and log-on IDs from disclosure.

Agency Response

It is FNS policy that security awareness training be conducted on a yearly basis. The FNS Security Office plans to conduct training for all employees during the fourth quarter of the fiscal year. Additional security measures are being planned that will require users to sign a statement certifying that they affirm to protect FNS IDs and passwords. This form will be in use by January 1, 2002.

OIG Position

We concur with FNS' proposed management decision.

FINDING NO. 5**IMPROVED ACCESS CONTROLS
ARE NEEDED FOR TREASURY
SYSTEMS**

FNS has not established adequate compensating controls over access to Treasury systems. Although Treasury allows shared IDs and passwords, FNS needs to implement additional controls that require periodic review of the need for, and propriety of, access to Treasury data. Without these additional controls there is an increased risk that

unauthorized access to Treasury data will not be prevented or detected.

USDA agencies are required to comply with the standards in the NIST guide²⁰. This guide recommends the protection of financial transaction systems through proper security. NIST principles and practices²¹ state that it is necessary to have a process for requesting, establishing, and closing user accounts. Organizations should periodically review all users for continued need and determine whether accounts are still active. It further states that an organization should require users to uniquely identify themselves and recommends that passwords be frequently changed.

FNS utilizes five Treasury systems to query and transmit financial data. These systems are used for transmission of payment data to Treasury and query the movement of funds. There is no Privacy Act information contained in these Treasury systems. The data in these systems relate to State organizations and users and are not individual specific. Treasury provides all access instructions and controls the access to these systems.

We tested controls over access for the Treasury systems at three locations and noted the following.

- For one system, ten users at two locations shared two user IDs and passwords. These same user IDs and passwords have not been changed for several years.
- For one system, one user approved their-own access; FNS procedures indicate supervisory approval is required.
- For four systems, user request documentation was not maintained.

Treasury periodically requests the FNS National Office to identify authorized users of Treasury systems at FNS. However, all locations are not contacted when preparing this list. As a result, FNS' controls for ensuring only authorized users have access to Treasury systems are inadequate. All locations are not periodically identifying and reviewing the list of authorized users of Treasury systems for continuing need.

FNS maintains system access request documentation for all FNS systems indefinitely. Requests for access to Treasury systems should be maintained for the same period of time.

FNS stated that Treasury is implementing, in April 2001, an Intranet version of one of its systems. This new system will require individual user IDs and

²⁰ NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, dated December 1998.

²¹ NIST Generally Accepted Principles and Practices for Securing Information Technology Systems manual, Practice 3.5.2, Practice 3.11.1, and Practice 3.11.3, dated September 1996.

passwords, thereby correcting existing problems with shared user IDs and passwords.

FNS needs to establish additional compensating controls over access to Treasury systems. These should include maintaining Treasury system access documentation, and implementing procedures at all locations for the periodic identification and review of all authorized users of Treasury systems. Without these additional controls unauthorized access to Treasury data is at increased risk of not being prevented or detected. At the exit conference on May 30, 2001, FNS officials agreed to implement necessary access controls over Treasury systems. Subsequently, FNS also provided documentation to support supervisory approval for the identified system user who approved their own Treasury access.

RECOMMENDATION NO. 15

Establish procedures to ensure system access request documentation of FNS users for Treasury systems is maintained in the same manner as FNS systems.

Agency Response

The Security Office has an existing policy for controlling access to its systems or Treasury Data. The following controls are in place. The agency has the FNS-674 form, which must be completed for all system access or deletions; no action is taken without the FNS-674 being completed; each system is also assigned an authorizing official, which must sign off on all FNS-674 requests; the FNS-674 must be signed by the requestor's supervisor; and Agency policy also requires periodic reviews of IDs.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 16

Implement procedures at all locations to periodically identify and review the list of authorized users of Treasury systems for continued need.

Agency Response

FNS will develop procedures so that system managers review the list of active IDs on a periodic schedule. See the FNS Responses to Recommendations No. 7 and 8. We anticipate full implementation by December 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

FNS' planning for contingencies need improvement. FNS has not always updated or tested its contingency plans in a timely manner nor were deficiencies identified in its vulnerability assessments always corrected. Experience has demonstrated that testing a contingency plan can significantly improve its viability. Untested plans may create a false sense of ability to recover in a timely manner. As a result, FNS' computer facilities are more susceptible to damage or unplanned down time in the event of a disaster or unexpected events.

FNS Handbook 702²² requires contingency plans for each major FNS information facility. FNS addresses these requirements through a separate contingency plan for each location. In several instances there are multiple contingency plans for different systems at the same location. Agency requirements²³ also state that as part of contingency planning, backup storage and environmental controls should be considered.

FINDING NO. 6

CONTINGENCY PLANS NEED TESTING AND UPDATING

FNS has not always updated or tested its contingency plans in a timely manner. FNS officials advised that this occurred because ITD has not placed a priority on, or budgeted funds for, contingency planning or established a schedule for updating and testing its contingency plans. As a result, FNS has

reduced assurance that it can minimize damage caused by unexpected and undesirable events that impact information system operations.

