USDA

U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

FISCAL YEAR 2003 NATIONAL FINANCE CENTER REVIEW OF INTERNAL CONTROLS

Report No. 11401-15-FM
November 2003

USDA

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: NOV 19 2003

REPLY TO
ATTN OF: 11401-15-FM

SUBJECT: Fiscal Year 2003 National Finance Center Review of Internal Controls

TO: Edward R. McPherson
Chief Financial Officer
Office of the Chief Financial Officer

This report presents the results of our review of the internal controls at the Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) for fiscal year 2003. The report describes weaknesses in OCFO/NFC's internal control policies and procedures that may be relevant to the internal control structure of OCFO/NFC customer agencies. However, the accuracy and reliability of the data processed by OCFO/NFC and the resultant reports ultimately rests with the customer agency and any accompanying compensating controls implemented by such agency. In addition, the projections of any conclusions based on our audit findings, to future periods are subject to the risk that changes may alter the validity of such conclusions.

Your response to our draft report is included in its entirety in exhibit A. Based on your corrective actions taken prior to report issuance, we have removed some of the original recommendations. For those recommendations where your actions are still pending, we have incorporated excerpts from your response into the findings and recommendations section of the report. Based on the information provided in the response, we have reached management decision for all recommendations. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer.

This report is intended solely for the management of OCFO/NFC, its customer agencies, and their auditors.

Richard D. Long

RICHARD D. LONG
Assistant Inspector General
for Audit

Executive Summary

Review of Internal Control Structure at OCFO/NFC

Results in Brief

We identified weaknesses in the control structure of the Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) that could jeopardize the confidentiality, integrity, and availability of the data it processes. Specifically, OCFO/NFC was not always protecting information from improper access on its mainframe and network systems. While OCFO/NFC had implemented a program to promptly detect attempts by outside individuals to gain unauthorized access, the center was not consistently reviewing access activity on its mainframe or network systems to identify and investigate unusual or suspicious activity once access was obtained. These access control weaknesses existed mainly because certain OCFO/NFC procedures were not adequately designed and/or operating effectively. As a result, OCFO/NFC systems are at an increased risk of inadvertent or deliberate misuse without detection.

Our audit also disclosed that OCFO/NFC had not fully complied with the security management requirements included in the Federal Information Security Management Act and further described in the Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Specifically, OCFO/NFC had not (1) finalized security plans or the underlying risk assessments for its general support systems and major applications or (2) certified and accredited its general support systems. We also found that OCFO/NFC had not performed proper background investigations for its employees as required by other Federal regulations. OCFO/NFC had procedures in place to perform these requirements; however, it was not always following them as prescribed. These activities had recently begun to receive increased emphasis. However, until OCFO/NFC fully complies with Federal requirements, it will not have adequate assurance that effective security controls are established and maintained.

Finally, we found that system software change controls required improvement. OCFO/NFC had not always adequately tested system software changes or evaluated the security impact resulting from system software changes. We also found that OCFO/NFC had not established adequate controls over the configuration of its mainframe operating system. Until OCFO/NFC addresses these issues, it faces increased risk that system software will not be configured and maintained in a manner that affords proper protection to its systems and the sensitive financial and personnel data that is maintained on those systems.

Recommendation In Brief

OCFO/NFC is in the process of implementing significant actions to correct the weaknesses identified in past Office of Inspector General reports. Therefore, we are making no additional recommendations for conditions previously addressed. Other recommendations made in this report include:

- We recommended that OCFO/NFC establish and/or improve current procedures and guidance to prevent and detect unauthorized access to sensitive data and resources on its systems.

- We also recommended that OCFO/NFC finalize security plans and the underlying risk assessments for OCFO/NFC general support systems and major applications and complete revisions to OCFO/NFC's certification and accreditation program to ensure that both application and general support systems are certified.

- In addition, we made recommendations to help ensure that system software changes are sufficiently tested and security impacts associated with these changes to system software are adequately addressed during the system software change control process.

We believe that OCFO/NFC should designate information security weaknesses, as a whole, as material in its Federal Managers' Financial Integrity Act submission until corrected.

Abbreviations Used in This Report

ADP	Automated Data Processing
APF	Authorized Program Facility
DR	Departmental Regulation
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	United States General Accounting Office
HRMS	Human Resources Management Staff
ID	Identification
IRMD	Information Resources Management Division
ISPCS	Information Systems Policy and Control Staff
ISSO	Information System Security Office
IT	Information Technology
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PRI	Periodic Reinvestigation
SP	Special Publication
SVC	Supervisor Call
TCP/IP	Transmission Control Protocol/Internet Protocol
TSP	Thrift Savings Program
USDA	United States Department of Agriculture

Table of Contents

Background and Objectives

Background

The National Finance Center (NFC), which is operated by the U.S. Department of Agriculture's (USDA) Office of the Chief Financial Officer (OCFO) in New Orleans, Louisiana, develops and/or operates administrative and financial systems that support the missions of USDA and its customers. OCFO/NFC is responsible for developing and operating the Payroll/Personnel System, Administrative Billings and Collections System, Centralized Enrollment Reconciliation Clearinghouse System, and Direct Premium Remittance System. OCFO/NFC is also responsible for operating the computers that are used to process USDA's administrative payment systems and corporate financial management system. In fiscal year (FY) 2002, OCFO/NFC processed more than $60 billion in disbursements and collections for USDA and its other customers. Activities performed by OCFO/NFC are financed on a cost-reimbursable basis through the USDA Departmental Working Capital Fund and reimbursable agreements.

OCFO/NFC uses two mainframe computers with the z/OS operating system and other system software[1] to establish and control the environment in which the administrative and financial applications are processed. The center also relies on a nationwide telecommunication network that links computer hardware at remote locations to the OCFO/NFC mainframe computers. Certain financial applications, such as the Purchase Card Management System, are also processed on the network.

Information security has become increasingly important as computer technology has advanced and Federal agencies have become more and more dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Presidential Decision Directive 63, "Policy on Critical Infrastructure Protection," issued May 22, 1998, requires the Government to take all necessary measures to swiftly eliminate any significant vulnerability to either physical or cyber attacks on critical infrastructures[2] and places particular emphasis on information technology (IT) systems. In addition, the E-Government Act (Public Law 107-34), which was signed into law in December 2002, recognizes the importance of information security to the economic and national security interests of the United States. Title III of this Act, entitled the Federal Information Security Management Act (FISMA), requires each

[1] Generally, one set of system software is used to support and control all of the applications that are processed on a particular computer system. System software helps control and coordinate input, processing, output, and data storage associated with all of the applications that run on a computer system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, file maintenance software, security software, data communications systems, and database management systems.

[2] Presidential Decision Directive 63 defines critical infrastructures as those systems that are essential to the minimum operation of the economy and Government, and includes telecommunications, banking and finance, energy, transportation, and other essential Government services.

Federal agency to develop, document, and implement agency-wide information security programs to protect the information and information systems that support the operations and assets of the agency.

In September 1998, the U.S. General Accounting Office (GAO) released a report to the Committee on Government Affairs, U.S. Senate, that noted serious and widespread information security weaknesses that impact the Federal Government's ability to adequately protect Federal assets from fraud and misuse, sensitive information from inappropriate disclosure, and critical operations from disruption.[3] The report noted that individual agencies have not yet done enough to effectively address these problems, including instituting procedures for ensuring that risks are fully understood and implementing controls to mitigate these risks. GAO also issued a report in July 1999 that described serious information system access control weaknesses that rendered sensitive information contained in OCFO/NFC systems, including financial transaction data and personnel information, vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.[4]

To assist auditors in evaluating the effectiveness of information system controls, GAO issued the Federal Information System Controls Audit Manual (FISCAM)[5] in January 1999. This manual describes computer-related controls that auditors should consider when assessing the integrity, confidentiality, and availability of computerized data and includes a methodology for assessing these controls. FISCAM describes six major categories of computer-related general controls that create the environment in which application systems and controls operate.

- Entity-wide security program planning and management controls provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the organization's computer-related controls.

- Access controls are used to limit or detect access to computer resources (data, programs, equipment, and facilities) and, thereby, protect these resources against unauthorized modification, loss, and disclosure.

[3] "INFORMATION SECURITY: Serious Weaknesses Place Critical Federal Operations and Assets at Risk" (GAO/AIMD-98-92, September 1998)

[4] "USDA INFORMATION SECURITY: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure" (GAO/AIMD-99-227, July 1999)

[5] Federal Information System Controls Audit Manual, Volume 1 – "Financial Statement Audits" (GAO/AIMD-12.19.6, January 1999)

- System software controls limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

- Segregation of duties controls include the policies, procedures, and organizational structure established to prevent one individual from controlling key aspects of computer-related operations that could be used to conduct unauthorized actions or gain unauthorized access to assets or records.

- Application software development and change controls prevent unauthorized programs or modifications to existing programs from being implemented.

- Service continuity controls ensure that, when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

Objectives

Our audit objectives were to determine if (1) access and system software controls provided a secure environment for OCFO/NFC application systems and controls, (2) security program planning and management ensured that appropriate information system controls had been established and maintained, (3) segregation of duties controls prevented any one individual from performing incompatible computer-related functions, and (4) service continuity controls provided adequate assurance that critical OCFO/NFC operations would continue or resume promptly in the event of an unexpected disruption.

Findings and Recommendations

Section 1. Controls Over Access Need Strengthening

We found that OCFO/NFC had not established adequate access controls over its mainframe and network systems. These access control weaknesses existed because OCFO/NFC procedures were not always adequately designed and/or operating effectively. Consequently, OCFO/NFC faces increased risk of inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction of the sensitive financial, payroll, and personnel information on its systems, without detection.

Finding 1

Access to Sensitive Production and System Software Resources Was Not Adequately Restricted

We determined that OCFO/NFC was not sufficiently restricting access to sensitive production and system software resources, including production source code, production load libraries, sensitive operating system files, Authorized Program Facility (APF) libraries,[6] and sensitive utility programs.[7] We also found that they were not properly disabling inactive OCFO/NFC user identifications (ID). This occurred because OCFO/NFC did not have suitably designed policies and procedures in place to adequately (1) maintain access profiles that reflected organizational job functions, (2) review access to sensitive operating system files and system software libraries, (3) modify access when employees were reassigned, and (4) identify important system resources that required protection as part of its risk assessment processes. Until these issues are addressed, OCFO/NFC will face increased risk that security controls could be circumvented, either inadvertently or deliberately, to improperly modify or destroy sensitive financial, payroll, or personnel information.

