U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Fiscal Year 2004 – Review of the National Finance Center General Controls

Report No. 11401-20-FM
October 2004

USDA

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

OIG

DATE: OCT 25 2004

REPLY TO
ATTN OF: 11401-20-FM

SUBJECT: Fiscal Year 2004 – Review of the National Finance Center General Controls

TO: Patricia E. Healy
Acting 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) as of June 30, 2004. The audit was conducted in accordance with "Government Auditing Standards" issued by the Comptroller General of the United States including American Institute of Certified Public Accountants Professional Standards AU Sections 316, 319, and 324 as amended by applicable Statements on Auditing Standards (SAS), commonly referred to as a SAS 70 audit. While OCFO/NFC has taken significant corrective actions during the fiscal year, the report contains a qualified opinion on the internal control structure because certain control policies and procedures, as described in the report, were not suitably designed or operating effectively.

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

In accordance with Departmental Regulation 1720-1, please furnish a reply within 30 days describing the corrective actions taken or planned, and the timeframes for implementation. Please note that the regulation requires a management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

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

Robert W. Young

ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Fiscal Year 2004 - Review of the National Finance Center General Controls

Results in Brief

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) as of June 30, 2004. While the center has taken significant corrective actions during the fiscal year, the report contains a qualified opinion on the internal control structure because certain control policies and procedures, as described in the report, were not suitably designed, and/or operating effectively at the time of our review.

Our objectives were to perform testing necessary to express an opinion about (1) whether the control objectives and techniques in exhibit A for the U.S. Department of Agriculture's OCFO/NFC present fairly, in all material respects, the aspects of the OCFO/NFC policies and procedures in place and operating effectiveness during the period October 1, 2003, through June 30, 2004, (2) whether this control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily, and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

Our audit disclosed that, except for the matters referred to below, the control objectives and techniques identified in exhibit A present fairly, in all material respects, the relevant aspects of OCFO/NFC. Also, in our opinion, except for the deficiencies described below, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the remaining control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

OCFO/NFC has made significant improvements to ensure compliance with Federal regulations is achieved; however, we found that OCFO/NFC had not completed certification and accreditation of its major applications and general support systems. We found that OCFO/NFC had not updated its directive and functional statements to clearly define security responsibilities after its 2002 reorganization. Further, OCFO/NFC had not completed all required background investigations for individuals in high-risk positions. OCFO/NFC has continued to make progress in these areas and completed its certification and accreditation by September 30, 2004, in accordance with departmental guidance. OCFO/NFC plans to initiate a review to evaluate security responsibilities, and continue obtaining security clearance as funds permit. Without clearly defined security responsibilities, and adequate background investigations, OCFO/NFC will not be adequately assured that its security management structure is operating effectively; and thus putting its critical resources at increased risk of loss, misuse, and improper modification.

We found OCFO/NFC personnel and some of its clients had access to critical payroll and personnel applications that exceeded what was required to perform their job functions. In some instances, the access provided also violated separation of duty controls. We also determined that OCFO/NFC was not adequately ensuring that access to sensitive client information that was extracted from these systems was adequately protected from unauthorized disclosure. This occurred because OCFO/NFC had not adequately restricted access based on job responsibilities or complied with its prescribed guidance to monitor access for all its employees and external users. As a result, OCFO/NFC systems are at an increased risk of inadvertent or deliberate misuse without detection.

We also found that OCFO/NFC had not ensured that modems on its network were adequately tracked or properly secured, that its firewall configurations were appropriately maintained, or that logs were periodically reviewed on its Web and Unix servers. This occurred because OCFO/NFC had not established adequate controls or complied with its own guidelines to monitor and secure these critical network resources. As a result, OCFO/NFC's network is at unnecessary risk of intrusion and unauthorized access that may not be detected in a timely manner.

Finally, despite prior recommendations, we found that OCFO/NFC needed to strengthen its controls over application changes. Although NFC was documenting application software change requests and approvals, we found that OCFO/NFC needed to ensure that it (1) completes documentation of application change testing, (2) performs user acceptance testing on mandated application software changes, (3) obtains users' approval of application software requirements, and (4) notifies users of emergency changes for subsequent review. These occurred because OCFO/NFC was not adequately enforcing its established guidance. Until these issues are addressed, OCFO/NFC will face increased risk that application software changes may not meet user needs, not operate as intended, or cause unforeseen adverse impacts on the application.