FNS Handbook 701²⁴ states in part that contingency plans should be tested, reviewed, and updated at least annually, or when a major change in the system occurs. FNS Handbook 702²⁵ states that contingency plans are required at each FNS information system facility to minimize damage caused by unexpected and undesirable events. FNS Handbook 702²⁶ also states that emergency plans should be tested annually, including testing fire fighting, loss control, evacuation, bomb threats, and other emergency procedures to ensure that plans are adequate and workable and to train

²² FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Part 301, Contingency Plans, dated November 1997.

²³ FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Part 315, Steps for Developing Contingency Plans, dated November 1997.

²⁴ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Part 811, Contingency Plans, dated October 1996.

²⁵ FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Part 301, Contingency Plans, dated November 1997.

²⁶ FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Part 316, Testing Contingency Plans, dated November 1997.

personnel. In order to ensure that personnel are fully informed about the system contingency plan, the plan should include the results of testing.

OMB Circular A-130²⁷ requires contingency planning by major system. FNS' mainframe systems are addressed through its national office and BRSB contingency plans. The MARO prepared a contingency plan for its LAN and a separate plan for ROAP, a client server system. A contractor prepared the contingency plan for the ALERT system, a client server system resident at the FNS National Office.

FNS officials stated that it will replace its current Dec AlphaServer 4000 minicomputers with Compaq brand servers by April 1, 2001, in all locations. Upon installation of the servers FNS will need to update its contingency plans to incorporate any necessary changes.

We identified the following about four systems at the three locations reviewed.

- Contingency plans were not updated on an annual basis. Two contingency plans were updated in 1998 and two in 1999. There have been changes in one location's operating environment that have been completed since the plan was developed in 1998. In FY 2000, this location upgraded their communication link by switching from token ring to Ethernet. The location also switched from a shared communication line (with another USDA agency) to a direct connection to NITC. Another plan did not include technological changes that have been made in the system. A third contingency plan listed outdated equipment and an outdated emergency notification list.
- Contingency plans did not always include all the mission critical systems that impact the location's operations including those that reside at NITC or that are addressed by another contingency plan.
- Contingency plans for two systems need to be incorporated into the location's contingency plan. The ability to carry out a system's contingency plan is dependent, in part, on the location's LAN contingency plan.
- Contingency plans were not always tested on an annual basis. Two contingency plans were tested in 1998, and the other two were tested in 1999 and 2000, respectively.

²⁷ OMB Circular A-130, Security of Federal Automated Information Resources, Appendix III, dated February 9, 1996.

- Contingency plans did not include the date and results of prior contingency plan testing.

In April 2000, ITD participated in a contingency planning test at NITC. The test focused on how NITC would respond in case of disaster. FNS also tested its web server at the Washington Service Center in March 2000. However, the results of these tests did not address how FNS would respond to an emergency.

ITD officials stated that program and computer center managers identified their testing needs and ITD developed a schedule for testing contingency plans in 2001. ITD officials also stated that FNS plans to contract, in FY 2002, for updating contingency plans. At the exit conference on May 30, 2001, FNS officials agreed to implement necessary controls over contingency planning.

RECOMMENDATION NO. 17

Establish controls for ensuring contingency plans are tested, reviewed, and updated at least annually, or when a major change in the system occurs.

Agency Response

The Security Manager will review the schedule to ensure that contingency plans are tested, reviewed and updated annually or when a major change occurs. This will occur each July, beginning in July 2002, in conjunction with the submission of the annual cyber security plan submission to OCIO.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 18

Update all contingency plans to include all operating environment changes and system improvements. The plans should include the results of prior contingency tests.

Agency Response

The Agency will include all operating environment changes and system improvements in this year's updated plan. We will also include the results of prior contingency tests where possible. All contingency plans will be updated by May 2002.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 19

For each location, incorporate individual system contingency plans into one plan.

Agency Response

FNS will incorporate individual system contingency plans into each location's contingency plan. The FNS Security Office will review a copy of each location's contingency plan. This will be completed by May 2002.

OIG Position

We concur with FNS' proposed management decision.

FINDING NO. 7

BACKUP STORAGE NEEDS TO BE MOVED FOR ONE COMPUTER FACILITY

The backup storage site for one computer facility is located too close to its primary site. According to FNS officials, the backup storage site is used because it is cost-effective and convenient. FNS did not consider the threat to both the primary and backup sites to be significant enough to relocate the backup site. In case of disaster, location staff may not have

access to the data at the computer center or the backup storage site.

FNS Handbook 702²⁸ states that off-site storage should be in a location that provides safe and secure storage for critical systems, including data files and associated documentation. In selecting an off-site storage location, FNS should consider the natural disasters that provide a threat to the current facility. Potential off-site storage locations include other Federal offices with a secure safe or vault.

Production data for this system and the location's LAN is backed up on storage tapes every night. Additional backups are performed every weekend and every month. On a typical night, boxes of storage tapes are loaded on a hand truck and transported to the backup storage site, a Federal building located across the street from the primary location. We were informed that the backup storage tapes are stored in a walk-in safe.