Office of Management and Budget (OMB) Circular A-130[8] stresses the importance of management controls affecting users of IT. These controls help to protect operating systems and other software from unauthorized modification and protect the integrity, availability, and confidentiality of information by restricting the number of users and providing protection from disclosure of information to unauthorized individuals. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, "An

[6] APF is an operating system facility that controls which programs are allowed to use restricted system functions. Programs that reside in APF libraries can be allowed to use restricted system functions that are capable of circumventing all security controls.

[7] Utility programs are generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery).

[8] OMB Circular A-130, Appendix III, Section A, November 30, 2000.

Introduction to Computer Security: The NIST Handbook," recognizes that effective administration of users' computer access is essential to maintaining security. This publication defines user administration to include (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; (3) reviewing user access permissions periodically to ensure conformity with the concept of least privilege and determine if authorizations are up-to-date; and (4) modifying or removing access permissions in a timely manner for employees who are reassigned, promoted, terminated, or who retire. In addition, NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," states that organizations should disable user IDs that have been inactive on the system for a specified period of time (e.g. 3 months).

Access to Sensitive Resources

We obtained listings of OCFO/NFC staff members with access to production source code, production load modules, production batch operational procedures, sensitive operating system files, APF libraries, system logging files, and sensitive utility programs on OCFO/NFC mainframe systems. Our analysis disclosed that over 45 OCFO/NFC personnel had unnecessary access to these resources, except production batch operational procedures and system logging files. OCFO/NFC officials told us that they were in the process of restricting the inappropriate access.

The types of inappropriate access to sensitive production and system software resources that we identified could have been avoided had OCFO/NFC properly (1) maintained access profiles that reflected organizational job functions for the staff members that are involved in developing, operating, maintaining, and securing its IT systems, (2) reviewed staff members with access to sensitive operating system files and system software libraries, (3) modified access when employees were reassigned, and (4) identified important system resources that required protection as part of its risk assessment processes. Risk assessments are discussed further in Section 2 of this report. The remaining issues are discussed below.

USDA's Office of the Chief Information Officer (OCIO) issued guidance on mainframe security standards (CS-011) that states that access profiles for users and resources should be developed based on similar access requirements (e.g., test system, production code maintenance, application access only, etc.). This guidance also requires access to be limited to the least level of privilege needed. OCFO/NFC Information System Security Office (ISSO) officials told us that profiles providing access to the specific data and resources required to perform the functions assigned to different OCFO/NFC organizations had been developed about 10 years ago. OCFO/NFC identified these profiles by the organization number, but they had not properly documented the job functions associated with the profiles and the resources included in the profiles. Currently, OCFO/NFC employees request access to specific datasets and/or resources. ISSO staff members then try to determine if the requested access should be permitted through an established profile or directly to that user's ID. However, this process is unnecessarily cumbersome because the job functions and resources associated with current profiles are not documented. Without additional documentation describing the data and resources included in the profile and which job functions should be assigned these profiles, it is unlikely that access will be granted consistently and effectively in accordance with principle of least privilege. In addition, OCFO/NFC had not established procedures to proactively maintain organizational profiles to ensure that they reflect current job duties.

We also found unnecessary access to APF libraries because current procedures were not effectively identifying inappropriate access to these libraries. ISSO officials told us that they had created security reports to identify users with access to APF libraries. These reports were then used to create access rules that limited update access to these libraries for staff members outside of the Information Resources Management Division's (IRMD) System Engineering Branch and Telecommunications and Office Automation Branch. However, our review disclosed that only subsets of each of these branches needed this level of access. We also identified staff members outside of these two groups who were allowed to update certain APF libraries.

In addition, OCFO/NFC was not always modifying access when employees were reassigned. We obtained a listing of OCFO/NFC reassignments from October 1, 2002, through February 21, 2003. From these reassignments, we identified three staff members from the Government Employee Services Division or IRMD that had been reassigned to a different section, branch, and/or division and reviewed the access permissions for these staff members. Our review disclosed that access for two of these three employees had not been appropriately adjusted to remove access associated with their previous job duties.

OCFO/NFC Management and Administrative Directives Manual, Chapter 11, "Information Systems Management," Directive 40, "Internal Controls for Access to Data and Software (Revision 1)," dated August 28, 2000, states that when an employee transfers from one position to another, the directorate losing the employee is supposed to submit a form canceling that employee's access and the directorate gaining the employee is supposed to submit a request for the new access that the transferring employee needs. While ISSO personnel indicated that they usually receive documentation asking for an expansion of employee access from the gaining directorate, they did not always receive the documentation from the losing directorate asking for the removal of the prior accesses. In addition, ISSO had created a report that identifies OCFO/NFC employees that have been reassigned, but ISSO had not established formal procedures for reviewing this report on a regular basis and following up to ensure that access granted to reassigned employees is adjusted appropriately. Regular use of this report would help to ensure all access remains appropriate when an employee transfers within OCFO/NFC.

The OCFO/NFC agreed that role based security would better serve the center and will work to define the roles and responsibilities of all information technology specialists. They will then create security profiles based on their duties and responsibilities. Below are corrective actions completed by OCFO/NFC prior to the issuance of this report:

- OCFO/NFC developed a listing of sensitive files to be monitored and provided the listing to the Information Systems Policy and Control Staff's (ISPCS) ISSO. ISSO manually produces a daily report showing access to these sensitive files and monitors the activity to ensure only authorized staff members have access to the files. ISSO is currently in the process of automating the reports. Every 6 months, IRMD and ISSO will review the list of sensitive files to determine if the list is accurate and/or needs updating.

- On the first Monday of the every pay period, ISSO now produces a report entitled, "The Tracking Employees Security Access To Mainframes." This report lists all employees transferred in the previous pay period. ISSO sends the report to the Division Security Coordinator of the division losing the transferred employee. A cover memo accompanies the report informing managers to review the listing and to take the necessary action to remove the access of the losing employee.

Inactive User IDs

Finally, we determined that OCFO/NFC had allowed over 450 employee user IDs that had not been used in more than 150 days to remain active on its mainframe systems. This situation existed because ISSO's process to eliminate inactive user IDs was not functioning properly due to a programming error. In addition, ISSO had not established an automated process to ensure that user IDs are suspended before 150 days of inactivity. Allowing inactive IDs to remain available poses needless risk that dormant IDs will be used to gain inappropriate access.

OCFO/NFC recognized the importance of eliminating inactive user IDs and published Title VII, Chapter 11, Directive 46, "Suspension/Deletion of Unused Accessor Identifications," which specifies that user IDs should be suspended after 60 days of inactivity and deleted after 150 days. To implement the guidance established in Title VII, Chapter 11, Directive 46,. ISSO had set up an automated process to delete user IDs after 150 days of inactivity.

We had obtained and analyzed a file of mainframe user IDs to identify user IDs that had not been used in more than 150 days. While the automated process appears to be functioning adequately for external organizations, we determined that more than 17 percent (460 of 2,622) of the user IDs assigned to OCFO/NFC staff members had not been used in more than 150 days as of March 2003. Upon our notification, ISSO determined that a programming error had allowed OCFO/NFC user IDs on the mainframe to remain available despite the fact that they had not been used in more that 150 days. OCFO/NFC officials told us that they had updated the automated process and started deleting inactive IDs assigned to OCFO/NFC staff members and security administrators in July 2003. We also determined that OCFO/NFC processes did not ensure that inactive IDs would be suspended from use prior to 150 days of inactivity.

Subsequent to our fieldwork but prior to report release, OCFO/NFC provided documentation that the following corrective actions had been taken:

- In addition, ISSO modified the automated process to delete inactive user IDs. This process encompasses deletion of all user IDs, including OCFO/NFC users. The process has been properly tested and is operating effectively.

- ISSO also implemented a procedure, which suspends any user ID inactive for a period in excess of 60 days, as stated in Title VII, Chapter 11, Directive 46. As of October 7, 2003, ISSO had suspended 3,472 user IDs.

Therefore, we are not making recommendations to address these issues.

Recommendation No. 1

Implement procedures to document and establish controls to maintain organizational access profiles for internal users involved in developing, operating, maintaining, and securing its IT systems to ensure that these profiles provide access based on current job functions.

Agency Response. OCFO agrees with this recommendation with respect to information technology specialist positions. The Information Resources Management Division (IRMD) is developing a Trusted Facilities Manual (TFM) The TFM will define the roles and responsibilities of all information technology specialists. Once IRMD completes the TFM, the Information Systems Policy and Control Staff's (ISPCS) Information Systems Security

Office (ISSO) will use the defined roles from the TFM to create security profiles associated with each information technology specialist's duties and responsibilities. OCFO/NFC agrees to implement these profiles by June 30, 2004.

OIG Position. We concur with the management decision

Finding 2 Network Access Controls Need Strengthening

We determined that at least 60 modem phone lines did not require a password for access. While OCFO/NFC had established procedures to identify active modem lines, they were not evaluating the security measures in place to ensure that these modem phone lines were properly protected. While we did not attempt to penetrate OCFO/NFC systems, this weakness could allow unsecured access to OCFO/NFC systems. We also found that OCFO/NFC was not always (1) requiring users to change their network passwords or (2) specifying an expiration date for contractor accounts. This occurred because OCFO/NFC could not effectively scan its own network because their network assessment tool was not fully compatible with the version of its network operating system that was implemented in August 2002. Without these controls operating effectively, OCFO/NFC faces the risk of improper access to their sensitive systems and networks.

Remote Access

Active modems provide a gateway into an organization's network by converting digital and analog signals for transmission between components. Departmental Regulation (DR) 3140-1, "USDA Information System Security Policy," Section 16, requires agencies to evaluate security measures in place on network gateways. An unsecured data modem that can be called from a remote location is a potential vulnerability. If the modem or attached computer does not require a password for access and is connected to the OCFO/NFC network, it is a severe threat and the modem should be removed or secured immediately. Modems that can be accessed with either no password or an easily guessed password are vulnerable to computer criminals that call numbers systematically until they find a phone number that connects to an unsecured modem. Firewalls may not protect OCFO/NFC systems against this type of attack because access is obtained through phone lines, which could bypass firewall protection.