We believe that the internal control weaknesses discussed in this report constitute a material weakness, taken as a whole, and should be reported in OCFO's Federal Managers' Financial Integrity Act until corrected.

Recommendations In Brief

OCFO/NFC is in the process of implementing significant actions to correct the weaknesses we identified in this report and based on prior Office of Inspector General recommendations. Therefore, we make no additional recommendations on outstanding issues. However, we have made recommendations for OCFO/NFC to:

- Update its functional statements, management directives, and any applicable procedures to clearly define and delineate separation of security functions;

- document and implement access profiles based on job responsibilities and separation of duties principles, and establish a process to periodically review user access to ensure that it remains consistent with job functions and separation of duties principles;

- document adequate justification and develop effective compensating controls for those branches that require update access to applications that violate separation of duty controls;

- identify modem phone lines during business hours, expand current procedures to ensure that the modems identified are adequately secured, survey its organizations to identify modems that are currently in use and authorized and update the database accordingly, and establish a process to annually verify that faxes/modems are still needed;

- document the current firewall configuration, establish a formal configuration change management process for the firewall, and begin performing periodic reviews of the firewall configuration;

- develop a process to ensure that adequate testing has been performed and properly documented by the development organization before its approving official signs change requests; and

- establish controls to ensure that acceptance testing is performed or a waiver is obtained prior to implementation for all mandated changes.

Agency Response

OCFO agreed with the findings and recommendations and will provide a specific response to the recommendations under separate cover.

Abbreviations Used in This Report

ADP	Automated Data Processing
CIO	Chief Information Officer
CSS	Cyber Security Staff
DR	Departmental Regulation
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
ID	Identification
IDP	Individual Development Plans
ISSPM	Information Systems Security Program Manager
IT	Information Technology
MOU	Memorandum of Understandings
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SP	Special Publication
T&A	Time and Attendance
USDA	U.S. Department of Agriculture

Table of Contents

Background and Objectives

Background

The National Finance Center (NFC), located in New Orleans, Louisiana, is operated by the U.S. Department of Agriculture's (USDA) Office of the Chief Financial Officer (OCFO). The center operates administrative and financial systems that support the missions of USDA and other Federal Departments. Most importantly, the center is responsible for developing and operating the Payroll/Personnel System. In fiscal year 2003, OCFO/NFC processed more than $66.9 billion in disbursements and collections for USDA and its other customers.

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.

Information security has become increasingly important as computer technology has advanced and Federal agencies have become more dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Homeland Security Presidential Directive (HSPD) – 7, "Critical Infrastructure Identification, Prioritization, and Protection," dated December 17, 2003,[2] requires agencies to identify, prioritize, assess, remediate, and protect their internal critical infrastructure and key resources, and places particular emphasis on information technology (IT) systems. On December 17, 2002, the President signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act. The Act requires each 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.

To assist auditors in evaluating the effectiveness of information system controls, the Government Accountability Office issued the Federal Information System Controls Audit Manual (FISCAM) 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

[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] HSPD-7 supersedes Presidential Decision Directive 63, "Policy on Critical Infrastructure Protection," dated May 22, 1998.

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.

- 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 overall objective was to obtain reasonable assurance about whether the internal control structure of the OCFO/NFC is suitably designed to protect the integrity of the data processed at the OCFO/NFC. More specifically, we performed testing necessary to express an opinion about (1) whether the control objectives and techniques in exhibit A for OCFO/NFC present fairly, in all material respects, the aspects of the OCFO/NFC policies and procedures in place and operating effectiveness, as of June 30, 2004, (2) whether this control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily, and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

Report of the Office of Inspector General

TO: Patricia E. Healy
Acting Chief Financial Officer
U.S. Department of Agriculture

We have examined the control objectives and techniques identified in exhibit A for the U.S. Department of Agriculture's (USDA), Office of the Chief Financial Officer/National Finance Center (OCFO/NFC). Our examination included procedures to obtain reasonable assurance about (1) whether the control objectives and techniques of the OCFO/NFC present fairly, in all material respects, the aspects of the OCFO/NFC's policies and procedures in place and operating effectiveness during the period October 1, 2003, through June 30, 2004, (2) whether the control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily, and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives. The control objectives were specified by OCFO/NFC.