²⁸ FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Section 315, Part A, Backup Operations, dated November 1997.

An independent contractor completed a vulnerability assessment of this location's computer operations in 1998. The independent contractor also identified that the backup storage site was too close to the primary site. If a disaster or crime would occur in the area, FNS staff may likely not be able to access their computer or their backup sites. As a result, FNS agreed to perform a cost benefit study of alternative sites.

We reviewed FNS' progress toward identifying an alternative site. FNS staff obtained some information on alternative sites, but did not select a site. They explained that the Federal building storage is free and there is significant convenience in its current location. Because FNS must physically transport a significant number of storage tapes to the backup site, FNS staff would prefer to obtain new technology that would allow 40 times more data storage per tape prior to any relocation of the backup site, thereby making an alternative backup storage site more practical. However, FNS does not have this type of storage technology and there are no indications that it will be obtained in the foreseeable future.

There is no standard that requires a specific distance between the primary site and the backup storage site. However, backup storage sites at other FNS locations are several miles from the primary site.

We discussed this issue with the FNS security officer in ITD, who agreed that the backup storage site is too close to the primary site. The security officer stated that a location 20 miles away would be preferable. We recommended a backup site be located outside of the immediate vicinity of the primary facility. With the current site, if there were a natural disaster, a crime scene, or an emergency, both locations would very likely become inaccessible. Effective, June 1, 2001, FNS contracted with an electronic media courier and storage company to store system backup tapes at their site, approximately 12 miles from the FNS location. Therefore, no further recommendation is being made.

FINDING NO. 8

ADEQUATE FIRE SUPPRESSION EQUIPMENT IS LACKING IN ONE COMPUTER FACILITY

One computer facility lacked adequate fire suppression in its computer room. FNS has not addressed the lack of adequate fire suppression equipment in its building lease or how it would handle a fire emergency during off-hours. As a result, FNS is placing personnel, equipment, and property at risk.

FNS Handbook 701²⁹ addresses fire suppression systems. Type II facilities, which include the FNS National Office and FNS Regional Offices, are to have the necessary countermeasures in place to prevent, detect, and suppress fires. Fire suppression in the computer room should include fire extinguishers and automatic fire suppression systems. A pre-action dry pipe system is the more acceptable fire suppression system for Type II facilities.

We toured the location's computer room and found that both the computer room and the office suite lack an overhead fire suppression system. We observed that there were fire extinguishers on hand in the computer room.

FNS performed a vulnerability assessment in 1998, and also identified that the facility lacks a fire suppression system in its computer room and office suite. FNS staff recommended a pre-action dry pipe fire suppression system be installed.

A pre-action dry pipe system does not have water in the immediate overhead pipes. The system is heat activated, therefore, when heat is detected, water is sent to the sprinkler heads and activated. A traditional sprinkler system has water in the overhead pipes. Other FNS computer facilities have either a halon gas fire suppression system or a sprinkler system.

FNS staff responded that they do not have funding to install a fire suppression system. The facility is a leased building and any sprinkler system would require substantial remodeling of the computer room and office suite. Currently, FNS is in the third year of a 5-year lease with another 5-year option.

Fire extinguishers present in the building could address a fire emergency if it occurred during operating hours, between 7 am to 6 pm, Monday through Friday. FNS staff indicated that if a fire occurred during off-hours the local fire department, which is an estimated three miles away, would respond to the fire alarm. The lack of a fire suppression system places unnecessary risk for FNS personnel, property and equipment.

²⁹ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Section 311, Environmental Threats, Part A, Fire, dated October 1996.

RECOMMENDATION NO. 20

Implement a fire suppression system at this location.

Agency Response

The presence of an application server elevates this location to a Type II computer facility. GSA has indicated that they do not require a sprinkler system for buildings less than three floors. However, FNS plans to relocate the application server to another FNS location that already has appropriate fire suppression equipment. We expect to have this move completed by March 2002.

OIG Position

We concur with FNS' proposed management decision.

FNS has not always adhered to OMB requirements that risk assessments and system certifications be completed at least every 3 years. OMB requires agencies to use a risk-based approach that includes consideration of the following major factors in risk management: the value of the system, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. The agency administrator must also certify (system certification) that the system meets OMB, legislative security, and Privacy Act requirements.

FINDING NO. 9

CURRENT RISK ASSESSMENTS ARE NEEDED

FNS has not adhered to OMB circular requirements or its own policies that require risk assessments on its mission critical computer systems. Five of nine mission critical systems, which contain critical and sensitive information, have not been assessed within the past 3 years. FNS officials advised that this

occurred because ITD has not placed a priority on, or budgeted funds for, conducting risk assessments or established a schedule for updating these assessments. As a result, the vulnerability of the systems and its data is substantially increased.

OMB Circular A-130³⁰ defines risk assessment as a formal, systematic approach to assessing the vulnerability of information system assets, identifying threats, quantifying the potential losses from threat realization, and developing countermeasures to eliminate or reduce the threat or amount of potential loss. Risk assessments assist information technology department management to obtain a balance between the impact of risks and the cost of protective measures. Risk assessments should be performed every 3 years, or when there is a change in operations or technology. Further, Presidential Decision Directive (PDD) 63³¹ requires agencies to assess the risks to their networks and establish a plan to mitigate the identified risks.