To conduct our analysis we used a commercially available software product that was designed to help us identify security risks posed by modems that are unknown to OCFO/NFC and that have not been properly secured. We used this software product to assess security over authorized modem phone numbers provided by OCFO/NFC during May 2003. We also obtained the results of a more complete evaluation of phone numbers performed by OCFO/NFC during the period of May 26 through June 9, 2003.

Our analysis disclosed that 76 of the 6,933 phone numbers evaluated were attached to modems. At least 60 of these 76 modem phone numbers did not require a password for access. OCFO/NFC officials told us that they had not yet established procedures to investigate potentially unsecured modem phone lines identified by their assessments to determine if vulnerabilities existed. Our review also disclosed that OCFO/NFC's database of authorized modem phone lines was not accurate.

In July 2003, OCFO/NFC indicated that the center would expand procedures for assessing phone lines to include steps to ensure that modem phone lines are adequately secured.

Local Area Network Access

We found that OCFO/NFC was not always (1) requiring users to change their passwords or (2) specifying an expiration date for contractor accounts on the network. This occurred because OCFO/NFC could not effectively scan its own network. OCFO/NFC's network assessment tool was not fully compatible with the version of its network operating system that was implemented in August 2002. We also found that OCFO/NFC was not consistently disabling accounts after 150 days of inactivity. This situation existed because OCFO/NFC had not established formal (1) guidelines for how long its internal network user IDs had to remain idle before being considered inactive or (2) procedures for identifying and disabling inactive network user IDs. Not promptly removing inactive IDs from its network increases the risk that unnecessary user IDs will be used to gain unauthorized access.

We used a commercially available software product to conduct a detailed assessment of the security over OCFO/NFC's internal network operating systems. Our assessment software provided a comprehensive analysis of numerous access control settings, such as user account characteristics and password controls. We tested the network operating systems on OCFO/NFC's internal administrative network, which included a review of 16 servers and more than 2,000 user accounts. We immediately communicated the results of our assessment to OCFO/NFC management. We found OCFO/NFC was not always (1) requiring users to change their network passwords or (2) specifying an expiration date for contractor accounts.

Our analysis also identified 13 network accounts that had not been used in more than 150 days but still remained active. Nine of these 13 accounts were contractor accounts that had not been used since March 1999 and one was a test user ID that had not been used since June 2002. NIST SP 800-14.

"Generally Accepted Principles and Practices for Securing Information Technology Systems," states that organizations should disable user IDs that have been inactive on the system for a specified period of time (e.g. 3 months). The OCFO/NFC network security policy requires monthly reviews of user ID inactivity. However, OCFO/NFC had not formally documented how long a network user ID had to remain idle to be considered inactive or procedures for identifying and disabling inactive network IDs. OCFO/NFC officials told us that network user IDs are disabled after 150 days of inactivity. Given the nature of OCFO/NFC's internal network, we believe that the center should modify its procedures to ensure that user IDs are suspended after no more than 90 days of inactivity, as suggested by NIST guidance.

OCFO/NFC officials investigated the accounts that had not been used in more than 150 days and deleted one of these inactive accounts that was no longer needed. OCFO/NFC told us that the remaining accounts are still required. Even so, these inactive accounts should have been disabled to prevent their use until needed.

These weaknesses could have been avoided had OCFO/NFC adequately considered security impacts when it upgraded its network operating system in August 2002. While OCFO/NFC had the same software package that we used to conduct our assessment, it did not upgrade its assessment software to ensure full compatibility with its new network operating system. OCFO/NFC implemented a newer version of its assessment software in February 2003. OCFO/NFC officials told us that, while some network monitoring was performed during this period, this monitoring was limited and more cumbersome without the full use of its assessment tool.[9]

As a result of our audit, ISSO implemented a monthly reporting process that selects all user accounts that have been inactive for 90, 120, and 150+ days. OCFO/NFC told us they are now disabling and/or deleting inactive user IDs according to the specific timeframes. These reports run parallel to the mainframe-automated process that reports inactive accounts on that platform. On August 4, 2003, all 16 contractor accounts were corrected to specify an expiration date. Consequently, we are not making any recommendations to address these issues.

Recommendation No. 2

Expand and formalize procedures and controls to ensure that all modems are identified, tracked, periodically reviewed, and properly secured.

[9] Our review of system software change controls is discussed in more detail in Section 5. Consequently, we are not making any recommendations relating to system software change control in this section.

Agency Response. OCFO agrees with this recommendation. ISPCS revised existing procedures and issued the procedures as of October 15, 2003, to ensure that all modems are identified, properly secured, and periodically reviewed.

OIG Position. We concur with the management decision.

Finding 3

Network Security Vulnerabilities Existed Despite OCFO/NFC Assessments

Our vulnerability assessments disclosed weaknesses in OCFO/NFC network system administration. We identified 10 high-risk and 57 medium-risk vulnerabilities on OCFO/NFC's internal network that required either correction or further investigation. While OCFO/NFC had established procedures to routinely perform its own vulnerability assessments and was aware of most of the vulnerabilities we found, OCFO/NFC had not ensured that all vulnerabilities were corrected in a timely manner. As a result, OCFO/NFC faces increased risk of internal attacks that could jeopardize the integrity and reliability of its data. Further, unauthorized external users could also exploit vulnerabilities on OCFO/NFC's internal network if firewall or other network gateway protections are compromised.

OMB Circular A-130, Appendix III requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce the threat or amount of potential loss. In addition, USDA DR 3140, dated May 15, 1996, establishes policies to ensure comprehensive security programs are in place to safeguard all IT resources. USDA managers must ensure security is in place to protect against accidental or deliberate alteration, destruction, delay, theft, or access to systems, data, applications, equipment, and telecommunications. In August 2001, OCFO/NFC issued Title VII, Chapter 11, Directive 80, "Network Vulnerability Self-Assessment," which establishes procedures for routinely identifying, analyzing, and resolving network vulnerabilities. The 2003 Computer Security Institute/Federal Bureau of Investigations Computer Crime and Security Survey reported that insider abuse of network access was the second-most cited form of attack or abuse.

We conducted our assessment on more than 400 systems connected to OCFO/NFC's internal network. We used a commercially available software product designed to identify security vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP)[10]. The results of our scans were provided to responsible OCFO/NFC personnel who immediately began taking corrective actions on the high-risk and medium-risk vulnerabilities. OCFO/NFC provided a written assessment of these vulnerabilities. We generally concurred with the resolution provided by OCFO/NFC in its written response.

Our analysis of OCFO/NFC responses to our assessment results identified a total of 24 high-risk and 129 medium-risk vulnerabilities that, if left uncorrected, could allow internal users unauthorized access to sensitive financial information processed on the network. While OCFO/NFC management was aware of most of the high-risk and medium-risk vulnerabilities identified by our assessment, we did identify 10 high-risk and 57 medium-risk vulnerabilities that required either correction or further investigation.

Seven of the medium-risk vulnerabilities that OCFO/NFC corrected after our assessment had been previously identified by the vulnerability assessment conducted by OCFO/NFC in January 2003. However, OCFO/NFC procedures had not ensured that these vulnerabilities were corrected prior to our assessment. As of May 2003, OCFO/NFC had either corrected or planned corrective action on all of the 10 high-risk and 48 of the 57 medium-risk vulnerabilities that required action.

OCFO/NFC officials agreed with our findings and will develop and implement a process to further strengthen its existing control programs to ensure that vulnerabilities identified by its internal scans continue to be promptly addressed. The plan is to use the existing scan database to not only document scan results but to also track corrective actions.

While conducting our assessment of network vulnerabilities, we also noted that the listing of static IP addresses[11] provided by OCFO/NFC was not accurate. This problem was reported in our November 2002 report on the OCFO/NFC internal control structure.[12] However, we found that more than 30 percent of the more than 450 IP addresses we selected for review were unreachable, indicating that they were not active at the time of our assessment. We also identified three active IP addresses that were not included on the lists provided by OCFO/NFC. Accurate and complete lists of IP addresses are needed to ensure that all systems are routinely scanned and that the OCFO/NFC network is properly monitored and secure.

[10] TCP/IP, the suite of communication protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

[11] A static IP address is a number that is assigned to a computer to be its permanent address on the Internet.

[12] Audit Report No. 11401-13-FM, "Fiscal Year 2001 – 2002 National Finance Center Review of Internal Control Structure," dated November 2002.

OCFO/NFC officials told us that the equipment using the three static IP addresses that were not included on OCFO/NFC's IP address listings were being used on a temporary basis and had subsequently been removed. OCFO/NFC also provided us with a draft policy that includes provisions for creating new static IP addresses, removing static IP addresses that are no longer needed, and periodically reviewing IP addresses to ensure that they are accurate and complete. This policy was finalized and implemented in July 2003. Consequently, we are not making any recommendations regarding maintaining static IP addresses.

Recommendation No. 3

Strengthen the existing controls to ensure that OCFO/NFC promptly addresses the vulnerabilities identified by its internal scans and the remaining high-risk and medium-risk vulnerabilities identified in our assessment.

Agency Response. OCFO agrees with this recommendation. OCFO/NFC will develop and implement a process to further strengthen its existing control programs to ensure that vulnerabilities identified by it internal scans continue to be promptly addressed. The plan is to use the existing scan database to not only document scan results but also to track corrective actions. OCFO/NFC agrees to implement these controls by September 30, 2004.

OIG Position. We concur with the management decision.

Finding 4 Mainframe and Network Access Activity Was Not Consistently Documented or Reviewed

OCFO/NFC was not adequately monitoring access to its mainframe or network systems. OCFO/NFC had created seven mainframe reports that documented certain types of access activity for review, but was not consistently producing or reviewing these reports. We also identified additional types of access to sensitive resources that, if monitored, would enhance OCFO/NFC efforts to identify and investigate unusual or suspicious access activity on its mainframe systems. OCFO/NFC had not (1) established controls to monitor mainframe access activity, (2) set criteria for identifying unusual or suspicious activity that required further investigation, or (3) formalized procedures for documenting and reporting potential security incidents. In addition, the OCFO/NFC had not monitored network access activity since August 2002, despite its internal requirement to do so. OCFO/NFC officials told us that not all of the operating system components required by its monitoring software were installed during its network operating system upgrade conducted in August 2002. Further, OCFO/NFC informed us that they had not fully considered all the security issues involved with this upgrade. Without a complete and effective mainframe and network access activity monitoring program, OCFO/NFC faces increased risk that unauthorized access to the sensitive financial and personnel information processed on these systems will not be detected promptly.

NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook," recognizes that monitoring the access activities of authorized users can help identify significant problems and deter users from inappropriate and unauthorized activities. NIST SP 800-12 also recognizes that, because the amount of security information is likely to be too voluminous to review manually, the most effective monitoring efforts are those that selectively target specific actions. These monitoring efforts should include provisions to identify and investigate both failed attempts to access sensitive data and resources and unusual or suspicious patterns of successful access. In September 2002, OCFO/NFC Management Support Staff issued a Quick Response Assessment that noted that OCFO/NFC was logging access activity but not monitoring these logs in a consistent manner. In response to this report, OCFO/NFC established a monitoring and reporting group within ISSO.

During our fieldwork, ISSO documented the titles, brief descriptions and frequency for the existing mainframe monitoring reports and began producing these reports on a consistent basis. However, this documentation did not include the purpose of the report, criteria for identifying unusual or suspicious activity on the report that required investigation, or guidance for documenting and reporting potential incidents to OCFO/NFC's Security Incident Response Coordinator. Such guidance is important to ensure that unusual or suspicious access to sensitive resources is consistently identified, documented, and investigated to effectively assess potential security incidents.

Our analysis of the reports created by ISSO disclosed that the reports documented access violations, security commands issued by users outside of ISSO, and the use of certain sensitive utilities. However, ISSO had not developed reports that targeted other types of unusual or suspicious access activity, such as (1) modifications to application programs that were not initiated by production control staff or (2) revisions to production data that were completed by system programmers, database administrators, or application programmers.

We also determined that ISSO had developed a process to identify changes to certain critical system security parameter files. However, the files identified were incomplete and did not target unusual activity. For example, ISSO had included database parameter files for some, but not all, of the databases on OCFO/NFC systems.

OCFO/NFC officials told us that they would develop a listing of sensitive system files that should be monitored and then they would produce a daily report showing access to these sensitive files and monitor the activity to ensure only authorized staff members accessed these files. Every 6 months they will review the list of sensitive system files to determine if the list is accurate and/or needs updating. In addition OCFO/NFC is working with the Cyber Security Staff to identify the level of priority for situations that should be elevated in the incident report in accordance with Title VII, Chapter 11, Directive 77, "Computer Intrusion Handling," dated October 4, 2000.

OCFO/NFC officials also told us that ISSO would (1) create reports that identify modifications to application programs that were not initiated by production control staff; (2) document revisions to production data that were completed by system programmers, database administrators, or application programmers; and (3) work with IRMD to identify additional sensitive system resources for which access activity should be monitored by the end of December 2003.

In addition to a lack of mainframe monitoring, we found that the OCFO/NFC had not been monitoring network access since August of 2002. OCFO/NFC's Network Security Policy[13] recognizes that the routine monitoring of users access activities, especially those of users who have the ability to alter sensitive programs and data, can help identify significant problems and deter users from inappropriate and unauthorized activities. The Network Security Policy also states that monitoring efforts will include provisions to review:

- Unsuccessful attempts to gain entry to a system or access sensitive information,
- deviations from access trends,
- successful attempts to access sensitive data and resources,
- highly sensitive privileged access, and
- access modifications made by security personnel.

OCFO/NFC officials told us that the center planned to install the operating system components that would allow ISSO to resume monitoring access activity.

[13] Title VII, Chapter 11, Directive 75

Recommendation No. 4

OCFO/NFC should (1) identify sensitive system resources that should be included in its active monitoring process, (2) develop, test, and document system reports used in its monitoring process, (3) establish guidance for documenting and reporting potential incidents to the Security Incident Response Coordinator, and (4) identify and document the types of unusual activity that should be investigated.

Agency Response. OCFO agrees with this recommendation. For the first two parts of this recommendation, IRMD developed a listing of sensitive system files that should be monitored and provided the listing to ISSO. ISSO manually produces a daily report showing access to these sensitive system files and monitors the activity to ensure only authorized staff members access these files. Every six months, IRMD and ISSO will review the list of sensitive system files to determine if the list is accurate and/or needs updating.

For the third and fourth parts of this recommendation, ISSO is working with the Cyber Security Staff (CSS) to identify the level of priority for situations that should be elevated in the incident report in accordance with Title VII, Chapter 11, Directive 77, Computer Intrusion handling, dated October 4, 2000. OCFO/NFC agrees to implement these controls by December 31, 2004.

OIG Position. We concur with the management decision.

Recommendation No. 5

OCFO should install the necessary operating system components and resume monitoring access activity on its network.

Agency Response. OCFO agrees with this recommendation. ISSO provided the requirements for the operating system components to IRMD. IRMD is coordinating with ISSO to install the required operating system components, which will allow ISSO to resume monitoring access activity on the network using NETWAR 6. OCFO/NFC agrees to install the operating system components by September 30, 2004

OIG Position. We concur with the management decision but believe a shorter implementation timeframe would better serve OCFO/NFC.

We found that OCFO/NFC had not fully complied with the security management requirements included in FISMA and further described in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Specifically, OCFO/NFC had not (1) finalized security plans or the underlying risk assessments for its general support systems and major applications, or (2) certified and accredited its general support systems. We also found that OCFO/NFC had not performed proper background investigations for its employees as required by other Federal regulations. This occurred because OCFO/NFC was not adhering to its own procedures. We also identified issues that need to be addressed to ensure that critical operations can be restored quickly and effectively in the event of an emergency. Until OCFO/NFC fully complies with Federal requirements, it will not have adequate assurance that effective security controls are established and maintained.

Finding 5

Information Security Management Was Not Adequate

OCFO/NFC had not (1) finalized security plans or the underlying risk assessments for its general support systems and major applications, or (2) certified and accredited its general support systems. OCFO/NFC had procedures in place to perform these requirements; however, it was not always following them as prescribed. OCFO/NFC is in the process of finalizing security plans that are based on risk assessments for its general support systems and major applications. However, without adequate security planning and management, OCFO/NFC will face increased risk that the sensitive financial and personnel information processed on its systems will not be adequately protected from unauthorized access, use, disclosure, modification, or destruction.

FISMA, along with the supplemental guidance provided by OMB Circular A-130 and NIST special publications, recognizes the need for a continuous cycle of risk-based security management activities to ensure that effective security controls are established and maintained. This cycle includes (1) assessing risk; (2) developing security plans based on the results of risk assessments; (3) testing the effectiveness of security policies, procedures, and controls (certification); and (4) authorizing information systems processing (accreditation).

Risk assessments provide the foundation for security planning. Security plans document the security requirements and controls for information systems and, as such, should form the basis for the evaluation of security controls. Security certification determines (1) the effectiveness of management, operational, and technical security controls; and (2) the vulnerabilities in an information system after the implementation of such controls. The results of the security certification provide the factual basis for accrediting and authorizing information system processing. By accrediting the information system, the authorizing official accepts the risk associated with system and the implications on agency operations. OMB requires that information systems must be certified and accredited periodically after implementation and whenever there is a significant change to the system or its environment.

Risk Assessments

We determined that OCFO/NFC had not yet finalized risk assessments for its general support systems and major applications. In June 2003, OCFO/NFC officials told us that they were working with a contractor hired by OCIO to develop risk assessments for its major applications and plans to have these finalized by December 2003. In addition, OCFO/NFC officials told us that they were in the process of completing checklists developed by OCIO to identify vulnerabilities on its general support systems.

In March 2002, we recommended that OCFO/NFC establish a risk assessment framework for assessing risks associated with both general support systems and major applications that link security to business needs and provides for managing risk on a continual basis.[14] OCFO/NFC concurred with our recommendation and established the Risk Management and Internal Controls Office to implement such a program. Subsequent to this audit OCFO/NFC has completed three risk assessments and have started three more. In addition, OCFO/NFC officials told us that the center plans to hire a contractor to provide training and to develop security plans based on the risk assessments.

Despite these positive improvements, the center had yet to establish the type of risk assessment framework that we recommended. Such a framework is critical to ensure that IT risks related to OCFO/NFC's ability to accomplish its mission are being effectively identified, assessed, and mitigated through the establishment of appropriate controls. While we still believe that the establishment of a framework that provides for managing risk on a continual basis at OCFO/NFC is important, we are not making a recommendation to establish such a framework in this report because this was previously recommended in March 2002 and OCFO/NFC has begun to take corrective actions.

[14] Audit Report No. 11401-9-FM, "Selected Information Technology General Controls at the National Finance Center Need Strengthening," March 2002.

Security Plans

OCFO/NFC had drafted, but not yet finalized, security plans for its general support systems and major applications. In June 2003, OCFO/NFC officials told us that security plans for its general support systems and major applications had been drafted and submitted to the OCIO for review in April 2003. However, risk assessments for these systems had not yet been completed and the security plans had not yet been finalized. Without well-designed and updated security plans that are risk-based, security controls may be inadequate and IT resources may not be sufficiently protected. In addition, OCFO/NFC will not have adequate assurance that certifications effectively identify weaknesses in security controls until security plans are finalized and used in the certification process.

System Certification and Accreditation

OCFO/NFC had not certified or accredited its general support systems. OCFO/NFC had not finalized or implemented its procedures to certify or accredit these systems in accordance with OMB requirements. Without the necessary security certifications and accreditations, OCFO/NFC cannot ensure the secure operations of its systems and is, therefore, placing sensitive information at increased risk of loss, misuse, and improper modification.

USDA has issued draft guidance for certifying and accrediting systems, which is based on the draft NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems." In October 2003, OCFO/NFC revised its certification and accreditation process in accordance with the departmental guidelines.

OCFO/NFC is piloting their updated process in FY 2003, and plans to perform application certifications based on the new guidance in FY 2004. When performing FY 2004 application certifications, OCFO/NFC also plans to test security controls over the general support system components that are used by the application being certified. In addition, OCFO/NFC officials told us that, while they plan to eventually begin certifying general support systems, the ISPCS Standards and Certification Group does not currently have the resources to start these certifications until after FY 2004. We believe that the OCFO/NFC should consider contractor support to achieve a faster compliance timeframe.