Our audit was conducted in accordance with "Government Auditing Standards" issued by the Comptroller General of the United States and standards issued by the American Institute of Certified Public Accountants and included those procedures we considered necessary to obtain a reasonable basis for rendering our opinion.

While OCFO/NFC has made significant progress in fiscal year 2004, most notably in the security of its information technology (IT) systems, our audit disclosed that further improvements are needed. Specifically, OCFO/NFC needs to ensure that security responsibilities are clearly defined, and required background investigations are conducted. We also noted that improvements are needed with general network security, access controls, and application change controls. Until these security areas are addressed, OCFO/NFC faces an increased risk of exposing its systems to improper access.

In our opinion, except for the matters referred to above, the control objectives and techniques identified in exhibit A of this report present fairly, in all material respects, the relevant aspects of OCFO/NFC. Also, in our opinion, except for the matters referred to above, the policies and procedures, as described, were suitably designed to provide reasonable assurance that the remaining control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

Also, in our opinion, except for the matters referred to above, the policies and procedures that were tested, as described in the exhibit, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified were achieved during the period from October 1, 2003, through June 30, 2004. The scope of this engagement did not include tests to determine whether control objectives not listed in exhibit A were achieved; accordingly, we express no opinion on achievement of controls not included in exhibit A.

This information is provided to user organizations of OCFO/NFC and their auditors to be taken into consideration, along with information about the internal control structures at user organizations, when making assessments of control risk for user organizations. The relative effectiveness and significance of specific controls at OCFO/NFC and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of policies and procedures at OCFO/NFC is as of June 30, 2004, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 2003, through June 30, 2004. Any projections of such information to the future are subject to the risk that, because of change, they may no longer portray the system in existence. The potential effectiveness of specific policies and procedures at OCFO/NFC is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. The projections of any conclusions, based on our findings, to future periods are subject to the risk that changes may alter the validity of such conclusions. Furthermore, the accuracy and reliability of data processed by OCFO/NFC and the resultant reports ultimately rests with the user agency and any compensating controls implemented by such agency.

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

Robert W. Young

ROBERT W. YOUNG
Assistant Inspector General
for Audit

June 30, 2004

Findings and Recommendations

Section 1. Security Program Management and Compliance

Finding 1 Further Actions are Needed to Ensure Compliance with Federal Regulations and to Strengthen its Security Management Structure

OCFO/NFC has made significant improvements to comply with Federal regulations; however, we found that OCFO/NFC had not completed certification and accreditation of its major applications and general support systems. Further, we found that OCFO/NFC had not updated its directive and functional statements to clearly define security responsibilities after its 2002 reorganization. Further, OCFO/NFC had not completed all required background investigations for individuals in high-risk positions. OCFO/NFC has continued to make progress in these areas and completed its certification and accreditation by September 30, 2004, in accordance with departmental guidance. Finally, OCFO/NFC planned to initiate a review to evaluate security responsibilities, and continue obtaining security clearances as funds permit. Without clearly defined security responsibilities, and adequate background investigations, OCFO/NFC will not be adequately assured that its security management structure is operating effectively; and thus putting its critical resources at increased risk of loss, misuse, and improper modification.

The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) recognize 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). USDA's Chief Information Officer (CIO) has issued guidance for certifying and accrediting systems, which is based on the NIST[3] requirement that information systems' certification and accreditation be based on risk assessments and security plans.

OMB[4] also requires that security-related responsibilities of offices and individuals throughout the entity should be clearly defined to include those of (1) information resource owners and users, (2) information resources

[3] NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004.

[4] OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.

management and data processing personnel, (3) senior management, and (4) security administrators.