USDA Departmental Manual 3140³² requires each agency to submit an automated data processing security plan or an annual update to an existing plan by March 31 of each year to the OCIO. As part of the security plan, risk assessment documentation must be included for each agency Type II

³⁰ OMB Circular A-130, Security of Federal Automated Information Resources, Appendix III, dated February 9, 1996.

³¹ PDD 63, Policy on Critical Infrastructure Protection, dated May 22, 1998.

³² USDA Departmental Manual 3140, ADP Security Policy, Section DM 3140-1.1, Part 9, dated July 1984.

facility. The USDA Departmental Manual³³ also requires agency Type II facility's staff to perform risk analyses every 3 years or when an aspect of the computer system undergoes a significant modification.

FNS Handbook 701³⁴ incorporates the risk assessment definition and requirements, and guidance of OMB Circular A-130 and USDA Departmental Manual 3140-1. FNS requires that current risk assessments be reviewed annually and updated as necessary. Less formal assessments are required during the planning and design phases of software system development. All results, whether preliminary or final, must be reviewed by top management for reasonableness, policy adherence, and organizational unity before the implementation of countermeasures.

To determine if risks are periodically assessed, we reviewed FNS' risk assessment policies and identified the personnel who performed and reviewed these assessments. We also reviewed security plans, risk assessments, and conducted interviews with appropriate FNS personnel.

We identified that risk assessments for five of FNS' nine mission critical systems were completed in 1997. Two other systems' risk assessments were completed in 1998, and two in 1999.

Risk assessments are required to be conducted at least every 3 years or when significant changes are made to the computer system. FNS has not established procedures for ensuring that risk assessments are timely completed, including a schedule for conducting these assessments. Because these assessments have not been performed for all FNS critical systems, the vulnerability of threats to the confidentiality and integrity of information, the availability of its systems, and the protection of information resources are substantially increased. At the exit conference on May 30, 2001, FNS officials agreed to implement necessary procedures over risk assessments.

RECOMMENDATION NO. 21

Establish procedures to ensure that risk assessments of all computer systems are conducted every 3 years or whenever a significant modification is made to the system.

Agency Response

FNS will establish a schedule to ensure that risk assessments are conducted on all computer systems every three years, or whenever a

³³ USDA Departmental Manual 3140, ADP Security Policy, Appendix III, Section 3140-1.2, part 10, dated July 1984.

³⁴ FNS Handbook 701, FNS Information Systems Security Policy Handbook, dated October 1996; and FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Chapter 2, dated November 1997.

significant modification is made to the system. For those systems that have not had a risk assessment recently, we will perform risk assessments by May 2002.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 22

Immediately conduct risk assessments for the five mission critical systems that were assessed in 1997.

Agency Response

Two of the systems are in the process of major redesign. Risk assessments will be done on the new systems prior to installation. Risk assessments will be scheduled for the systems as quickly as possible. We will complete the risk assessments by January 2002.

OIG Position

We concur with FNS' proposed management decision.

FINDING NO. 10
SYSTEM CERTIFICATIONS AND
RE-CERTIFICATIONS ARE
NEEDED

System certifications and re-certifications have not been timely completed for six of FNS' nine mission critical systems. Certifications have not been obtained for three systems and the re-certification for three other systems are past due. In addition, FNS has not made substantial progress toward the re-certification of another system that is in the process of major changes.

FNS officials advised that this occurred because the certification and re-certification of these systems was not budgeted or planned. As a result, there is reduced assurance that controls are working properly for these systems.

OMB Circular A-130³⁵ requires that agencies provide a written authorization that major systems are ready for use. FNS accomplishes this through the system certification process. Prior to certification, two considerations must be addressed. A risk assessment must be completed and reviewed; and administrative, physical, and technical safeguards must be reviewed and found sufficient and operational.

³⁵ OMB Circular A-130, Security of Federal Automated Information Resources, Appendix III, dated February 1996.

FNS Handbook 701³⁶ states that information systems security certification is an official statement that approves the security of a major system. Sensitive automated systems require formal certification prior to the system being placed in operation. For sensitive systems, a risk assessment should be completed prior to the system being certified as having adequate technical and physical safeguards for implementation and production. Certification is not permanent. As a system or its security environment changes re-certification is needed to verify that security protection remains applicable. Re-certifications should be conducted for major modifications, changes in the security environment, occurrence of a significant security violation, audit findings, or every 3 years.

FNS Handbook 702³⁷ states that re-certification procedures are the same as certification procedures, except that portions of the process, depending on the reason for the certification may be abbreviated. If a change to the system is the reason for re-certification, the re-certification should focus on the change and how it impacts the security features of the rest of the system. If the re-certification is required due to a lapse of 3 years, then it must include all aspects of the system.

In our review of system certifications we noted the following.