Recommendation No. 6

Establish a time-phased plan of action to ensure compliance with FISMA and OMB requirements including (1) finalizing risk assessments for OCFO/NFC general support systems and major applications, (2) completion of security plans for its general support systems and major applications, and (3) implementation of its certification and accreditation program in accordance with Department-issued guidance.

Agency Response. OCFO agrees with this recommendation. OCFO/NFC completed risk assessments on three systems and is currently conducting risk assessments on three additional systems. OCFO/NFC is also in the process of conducting a risk assessment of the general support systems. OCFO/NFC also realizes these risk assessments are not final until we develop security plans. OCFO/NFC will contract for that service and include the results in the risk assessments. ISPCS/Information Systems Quality Assurance Office implemented its revised certification and accreditation process October 1, 2003, in accordance with the Departmental guidelines. OCFO/NFC agrees to complete all necessary risk assessments and security plans by September 30, 2004.

OIG Position. We concur with the management decision.

Finding 6

Required Background Investigations Were Not Obtained

OCFO/NFC had not performed security background investigations for all of its information resources management personnel or completed periodic reinvestigations (PRI) as required by its management directives. We also found that OCFO/NFC was not classifying most security administrator, system programmer, and application programmer positions as high-risk even though the functions associated with these positions met its high-risk definition. OCFO/NFC officials told us that this situation existed because they had not been following their own prescribed procedures. Without the necessary security background investigations and reinvestigations, OCFO/NFC faces the risk of exposing its information resources to loss or harm that could be caused by these individuals.

Executive Order 10450 states that the appointment of each civilian officer or employee in any Department or agency of the Government shall be made subject to investigation. In this regard, the Office of Personnel Management has established general requirements that every competitive service position be designated at a risk level commensurate with the public trust responsibilities of the position. In 1998, OCFO/NFC issued Title VII, Chapter 14, Directive 7, "Risk Levels, Position Sensitivity Designations, and Background Investigations for OCFO/NFC and Contractor Personnel." With this directive, OCFO/NFC established its policy, responsibilities, and procedures for assigning risk levels, designating position sensitivity, and obtaining required background investigations for OCFO/NFC and contractor personnel.

OCFO/NFC procedures require most OCFO/NFC and contractor personnel to have a background investigation. In addition, PRIs are required (1) every 5 years for personnel in positions designated as high-risk or (2) if an individual moves into a new position that requires a higher level of investigation. However, we found weaknesses in each of these areas.

In March 2003, OCFO/NFC provided us a file documenting the background investigation history for all OCFO/NFC employees and contractors. Our review disclosed the following:

- Security background investigations were not performed for 30 of the 302 classified as computer/IT specialists at OCFO/NFC. We determined that 23 of these 30 had been employed for at least 10 years.

- PRIs were not performed for 13 of the 14 critical high-risk positions. We also noted that two of the 14 high-risk positions had an initial investigation over 30 years ago, but had not had any reinvestigations.

- A PRI was not performed for the Chief of ISSO after he moved into this position, which required a higher level of investigation.

We also found that OCFO/NFC had only classified 13 individuals in computer/information systems positions as high-risk.[15] The 13 individuals classified as having high-risk computer/information systems positions included 7 staff members in upper level management positions and 6 application programmers. We believe that the majority of staff members in computer/information systems positions, especially those responsible for developing, implementing, and maintaining application, system, and security software, should also be included in the high-risk classification as defined by the OCFO/NFC directive. In addition, we noted that OCFO/NFC was not always updating position sensitivity levels in its tracking system.

OCFO/NFC officials told us they had not been following the prescribed directive, but would begin. As of April 2003, OCFO/NFC Human Resources Management Staff (HRMS) had 89 investigations in progress. HRMS has reviewed position sensitivity for all positions and reclassified positions such as security administrators, system programmers, and application

[15] OCFO/NFC Title VII, Chapter 14, Directive 7, "Risk Levels, Position Sensitivity Descriptions, and Background Investigations for OCFO/NFC and Contractor Personnel," dated February 19, 1998, defines high-risk levels for computer/information systems positions to include those in which the incumbent "is responsible for the planning, direction, and implementation of a computer security program; has major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or has the responsibility for maintenance of a computer system."

programmers as high-risk positions. Consequently, we are not making any further recommendations concerning the reclassification of position sensitivity levels.

Recommendation No. 7

Establish controls to ensure that OCFO/NFC maintains complete and up-to-date background investigation records and that it uses these records to ensure timely completion of all background investigations and reinvestigations of high-risk positions.

Agency Response. OCFO agrees with this recommendation. OCFO/NFC determined in early fiscal year 2003 that "controls for determining the trustworthiness, reliability, and good conduct and character of personnel" needed improvement. To that end, management mandated that controls for obtaining and tracking security clearances for employees and contractors take on a higher profile. OCFO/NFC began working closely with the Department of Agriculture's (USDA) Personnel Security Division Director, to ensure NFC is complying with Office of Personnel Management's and Departmental Regulations for employee background investigations and to determine when periodic reinvestigations are required. They are clarifying issues on proper Position Sensitivity Designation codes and periodic reinvestigations requirements. We believe that we now have controls in place to ensure that OCFO/NFC maintains complete and up-to-date documentation of background investigation records and that we use these records to ensure timely completion of all background investigations and reinvestigations of high-risk positions.

OIG Position. We concur with the management decision.

Finding 7

Disaster Recovery Planning and Testing Could Be Improved

While OCFO/NFC had developed a disaster recovery plan and routinely performed tests of this plan, we found that a demand for more immediate information could require OCFO/NFC to update its recovery methodology. Currently, OCFO/NFC relies on a tape-based method of restoring its systems, which could preclude the center from sufficiently improving its recovery time to meet customer requirements. This situation exists because OCFO/NFC has not fully explored alternative methods of restoration that would provide for quicker recovery of operations. As a result, OCFO/NFC may not be able to reestablish important business functions swiftly enough to ensure that critical business operations and services provided to other government agencies will not be disrupted.

FISMA requires agencies to develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. In addition, OMB Circular A-130 states that such plans should be tested. USDA Departmental Manual 3140-1, "Management Automated Data Processing (ADP) Security Manual," Section 11, reiterates these requirements and recognizes that thorough planning should address all aspects of the following tasks:

- Maintaining adequate materials at the backup or alternative site;
- handling the immediate emergency;
- maintaining liaison between facility management and users;
- moving people, data, and support supplies to the previously designated alternate site(s);
- processing at the alternate site(s);
- restoring or relocating the damaged facility; and
- returning to the primary site in an orderly manner.

OCFO/NFC operates systems, such as the Thrift Savings Program (TSP), that are moving toward providing their customers with more immediate information. For example, TSP has changed its system to provide daily rather than monthly transaction processing and valuation of customer accounts. OCFO/NFC officials informed us that the preliminary results of a disaster recovery business impact analysis noted that certain customers want the recovery timeframe reduced. However, because of its reliance on tape-based data recovery, it is unlikely that current OCFO/NFC processes will be able to be significantly improved to meet these needs.

OCFO/NFC currently uses backup tapes as the primary source for the restoration of business operations. The volume of backup tapes required to restore operations hampers any significant improvement in the speed of restoration. Currently, OCFO/NFC would be required to ship between 25,000 and 30,000 tapes to the restoration site in the event of a disaster. These tapes would then be hand-loaded into tape reading equipment when received at the restoration site. As more product lines and client agencies are added to the business operations at OCFO/NFC, the number of backup tapes will likely increase to the point of becoming unmanageable and the risk of missing backup tapes will increase. OCFO/NFC officials told us that they have a history of missing backup tapes during disaster recovery drills. A missing key tape could seriously impact the recovery time and ability to fully recover. OCFO/NFC officials further informed us that they are looking at alternative methods.

In October 2003, OCFO/NFC officials told us that they will establish a control to annually update the Business Impact Analysis to assess customers' expectations regarding continuity of NFC operations and to evaluate its disaster recovery process, including alternative methods of restoration, to ensure that customers' expectations are met.

Recommendation No. 8

OCFO/NFC should evaluate its disaster recovery process, including alternative methods of restoration, to ensure that they meet the expectations of the customers that use its critical systems.

Agency Response. OCFO agrees with this recommendation. OCFO/NFC will establish a control to annually update the Business Impact Analysis to assess customers' expectations regarding continuity of OCFO/NFC operations and to evaluate its disaster recovery process, including alternative methods of restoration, to ensure that customers' expectations are met. OCFO/NFC agrees to implement this control by March 31, 2004.

OIG Position. We concur with the management decision.

We found that OCFO/NFC had not always ensured that changes to system software had been adequately tested, and that OCFO/NFC had not always considered the security impact of system software changes. We also found that OCFO/NFC had not established adequate controls over the configuration of its mainframe operating system. These weaknesses occurred because OCFO/NFC had not established suitable controls to ensure that its policies and procedures were operating as intended. Until these issues are addressed, OCFO/NFC will face increased risk that system software will not be configured in a manner that affords proper protection to OCFO/NFC systems and the sensitive financial and personnel data that is maintained on these systems.

Finding 8

System Software Change Controls Need Improvement

Although OCFO/NFC had documented and approved changes to system software and required that such changes be tested before implementation, we found that OCFO/NFC had not always adequately tested non-emergency system software changes, evaluated the security impacts associated with non-emergency changes, or reviewed emergency changes. This situation existed because OCFO/NFC had not:

- Established guidance describing the test methodology and documentation required for different types of system software changes;
- implemented procedures to ensure that security impacts were adequately identified, documented, and addressed during the system software change control process;
- instituted a method of ensuring that only approved system software changes were implemented; or
- ensured that emergency system software changes are reviewed adequately. Until these issues are addressed, OCFO/NFC will face increased risk that unauthorized changes to system software could be used to bypass security controls and improperly modify OCFO/NFC application programs and the financial and sensitive personnel information processed by these applications.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. Therefore, it is important to ensure that changes are tested prior to implementation. In addition, NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," states that organizations should ensure that changes to the system do not unintentionally or unknowingly diminish security. In this regard, interim guidance on USDA configuration management (CS-009) recognizes that the failure to control system configurations and changes could result in weak or ineffective security controls protecting system data. In December 1991, OCFO/NFC issued Title VII, Chapter 11, Directive 59, "ADP Operating Environment Change Management (Revision 1)," which provides the policy, procedures, and responsibilities for requesting, recording, and implementing changes to the ADP operating environment, including system hardware and software. With this directive, OCFO/NFC required all system software changes to be documented and approved prior to implementation, and non-emergency changes to be tested prior to implementation whenever possible. The system software change control directive (Title VII, Chapter 11, Directive 59) also includes a provision for creating a monthly report of all change requests that were implemented.