- No system certification was obtained for three systems. These systems were placed in operation in 1981, 1996, and 1998, respectively.
- One system last certified in March 1996, was due for re-certification in March 1999, but it has not been performed. Two other systems last certified in January 1998 were due for re-certification in January 2001.

Additionally, for one system there was a major change in the computing environment. The system switched from the current mainframe environment to a client server in April 2001. As of November 2000, no substantial progress had been made toward the certification of the new system. System certification is a lengthy process and is required to be completed prior to placing the system in operation. ITD staff stated that certification for this system and the re-certification of several other systems, which were due in January 2001, are a priority to complete during FY 2001.

FNS has not established procedures for ensuring that system certifications and re-certifications are timely completed, including a schedule for conducting these certifications. At the exit conference on May 30, 2001,

³⁶ FNS Handbook 701, FNS Information Systems Security Policy Handbook, Part 630, dated October 1996.

³⁷ FNS Handbook 702, FNS Information Systems Security Standards and Procedures Handbook, Part 710, dated November 1997.

FNS officials agreed to implement necessary controls over system certifications and re-certifications.

RECOMMENDATION NO. 23

Establish controls to ensure system certifications and re-certifications are timely completed.

Agency Response

FNS will perform system certification/re-certification in conjunction with the risk assessments and contingency plans discussed in Recommendations 17, 18, 20 and 21. We anticipate completing the certification/re-certification by July 2002.

OIG Position

We concur with FNS' proposed management decision.

RECOMMENDATION NO. 24

Establish a schedule and expedite the completion of all required system certifications and re-certifications.

Agency Response

FNS will establish a schedule by September 30, 2001.

OIG Position

We concur with FNS' proposed management decision.

FINDING NO. 11

FNS has not validated that all data for one system is encrypted before transmission to NITC. This occurred because FNS has not conducted reviews to determine whether all

States have implemented the encryption software provided to them. As a result, sensitive Privacy Act data may be at risk when sent from States because it may not be encrypted.

OMB Circular A-130³⁸ requires Federal agencies to implement and maintain a program to ensure adequate security is provided for all agency information collected, processed, or transmitted in mainframe systems. USDA Departmental Regulation³⁹ states that all sensitive data, subject to Privacy Act considerations must be encrypted before transmission over the Internet.

The Privacy Act of 1974 prohibits disclosure of certain information to the public. This information includes any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, criminal, and certain types of employment history. In addition, the prohibited information includes any item of information containing the following about an individual: individual's name, identifying number or symbol, finger/voice print, or photograph.

We reviewed the security plans for FNS' nine mission critical systems and interviewed ITD personnel to determine whether sensitive data is encrypted prior to transmission over the Internet. We determined that three of FNS mission critical systems contain information or data that is protected from disclosure under the Privacy Act of 1974.

Access to three systems' data is provided via the departmental Intranet from FNS national, regional and field offices to the system mainframe. Data encryption exists for data transmission between the FNS national, regional and field offices, NITC and BRSB. Data encryption also exists for financial data sent between NITC and the National Finance Center and Treasury's financial systems.

Twenty State agencies, who receive almost \$6 billion in program funds, have a dial-up emulator, or connection, to NITC for submitting program

³⁸ OMB Circular A-130, Security of Federal Automated Information Resources, Appendix III, dated February 9, 1996.

³⁹ USDA Departmental Regulation 3140-2, USDA Internet Security Policy, dated March 7, 1995.

participation data. Those States that do not have a dial-up connection submit their data, manually, to FNS Regional Offices for data entry into the program database. All States that have an Internet protocol address to NITC received encryption software from FNS in October 1999. However, ITD did not ensure that these States have implemented and are utilizing the encryption software. ITD staff stated that they would have to review all the States to identify whether they have implemented the software. At the exit conference on May 30, 2001, FNS officials agreed to require regional offices to perform the necessary reviews to ensure encryption software is installed and being used by all applicable States.

RECOMMENDATION NO. 25

Perform reviews of all States to ensure that encryption software has been installed and is being utilized for the transmission of Privacy Act data.

Agency Response

FNS will request that the Regional Deputy Security Officers verify with all their State agencies that they are utilizing the appropriate encryption. Agency policy requires either use of appropriate encryption software or mailing Privacy Act data into the FNS Regional Office. The Regional Deputy Security Officers will report back to the Security Office by December 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

FINDING NO. 12

Incompatible duties exist within the ITD. The network LAN administrator, who is a super user of the LAN⁴⁰, is also the deputy security officer, who is responsible for maintaining the security over the LAN. As a result, there is increased risk that data could be altered and not be detected.

OMB Circular A-123⁴¹ requires specific management control standards, including separation of duties. Key duties and responsibilities in authorizing, recording, and reviewing official agency transactions should be separated among individuals. Management controls developed for agency programs should be logical, applicable, and efficient and effective in accomplishing management objectives. U.S. General Accounting Office Federal Information System Controls Audit Manual⁴² states different individuals should generally perform the following functions: system design, application programming, data security and network administration.

ITD identified the individuals responsible for automated system support. We reviewed computer support functions as identified by ITD and interviewed responsible personnel, as necessary. We identified that a Desktop Services Branch staff person is responsible for network administration. The network administrator is responsible for maintaining a secure and reliable on-line communications network and serves as liaison with user departments to resolve network needs and problems. This same individual is also a deputy security officer who is responsible for the adequacy of security controls over the LAN. This presents a conflict because the individual is a super user of the LAN and has access to all data and programs on the LAN and should not be responsible for controlling security or access to the LAN.

A more appropriate separation of controls over network security would be with the information systems security officer or the deputy information systems security officer. These individuals are responsible for FNS system security and are in charge of controlling access to mainframe systems, contingency planning, security planning, risk assessments, and other similar duties. At the exit conference on May 30, 2001, FNS officials agreed to

⁴⁰ A super user has access to all data and programs on the LAN.

⁴¹ OMB Circular A-123, Management Accountability and Control, revised June 21, 1995.

⁴² U.S. General Accounting Office, Federal Information System Controls Audit Manual, critical element Section SD-1, Segregation Incompatible Duties and Establish Related Policies, dated December 1996.

evaluate the responsibilities within the ITD and ensure adequate separation of duties.

RECOMMENDATION NO. 26

Delegate the responsibility for data security over the LAN to either the information systems security officer or the deputy information systems security officer.

Agency Response

The ITD is in the process of reorganizing. The separation of duties will be addressed during the reorganization. The reorganization will be completed by October 31, 2001.

OIG Position

We concur with FNS' proposed management decision.

EXHIBIT A – FNS RESPONSE TO DRAFT REPORT

Page 1 of 7



**United States
Department of
Agriculture**

**Food and
Nutrition
Service**

**3101 Park
Center Drive**

**Alexandria, VA
22302-1500**

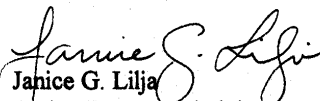
JUL 24 2001

**SUBJECT: Food and Nutrition Service (FNS)
Security Over Information Technology Resources**

**TO: Marlane T. Evans
Regional Inspector General for Audit
Office of the Inspector General**

As requested by your memo 27099-18-Hy of June 20, 2001, my staff has developed the FNS response to your audit recommendations. The response is attached.

I would like to comment on the thoroughness and professionalism of your audit team. This audit will assist FNS in improving the security over our information technology resources.


**Janice G. Lilja
Acting Deputy Administrator
Management**

Attachment

FINDING 1: Vulnerability Tests Disclosed Numerous Security Weaknesses on Systems in FNS' Network

Recommendation No. 1 - Take immediate action to eliminate the high and medium risk vulnerabilities found on FNS' systems.

FNS Response - All FNS workstations will be upgraded to Microsoft Workstation 2000 Professional by December, 31 2001. This will eliminate the ability of a person without proper credentials from accessing FNS systems. This accounts for the majority of the high and medium risk vulnerabilities discovered. FNS is awaiting the receipt of hardware to install ISS penetration and monitoring software. Once installed, new penetration studies will be run on all servers and workstations, and any deficiencies will be corrected immediately. File Transfer Protocol (FTP) is not allowed to be run on FNS systems unless it is protected via security software.

Recommendation No. 2 - Establish procedures for conducting periodic scans at all FNS national, regional and field offices where servers are maintained.

FNS Response - FNS is participating in the Department's global contract for Internet Security Systems software. By September 30, 2001, ISS will be installed and penetration studies will be made on all devices that are licensed under FNS. An operational Handbook will be published by September 30, 2001, which will include procedures for conducting scans of all devices on a quarterly basis. Additionally, scans of servers and more critical devices will be conducted on a weekly basis beginning by October 31, 2001.

Recommendation No. 3 - Implement a policy to use a corporate level approach to configuration management.

FNS Response - Desktop Services Branch of the Information Technology Division of FNS established a Configuration Management Team on January 1, 2001. The Team is made up of IT professionals from Headquarters and from each region. The charge is to provide design standards for information technology, such as servers, workstations, software products, and printers. The Team meets every three weeks. The current emphasis of the Team is Enterprise Computing, and implementing Microsoft's Exchange 2000, Active Directory and Systems Management Server (SMS) concepts. All standards are documented in the Desktop Services Branch Handbook.

FINDING 2: Physical Security of Computer Facilities Needs Improvement

Recommendation No. 4 - Establish controls that ensure security officers and computer room personnel keep computer rooms locked at all times.

FNS Response - Established policy already covers this area (See FNS Information Systems Security Policy Handbook 701 section 310 & 312) and in the Revised FNS Information Systems Security Policy Handbook 701 (see section 110 Policy). Computer room personnel have been briefed to challenge unescorted visitors to FNS controlled office space. In addition, computer

security reminders will be issued at least quarterly, beginning in August 2001, regarding keeping computer rooms doors locked.

Recommendation No. 5 - Establish procedures to ensure that security officers periodically change combinations to locks and after personnel are separated from employment.

FNS Response - FNS Headquarters and regional facilities are required by FNS Handbook 702 (see section 621) to establish their own procedures regarding physical access. For instance, FNS Headquarters does not utilize combination door locks to secure its computer room. To ensure regional facilities have such procedures, annual facility plans will be reviewed, and any shortcomings will be followed up within 60 days.