Testing System Software Changes

We judgmentally selected a sample of five non-emergency system software change requests completed from October 1, 2002, to May 16, 2003, for review to determine if system software changes were adequately documented, approved, and tested prior to implementation. OCFO/NFC officials told us that all of the changes in our sample had been tested, as required by its system software change control directive. However, we could not determine if testing was sufficient or complete because the associated test documentation was not adequate. Four of the five changes that we reviewed indicated that testing had occurred, but the test results field only reflected that the test was successful. For two of the four, we found that OCFO/NFC had maintained additional test documentation but the results were not described and/or referenced on the change request form. The following is an example of the inadequate testing we found:

- A new version of a system software package was implemented without adequately testing how it interacted with OCFO/NFC security routines. Consequently, users experienced problems with obtaining the correct data and an emergency change was implemented to revert back to the older version of the software. We obtained the change request form, which stated that the change was tested and implemented into production, but no data was provided in the test results field. OCFO/NFC provided us with additional test documentation relating to this change, but it did not sufficiently describe what functions had been tested or how testing was performed.

We recognize that system software changes require different levels and methods of testing based on the type of change. Therefore, OCFO/NFC should establish guidance that describes the test methodology and required documentation for different types of system software changes. OCFO/NFC should also establish controls to ensure that changes are consistently tested and documented in a sufficient manner.

Assessing the Security Impact of System Software Changes

We also found that OCFO/NFC had not thoroughly identified, documented, or addressed the security impacts associated with system software changes. This occurred because neither the OCFO/NFC system software change control directive nor the current change request form provide guidance for documenting and evaluating potential security impacts associated with system software changes. As a result, security weaknesses, such as those identified in Finding No. 2, went undetected. In addition, OCFO/NFC was not able to effectively monitor access activity on its internal network.

Ensuring Only Approved System Software Changes are Implemented

Furthermore, OCFO/NFC had not instituted a process to ensure that all changes to system software have been appropriately authorized. This is especially important at OCFO/NFC because system programmers rather than an independent control group generally implement changes to system software. While changes to system software may be logged, OCFO/NFC personnel told us that the center had not yet established a process to document and review changes to system software to ensure that only authorized modifications had occurred. OCFO/NFC is currently evaluating a configuration management tool that can be used to monitor changes to system software. However, until OCFO/NFC establishes a method of ensuring that only authorized changes to system software are made, it will face unnecessary risks that operating system-based security controls could be compromised and that the system may be impaired.

Reviewing Emergency System Software Changes

Finally, we determined that the current change control procedures do not ensure that emergency system software changes are reviewed adequately. OCFO/NFC requires emergency changes to system software when critical problems occur. While we would not expect emergency changes to be tested prior to implementation, such changes should be (1) documented and authorized at the time, and (2) subsequently reported and reviewed.

We selected 2 of the 49 emergency system software changes that occurred from October 1, 2002, to May 16, 2003. We found that OCFO/NFC had documented and authorized these changes; however, OCFO/NFC had not required that these emergency changes be subsequently reported for review. OCFO/NFC prepares and submits to management a report that documents change requests implemented during each maintenance period. We found that OCFO/NFC failed to include emergency changes on this report.

Another crucial step in evaluating emergency changes is documentation of how the emergency change was validated to ensure that the change was working properly. We found that this validation was documented on only 24 of the 49 emergency changes that occurred from October 1, 2002, to May 16, 2003.

Until OCFO/NFC establishes procedures for subsequently reviewing emergency changes and adequately document how emergency changes were validated, it will face increased risk that subsequent reviews of these changes will not occur on a consistent basis and/or identify instances where emergency changes may not be performing as intended. OCFO/NFC officials told us that they will establish controls to ensure that (1) only authorized system software modifications are implemented, (2) all system software changes and associated testing are documented and reported to management, and (3) emergency system software changes include documentation of validation procedures, and (4) implement procedures to ensure that security impacts associated with changes to system software are identified, evaluated, and adequately addressed.

Recommendation No. 9

OCFO/NFC should establish controls to ensure that (1) only authorized system software modifications are implemented, and (2) all system software changes and associated testing are documented and reported to management, and (3) emergency system software changes include complete documentation of validation procedures.

Agency Response. OCFO agrees with this recommendation. OCFO/NFC will establish controls to ensure that (1) only authorized system software modifications are implemented, (2) all system software changes and associated testing are documented and reported to management, and (3) emergency system software changes include documentation of validation procedures. OCFO/NFC agrees to implement these controls by September 30, 2004.

OIG Position. We concur with the management decision.

Recommendation No. 10

Implement procedures to ensure that security impacts associated with changes to system software are identified, evaluated, and adequately addressed as part of the system software change control process.

Agency Response. OCFO agrees with this recommendation. OCFO/NFC will implement procedures by September 30, 2004 to improve its existing change control process to ensure that security impacts associated with changes to system software are identified, evaluated, and adequately addressed.

OIG Position. We concur with the management decision.

Finding 9 System Software Configuration Controls Could Be Enhanced

We found three sensitive system software libraries that were unnecessarily designated as APF libraries. These libraries no longer required access to sensitive operating system functions that could be used to circumvent security controls. This occurred because OCFO/NFC had not established procedures to periodically review sensitive system software libraries for continued need. We also found that OCFO/NFC was not adequately documenting its review and testing of certain system software components that could be used to circumvent security access controls because it had not established guidance for documenting these reviews. Until OCFO/NFC addresses these issues, it will face increased risk that system software might be used to bypass security controls or gain unauthorized privileges to perform improper actions or circumvent edits and other controls built into application programs.

Access to sensitive operating system functions, which can be used to circumvent all security controls, are restricted to programs that reside in specially designated libraries, referred to as APF libraries. We obtained listings of APF libraries on OCFO/NFC's production mainframe systems and selected 12 for review. Our analysis indicated that 3 of these 12 APF libraries were no longer needed and could be removed. In July 1999, GAO reported that OCFO/NFC had not instituted a process to periodically review programs in APF libraries to identify and correct weaknesses. Since then, OCFO/NFC had begun identifying certain conditions that required correction, but had not established a procedure to periodically review APF libraries for continued need. OCFO/NFC officials informed us that all three of these libraries were removed before the completion of our fieldwork.

We also reviewed controls over supervisor calls (SVC), which could be used to bypass security controls and alter data, programs, and audit trail information. We obtained listings of SVCs that existed on OCFO/NFC's production mainframe systems and selected five for review. OCFO/NFC had established a requirement to either (1) obtain written integrity statements from vendors or (2) inspect the code to ensure that adequate safeguards are included in SVCs. However, OCFO/NFC could not provide documentation to show that it had obtained integrity statements or adequately reviewed and tested two of the five SVCs. During our fieldwork, OCFO/NFC obtained an integrity statement from the software vendor for one of these SVCs and retested the other.

Subsequent to this audit OCFO/NFC instituted a process to periodically review APF libraries and plans to develop and implement an improved process to expeditiously remove from the listing those APF libraries that are no longer required. They also agreed to establish controls to ensure compliance with these improved processes. In addition, they will establish controls to ensure that vendor integrity statements are obtained and that adequate testing is performed and documented for SVCs.

Recommendation No. 11

Establish controls to ensure that APF libraries are periodically reviewed and timely removed when no longer needed.

Agency Response. OCFO agrees with this recommendation OCFO/NFC has a process in place to periodically review Authorized Program Facilities (APF) libraries. OCFO/NFC also plans to develop and implement an improved process to expeditiously remove from the listing those APF libraries that are no longer required. OCFO/NFC will also establish controls to ensure compliance with these improved processes by September 30, 2004.

OIG Position. We concur with the management decision.

Recommendation No. 12

Establish controls to ensure that vendor integrity statements are obtained or that adequate testing is performed and documented for all SVCs.

Agency Response. OCFO agrees with this recommendation. OCFO/NFC will establish controls to ensure that vendor integrity statements are obtained and that adequate testing is performed and documented for Supervisor Calls by September 30, 2004.

OIG Position. We concur with the management decision.

Scope and Methodology

We reviewed the adequacy of security over the OCFO/NFC mainframe systems and internal networks, including logical and physical access controls, and controls over the modification of system software on these computer systems. We did not evaluate OCFO/NFC internal controls over (1) developing, implementing, and/or modifying application software; or (2) other general controls that applied directly to specific applications developed and/or operated by OCFO/NFC.

We performed our work at OCFO/NFC, which is located in New Orleans, Louisiana, from February 2003 through June 2003 in accordance with generally accepted Government Auditing Standards.

To accomplish our audit objectives, we (1) identified and reviewed security policies and procedures relating to IT general controls from USDA, OCIO, and OCFO/NFC; (2) held discussions with OCFO/NFC officials responsible for IT general controls; and (3) conducted tests of controls in operation to determine whether the IT general controls were in place, adequately designed, and operating effectively. Our testing included the following procedures:

- We obtained and reviewed listings of OCFO/NFC staff members with access to production source code, production load modules, production batch operational procedures, sensitive operating system files, APF libraries, system logging files, certain utility programs, and other system resources to determine if access to sensitive data and resources was adequately restricted.

- We performed Internet Security Software and BindView scans to identify network security vulnerabilities and network account and password management control weaknesses on OCFO/NFC internal networks.