FINDING 3: User Access Controls were not Adequate.

Recommendation No. 6 - Implement controls to remove log-on Ids and passwords from all FNS systems when employment terminates.

FNS Response - Human resources has agreed to issue monthly gains and losses reports to the Security Office beginning in August 2001. The Security Office will use this information to remove log-on Ids and passwords from all FNS systems when employment terminates.

The Security Office will send out lists of contractor employees to the Contracting Officer's Representative (COR) in the Agency on a quarterly schedule beginning in September 2001 to verify a current list of contractors.

Recommendation No 7 - Establish controls to ensure the security officer maintains and utilizes a master list of current users by system.

FNS Response - FNS will approach this recommendation in two steps. Initially, we are developing a system to capture FNS-674 information in a database. This will provide the capability to track who has access to specific systems. Reports will be available by system and by individual. The information will be updated and maintained by using the monthly gains and losses list from Human Resources and by the quarterly list of active contractors from the CORs. The users will be able to complete an FNS-674 on-line and the data will be captured into the data base. We are currently testing the system. We anticipate implementation by December 31, 2001.

Recommendation No 8 - Implement procedures that require managers to perform a critical review of system-generated reports of all users and identify and remove log-on Ids and passwords for all users who no longer have a need for access or who have been identified as inactive.

FNS Response - FNS will develop and implement a system to ensure that each System Manager reviews the list of approved users of their system. Log-on Ids and passwords for all users who no longer have a need for access or who have been identified as inactive will then be removed. The lists will be provided to each System Manager semi-annually. We will begin the cycle by October 31, 2001.

FINDING 4: Weaknesses Exist in Logical Controls.

Recommendation No. 9 - Modify system controls to require password length of 6 to 8 characters.

FNS Response - The Agency policy requires passwords on all systems, and that the passwords be at least 6 to 8 characters in length. The systems not currently compliant will be compliant by December 31, 2001.

Recommendation No. 10 - Modify system controls to require a maximum password life of ninety days.

FNS Response - All of our systems are required to have a password that expires every 90 days, except for NFC which requires users to change their passwords every 45, or every 18 days, depending on their access. The systems not currently compliant will be compliant by December 31, 2001.

Recommendation No. 11 - Modify system controls to require that a user immediately change an assigned password during the initial log-on.

FNS Response - The systems not currently compliant will be compliant by December 31, 2001.

Recommendation No. 12 - Establish procedures that require password files for all systems be encrypted.

FNS Response - The systems not currently compliant will be compliant by December 31, 2001.

Recommendation No. 13 - Implement a time-out feature for all systems.

FNS Response - All mainframe systems currently have a time-out feature. LAN based systems and client server systems will be protected by the workstation security. All FNS workstations will be upgraded to Microsoft Workstation 2000 Professional by December, 31 2001. All FNS workstations will have implemented screen savers. After a period of inactivity, the workstation will be locked, and only the logged-on user or an administrator can unlock the workstation.

Recommendation No. 14 - Conduct periodic security awareness training during which personnel are reminded to protect passwords and log-on IDs from disclosure.

FNS Response - It is FNS policy that security awareness training be conducted on a yearly basis. The FNS Security Office plans to conduct training for all employees during the fourth quarter of the fiscal year.

FNS has always formally and informally trained users to protect passwords and logon Identifiers (IDs) from disclosure. Users sign a FNS Security Acknowledgment/Certification Acceptance Form where they indicate that they accept their associated security responsibilities for protecting

their ID and passwords when they receive their LAN and mainframe IDs and passwords. Also, periodically, security notices and e-mail messages are sent to users as reminders of their responsibilities. Additional security measures are being planned that will require users to sign a statement certifying that they affirm to protect FNS IDs and passwords. This form will be in use by January 1, 2002.

FINDING 5: Improved Access Controls are Needed for Treasury Systems.

Recommendation No. 15 - Establish procedures to ensure system access request documentation of FNS users for Treasury systems is maintained in the same manner as FNS systems.

FNS Response - The Security Office has an existing policy for controlling access to its systems or Treasury Data. The following controls are in place:

1. The Agency requires that each State Agency have a State Information Security Officer (SISSO) that is responsible for keeping track of IDs for the State, which includes adding, and deleting IDs. As described in Handbook 701, the SISSO is responsible for maintaining the accuracy and usefulness of FNS users IDs and passwords.
2. The State Security Officer is then required to submit the requests to the Deputy Regional Information Systems Security Officer (DRISSO) in their area. The DRISSO then submits the request to the Headquarters Security Office.
3. The Agency has the FNS-674 form, which must be completed for all system access or deletions; no action is taken without the FNS-674 being completed.
4. Each system is also assigned an authorizing official, which must sign off on all FNS-674 requests.
5. The FNS-674 must be signed by the requestor's supervisor.
6. Agency policy also requires periodic reviews of IDs.

Recommendation No. 16 - Implement procedures at all field locations to periodically identify and review the list of authorized users of Treasury systems for continued need.

FNS Response – FNS will develop procedures so that system managers review the list of active IDs on a periodic schedule. See the FNS Responses to Recommendations No. 7 and 8. We anticipate full implementation by December 31, 2001.

FINDING 6: Contingency Plans Need Testing and Updating.

Recommendation No. 17 - Establish controls for ensuring contingency plans are tested, reviewed and updated at least annually or when a major change in the system occurs.

FNS Response - The Security Manager will review the schedule to ensure that contingency plans are tested, reviewed and updated annually or when a major change occurs. This will occur each July, beginning in July 2002, in conjunction with the submission of the annual cyber security plan submission to Office of the Chief Information Officer (OCIO).

Recommendation No. 18 - Update all contingency plans to include all operating environment changes and system improvements. The plans should include the results of prior contingency tests.

FNS Response - The Agency will include all operating environment changes and system improvements in this year's updated plan. We will also include the results of prior contingency tests where possible. While testing at the NITC is conducted annually, plans to test systems at Headquarters were not performed due to inadequate funding. However, funding made available in FY 2001 has been earmarked to help address major changes in FNS Headquarters and application systems at the Benefit Redemption Systems Branch in Minneapolis, MN. All contingency plans will be updated by May 2002.

Recommendation No. 19 - For each location incorporate individual system contingency plans into one plan.

FNS Response - FNS will incorporate individual system contingency plans into each location's contingency plan. The FNS Security Office will review a copy of each location's contingency plan. This will be completed by May 2002.

FINDING 8: Adequate Fire Suppression Equipment is Lacking in One Computer Facility.

Recommendation No. 20 - Implement a fire suppression system at this location.

FNS Response - The presence of an application server elevates this location to a Type II computer facility. GSA has indicated that they do not require a sprinkler system for building less than three floors. FNS plans to relocate the application server to another FNS location that already has appropriate fire suppression equipment. We expect to have this move completed by March 2002.

FINDING 9: Current Risk Assessments are Needed.

Recommendation No. 21 - Establish procedures to ensure that risk assessments of all computer systems are conducted every three years or whenever a significant modification is made to the system.

FNS Response - FNS will establish a schedule to ensure that risk assessments are conducted on all computer systems every three years, or whenever a significant modification is made to the system. For those systems that have not had a risk assessments recently, we will perform risk assessments by May 2002.

Recommendation No. 22 - Immediately conduct risk assessments for the five mission critical systems that were assessed in 1997.

FNS Response – Two of the systems are in the process of major redesign. Risk assessments will be done on the new systems prior to installation. Risk assessments will be scheduled for the systems as quickly as possible. We will complete the risk assessments by January 2002.

FINDING 10: System Certifications and Re-Certifications are Needed.

Recommendation No. 23 - Establish controls to ensure system certifications and re-certifications are timely completed.

FNS Response - FNS will perform system certification/re-certification in conjunction with the risk assessments and contingency plans discussed in Recommendations 17, 18, 20 and 21.

We anticipate completing the certification/re-certification by July 2002.

Recommendation No. 24 - Establish a schedule and expedite the completion of all required system certifications and re-certifications.

FNS Response – FNS will establish a schedule by September 30, 2001.

FINDING 11: Privacy Act Data Needs to be Encrypted

Recommendation No. 25 - Perform reviews of all States to ensure that encryption software has been installed and is being utilized for the transmission of Privacy Act data.

FNS Response – FNS will request that the Regional Deputy Security Officers verify with all their state agencies that they are utilizing the appropriate encryption. The Regional Deputy Security Officers will report back to the Security Office by December 31, 2001.

FINDING 12: Inadequate Separation of Duties Exist Within ITD

Recommendation No. 26 - Delegate the responsibility for data security over the LAN to either the information systems security officer or the deputy information systems security officer.

FNS Response – The Information Technology Division is in the process of reorganizing. The separation of duties will be addressed during the reorganization. The reorganization will be completed by October 31, 2001.

ABBREVIATIONS

ADP	
Automated Data Processing	4
ALERT	
Anti-Fraud Locator Using Electronic Benefits Transfer Retailer Transactions.....	1
BRSB	
Benefit Redemption Systems Branch	2
CNP	
Child Nutrition Programs	1
FNS	
Food and Nutrition Service.....	i
FSP	
Food Stamp Program.....	1
FY	
Fiscal Year.....	1
IT	
Information Technology.....	i
ITD	
Information Technology Division.....	1
LAN/WAN	
Local and Wide Area Networks.....	4
MARO	
Mid-Atlantic Regional Office.....	3
NIST	
National Institute of Standards and Technology.....	3
NITC	
National Information Technology Center	ii
OCIO	
Office of Chief Information Officer.....	4
OIG	
Office of Inspector General	4
OMB	
Office of Management and Budget.....	i

ROAP	
Regional Office Administered Programs.....	3
STARS	
Store Tracking and Redemption Subsystem.....	2
TCP/IP	
Transmission Control Protocol/Internet Protocol.....	5
USDA	
U.S. Department of Agriculture	1