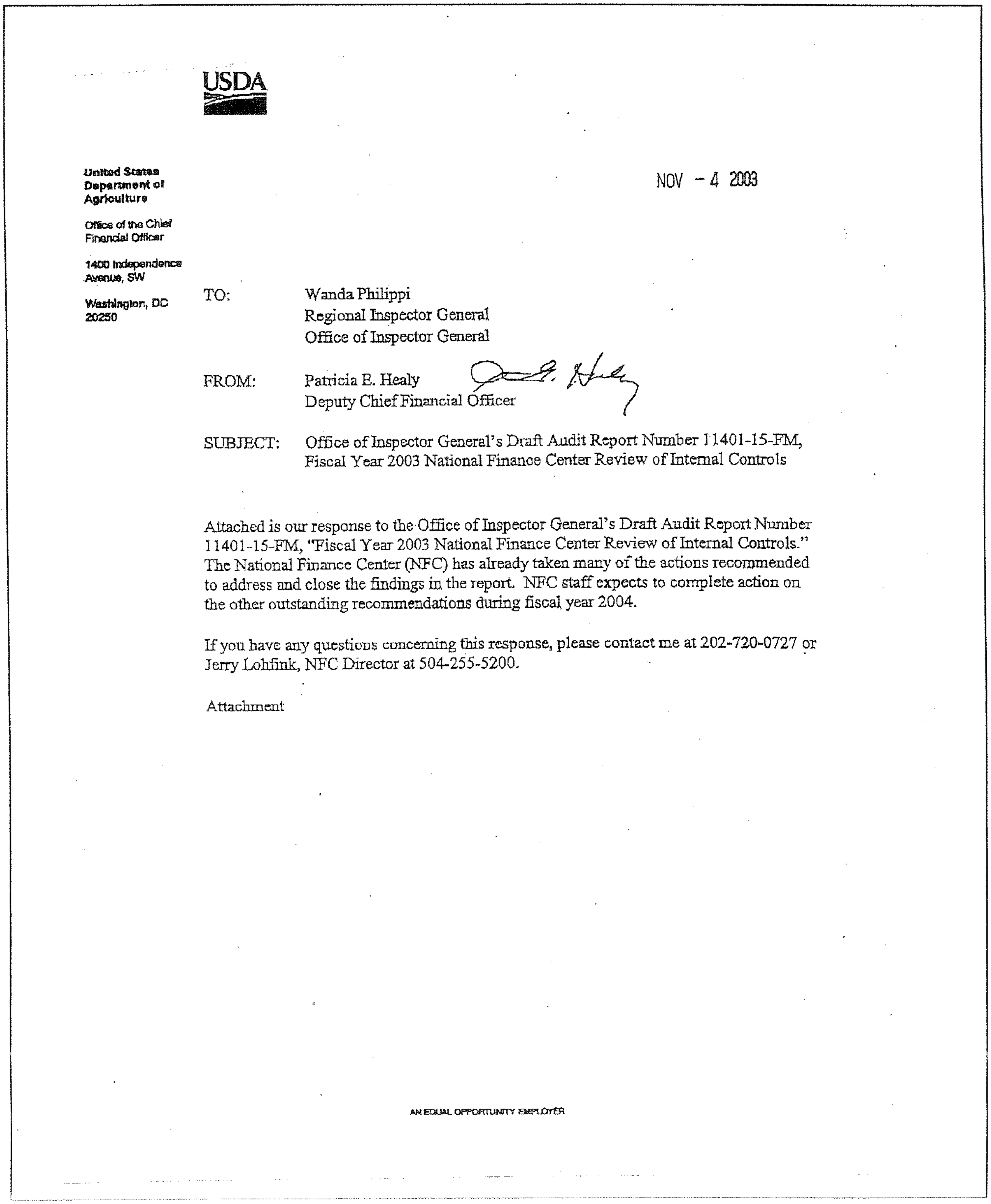
- We performed a PhoneSweep scan of authorized modem phone lines and reviewed a more complete review of OCFO/NFC phone lines to determine if access from remote locations was sufficiently secured.

- We reviewed a sample of system software changes completed from October 1, 2002 through May 16, 2003, to determine if changes were appropriately documented, tested, and approved. This sample was selected judgmentally to ensure that both emergency and non-emergency changes made by different OCFO/NFC organizational units were included.

- We evaluated OCFO/NFC disaster recovery plans and observed an OCFO/NFC disaster recovery test to determine if OCFO/NFC disaster recovery planning and testing provided reasonable assurance that the center could promptly recover from an unexpected interruption in service.

As suggested by OMB guidance on implementing FISMA, our evaluation was based on the guidance provided in GAO's FISCAM; OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources;" and guidance issued by NIST.

Exhibit A – Agency Response



USDA

United States
Department of
Agriculture

Office of the Chief
Financial Officer

1400 Independence
Avenue, SW

Washington, DC
20250

NOV - 4 2003

TO: Wanda Philippi
Regional Inspector General
Office of Inspector General

FROM: Patricia E. Healy
Deputy Chief Financial Officer

SUBJECT: Office of Inspector General's Draft Audit Report Number 11401-15-FM, Fiscal Year 2003 National Finance Center Review of Internal Controls

Attached is our response to the Office of Inspector General's Draft Audit Report Number 11401-15-FM, "Fiscal Year 2003 National Finance Center Review of Internal Controls." The National Finance Center (NFC) has already taken many of the actions recommended to address and close the findings in the report. NFC staff expects to complete action on the other outstanding recommendations during fiscal year 2004.

If you have any questions concerning this response, please contact me at 202-720-0727 or Jerry Lohfink, NFC Director at 504-255-5200.

Attachment

AN EQUAL OPPORTUNITY EMPLOYER

Response to the Office of Inspector General's
Draft Audit Report Number 11401-15-FM
United States Department of Agriculture
Fiscal Year 2003 National Finance Center
Review of Internal Controls

OIG Recommendation No. 1

Implement procedures to document and establish controls to maintain organizational access profiles for internal users to ensure that these profiles provide access based on current job functions.

Management Response:

We agree with this recommendation with respect to information technology specialist positions. The Information Resources Management Division (IRMD) is developing a Trusted Facilities Manual (TFM). The TFM will define the roles and responsibilities of all information technology specialists. Once IRMD completes the TFM, the Information Systems Policy and Control Staff's (ISPCS) Information Systems Security Office (ISSO) will use the defined roles from the TFM to create security profiles associated with each information technology specialist's duties and responsibilities.

Estimated Completion Date: June 30, 2004

Responsible Organization: IRMD, ISPCS

Contact Person: Gilbert Hawk, Jim Julian

OIG Recommendation No. 2

The Office of the Chief Financial Officer, National Finance Center (OCFO/NFC) should identify sensitive operating system files and establish controls to ensure that access is periodically reviewed to ensure that access is appropriately restricted to only authorized staff members based on job responsibilities.

Management Response:

We agree with this recommendation. IRMD developed a listing of sensitive files that should be monitored and provided the listing to ISSO. At this time, ISSO manually produces a daily report showing access to these sensitive files and monitors the activity to ensure only authorized staff members access the files. ISSO is currently in the process of automating the reports in the Scheduler. Every six months, IRMD and ISSO will review the list of sensitive files to determine if the list is accurate and/or needs updating.

Completion Date: September 25, 2003

Responsible Organization: IRMD, ISPCS

Contact Person: Gilbert Hawk, Jim Julian

OIG Recommendation No. 3

Establish procedures and controls to identify reassigned employees and adjust their level of access, as appropriate, in a timely manner.

Management Response:

We agree with this recommendation. On the first Monday of every pay period, ISSO produces a report entitled, "Tracking Employees Security Access To Mainframes." This report lists all employees transferred in the previous pay period. ISSO sends the report to the Division Security Coordinator of the division losing the transferred employee. In the cover memo accompanying the report, ISSO requests managers to review the listing and to take the necessary action to remove the access of the losing employee. ISSO also requests provide positive feedback on actions taken.

Completion Date: May 12, 2003

Responsible Organization: ISPCS

Contact Person: Jim Julian

OIG Recommendation No. 4

Ensure the automated processes used to delete inactive user IDs assigned to OCFO/NFC staff members are properly tested and are operating effectively.

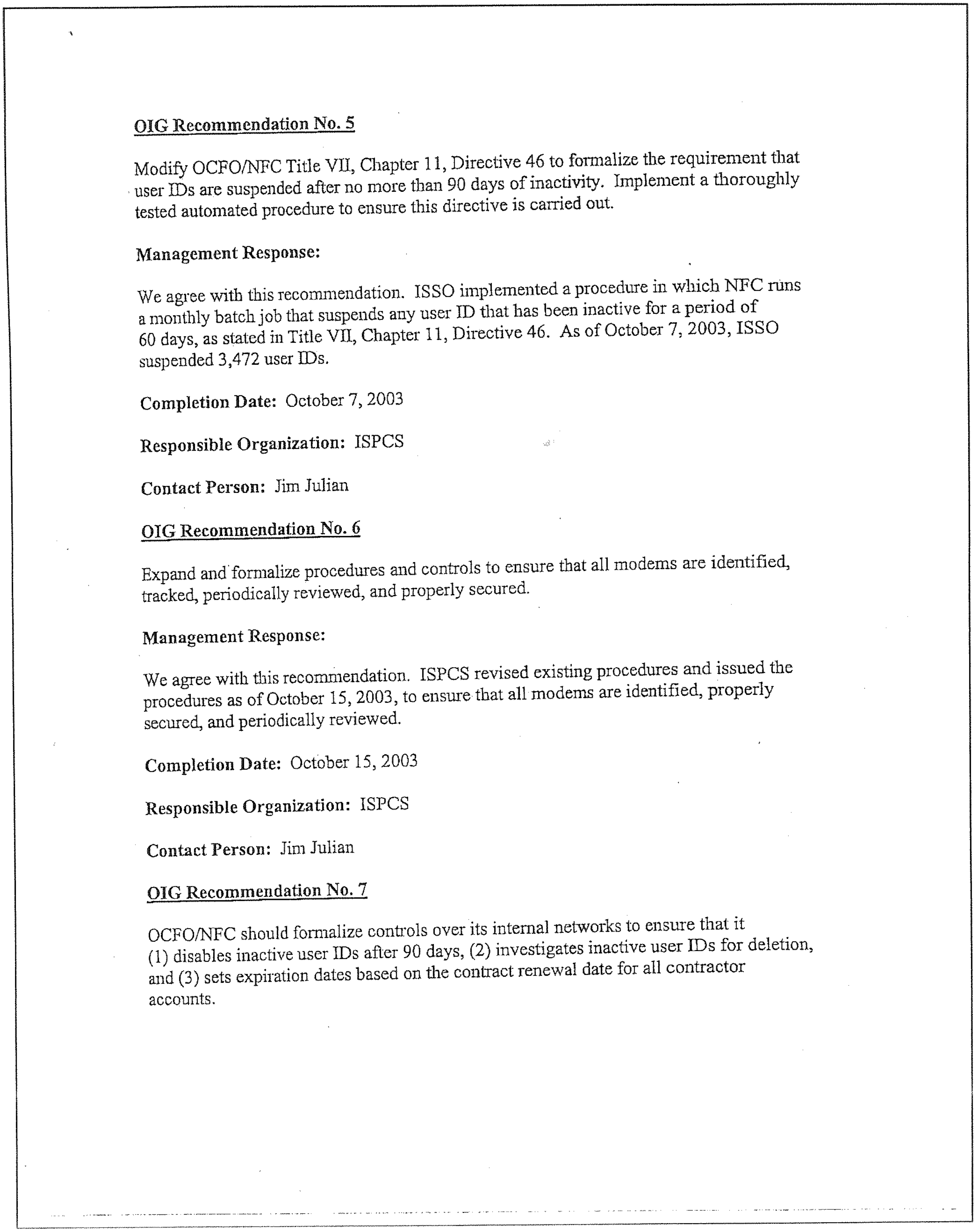
Management Response:

We agree with this recommendation. ISSO modified the automated process to delete inactive user identifications (ID). This process encompasses deletion of all user IDs, including NFC users. The process has been properly tested and operating effectively since June 2003.

Completion Date: June 30, 2003

Responsible Organization: ISPCS

Contact Person: Jim Julian



OIG Recommendation No. 5

Modify OCFO/NFC Title VII, Chapter 11, Directive 46 to formalize the requirement that user IDs are suspended after no more than 90 days of inactivity. Implement a thoroughly tested automated procedure to ensure this directive is carried out.

Management Response:

We agree with this recommendation. ISSO implemented a procedure in which NFC runs a monthly batch job that suspends any user ID that has been inactive for a period of 60 days, as stated in Title VII, Chapter 11, Directive 46. As of October 7, 2003, ISSO suspended 3,472 user IDs.

Completion Date: October 7, 2003

Responsible Organization: ISPCS

Contact Person: Jim Julian

OIG Recommendation No. 6

Expand and formalize procedures and controls to ensure that all modems are identified, tracked, periodically reviewed, and properly secured.

Management Response:

We agree with this recommendation. ISPCS revised existing procedures and issued the procedures as of October 15, 2003, to ensure that all modems are identified, properly secured, and periodically reviewed.

Completion Date: October 15, 2003

Responsible Organization: ISPCS

Contact Person: Jim Julian

OIG Recommendation No. 7

OCFO/NFC should formalize controls over its internal networks to ensure that it (1) disables inactive user IDs after 90 days, (2) investigates inactive user IDs for deletion, and (3) sets expiration dates based on the contract renewal date for all contractor accounts.

Management Response:

We agree with this recommendation. ISSO implemented a monthly reporting process that selects all user accounts that have been inactive for 90, 120, and 150+ days. The appropriate action is taken according to the specific timeframes. These reports run parallel to the mainframe-automated process that reports inactive accounts on that platform. On August 4, 2003, all 16 contractor accounts were corrected to specify an expiration date. ISSO will ensure access is provided in accordance with the NFC Management Directives.

Completion Date: October 1, 2003

Responsible Organization: ISPCS

Contact Person: Jim Julian

OIG Recommendation No. 8

Strengthen the existing controls to ensure that OCFO/NFC promptly addresses the vulnerabilities identified by its internal scans and the remaining high-risk and medium-risk vulnerabilities identified in our assessment.

Management Response:

We agree with this recommendation. NFC will develop and implement a process to further strengthen its existing control programs to ensure that vulnerabilities identified by it internal scans continue to be promptly addressed. The plan is to use the existing scan database to not only document scan results but to also track corrective actions.

Estimated Completion Date: September 30, 2004

Responsible Organization: IRMD

Contact Person: Gilbert Hawk

OIG Recommendation No. 9

OCFO/NFC should (1) identify sensitive system resources that should be included in its active monitoring process, (2) develop, test, and document system reports used in its monitoring process, (3) establish guidance for documenting and reporting potential incidents to the Security Incident Response Coordinator, and (4) identify and document the types of unusual activity that should be investigated.

Management Response:

We agree with this recommendation. For the first two parts of this recommendation, IRMD developed a listing of sensitive system files that should be monitored and provided the listing to ISSO. ISSO manually produces a daily report showing access to these sensitive system files and monitors the activity to ensure only authorized staff members access these files. Every six months, IRMD and ISSO will review the list of sensitive system files to determine if the list is accurate and/or needs updating.

For the third and fourth parts of this recommendation, ISSO is working with the Cyber Security Staff (CSS) to identify the level of priority for situations that should be elevated in the incident report in accordance with Title VII, Chapter 11, Directive 77, Computer Intrusion handling, dated October 4, 2000.

Completion Date for Parts 1 and 2: September 25, 2003.

Estimated Completion Date for Parts 3 and 4: December 31, 2003

Responsible Organization: IRMD, ISPCS, CSS

Contact Person: Gilbert Hawk, Jim Julian, Archie Bertrand

<u>OIG Recommendation No. 10</u>

OCFO/NFC should install the necessary operating system components and resume monitoring access activity on its network.

Management Response:

We agree with this recommendation. ISSO provided the requirements for the operating system components to IRMD. IRMD is coordinating with ISSO to install the required operating system components, which will allow ISSO to resume monitoring access activity on the network using NETWAR 6.

Estimated Completion Date: September 30, 2004

Responsible Organization: IRMD, ISPCS

Contact Person: Gilbert Hawk, Jim Julian

<u>OIG Recommendation No. 11</u>

Establish a time-phased plan of action to ensure compliance with FISMA and OMB requirements including (1) finalizing risk assessments for OCFO/NFC general support systems and major applications, (2) completion of security plans for its general support by controlling guidelines. We believe that we now have controls in place to ensure that NFC maintains complete and up-to-date documentation of background investigation records and that we use these records to ensure timely completion of all background investigations and reinvestigations of high-risk positions.

Completion Date: September 30, 2003

Responsible Organization: HRMS

Contact Person: Albert Bryden

OIG Recommendation No. 13

OCFO/NFC should establish controls to periodically evaluate its disaster recovery process, including alternative methods of restoration, to ensure that they meet the expectations of the customers that use its critical systems.

Management Response:

We agree with this recommendation. NFC will establish a control to annually update the Business Impact Analysis to assess customers' expectations regarding continuity of NFC operations and to evaluate its disaster recovery process, including alternative methods of restoration, to ensure that customers' expectations are met.

Completion Date: March 31, 2004

Responsible Organization: Cyber Security Staff

Contact Person: Archie Bertrand

OIG Recommendation No. 14

OCFO/NFC should ensure that a full test of payroll processing, from the receipt of T&A data through the generation of Statements of Earnings and Leave is periodically performed to verity that the restoration process is functioning as required.

Management Response:

We believe we have already met the intent of this recommendation. NFC conducts twice a year disaster recovery tests at a different location. We have planned and tested and continue to test all essential portions of payroll processing throughout the process over multiple test windows. We have documentation of past tests to demonstrate this. Therefore, we suggest that this recommendation is unnecessary.

Completion Date: December 31, 2002

Responsible Organization: CSO

Contact Person: Archie Bertrand

OIG Recommendation No. 15

Develop procedures for establishing and maintaining detailed listings for equipment and supplies required by organizational units involved in OCFO/NFC disaster recovery. Include the listings within OCFO/NFC Disaster Recovery Plans or refer to the listings so that they can be easily located.

Management Response:

We believe we have already met the intent of this recommendation. NFC has a Corporate-Wide Disaster Recovery Program that identifies the required baseline equipment and supplies. Additionally, each organization has a Disaster Recovery document that identifies any required equipment and supplies that have not been identified in the Corporate-Wide document. Based on this, we suggest that this recommendation is unnecessary.

Completion Date: December 31, 2002

Responsible Organization: CSS

Contact Person: Archie Bertrand

OIG Recommendation No. 16

OCFO/NFC should establish controls to ensure that (1) only authorized system software modifications are implemented, and (2) all system software changes and associated testing are documented and reported to management, and (3) emergency system software changes include complete documentation of validation procedures.

Management Response:

We agree with this recommendation. NFC has documented the guidance for use of the batch emergency ID and will include this documentation in the next release of the Scheduling Desk Procedures Manual. NFC will also establish controls to ensure that (1) only authorized system software modifications are implemented, (2) all system software changes and associated testing are documented and reported to management, and (3) emergency system software changes include documentation of validation procedures.

Estimated Completion Date: September 30, 2004

Responsible Organization: IRMD

Contact Person: Gilbert Hawk

OIG Recommendation No. 17

Implement procedures to ensure that security impacts associated with changes to system software are identified, evaluated, and adequately addressed as part of the system software change control process.

Management Response:

We agree with this recommendation. NFC will implement procedures to improve its existing change control process to ensure that security impacts associated with changes to system software are identified, evaluated, and adequately addressed.

Completion Date: September 30, 2004

Responsible Organization: IRMD

Contact Person: Gilbert Hawk

OIG Recommendation No. 18

Establish controls to ensure that APF libraries are periodically reviewed and timely removed when no longer needed.

Management Response:

We agree with this recommendation. NFC has a process in place to periodically review Authorized Program Facilities (APF) libraries. NFC also plans to develop and implement an improved process to expeditiously remove from the listing those APF libraries that are no longer required. NFC will also establish controls to ensure compliance with these improved processes.

Completion Date: September 30, 2004

Responsible Organization: IRMD

Contact Person: Gilbert Hawk

OIG Recommendation No. 19

Establish controls to ensure that vendor integrity statements are obtained or that adequate testing is performed and documented for all SVCs.

Management Response:

We agree with this recommendation. NFC will establish controls to ensure that vendor integrity statements are obtained and that adequate testing is performed and documented for Supervisor Calls.

Completion Date: September 30, 2004

Responsible Organization: IRMD

Contact Person: Gilbert Hawk