Further, Executive Order No. 10450,[5] as amended, established general requirements that every competitive service position be designated at a risk level commensurate with the public trust responsibilities of the position, and be made subject to investigation. In 1998, OCFO/NFC issued its own directive[6] to implement the background investigation requirements.

Certification and Accreditation of OCFO/NFC General Support Systems and Major Applications Not Yet Completed, as of June 30, 2004

OCFO/NFC had revised its certification and accreditation process in accordance with departmental guidelines, completed risk assessments and security plans for its general support systems and major applications, and begun to perform certifications of its information systems based on its new procedures. However, it had not completed the certification and accreditation of its general support systems and major applications by the end of our fieldwork. Without the necessary security certifications and accreditations, OCFO/NFC could not ensure the secure operations of its information systems; therefore, placing sensitive information at increased risk of loss, misuse, and improper modification, for the period under review.

OCFO/NFC officials informed us that certifications of its general support systems and major applications were completed by September 30, 2004.Security Responsibilities Not Clearly Defined

During fiscal year 2002, OCFO/NFC went through a major reorganization change and some security responsibilities were transferred within the organization. However, we noted that OCFO/NFC had not updated certain procedures to clearly identify security responsibilities and the individuals who were responsible to perform those security functions. When security procedures are not updated to clearly delineate separation of security functions, individuals may misunderstand or improperly implement their security responsibilities and therefore, controls may be inconsistently applied.

Prior to 2002, most security functions at OCFO/NFC were within the Information Systems Policy and Control Staff (ISPCS). In April 2002, OCFO/NFC created the Cyber Security Staff (CSS) to provide overall security guidance and oversight. OCFO/NFC transferred some of the functions such as disaster recovery and security awareness from ISPCS to CSS, while other functions such as preparing security plans and risk assessments were transferred to system owners. However, we found that

[5] Executive Order No. 10450, “Security Requirements for Government Employment,” signed April 27, 1953.

[6] Title VII, Chapter 14, Directive 7, “Risk Levels, Position Sensitivity Descriptions, and Background Investigations for OCFO/NFC and Contractor Personnel”

security responsibilities have not been updated in OCFO/NFC directives, functional statements, and service center description to clearly delineate separation of security functions.

For example, OCFO/NFC had not updated its directives to move the Information Systems Security Project Manager (ISSPM) responsibilities to the Chief of CSS. OCFO/NFC management advised us that the ISSPM designation was made to the Chief of CSS; however, a position in the organization structure has not been created or position description written defining the ISSPM.

OCFO/NFC is currently going through another reorganization. Officials advised us that they would initiate a review to further clarify security responsibilities. OCFO/NFC had already established a team to review the functional and organizational changes and develop individual organizational responsibilities and accountability. Further OCFO/NFC officials informed us that they have requested funding to have an independent assessment of the IT security program to determine the best alignment of security functions according to industry best practices.

Required Background Investigations Not Obtained

While OCFO/NFC has revised its controls to implement the Office of Personnel Management (OPM) requirements for assigning risk levels and performing background investigations, we determined that these controls were not fully operational. Even though progress has been made, we determined that background investigations or reinvestigations within the required timeframe have not been completed for 27 high-risk IT specialist positions.[7] 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.

We obtained a background investigation status report from OCFO/NFC and performed an analysis to determine if progress has been made relating to background investigations. We noted that OCFO/NFC had taken some corrective actions and reclassified positions such as security administrators, system programmers, and application programmers as “high-risk.” In total, OCFO/NFC had classified 131 information system positions as high-risk, compared to only 13 during our prior audit. However, despite this progress, we identified an additional 27 high-risk information system positions that either did not have a background investigation or did not have a reinvestigation within the required 5-year period.[8]

[7] Our review was limited to high-risk IT positions (series 2210) in four divisions of OCFO/NFC.

[8] One of these positions had not had an investigation, and the person had been employed at OCFO/NFC since at least 1990. The other 26 positions had not had a reinvestigation within the required timeframe; several of these 26 positions had an initial investigation from the 1970s.

OCFO/NFC recently updated its procedures for conducting background investigations in a timely manner. OCFO/NFC's goal is to complete as many reinvestigations as funding would permit.

Since we recommended in our prior audit that background investigations be completed in a timely manner and renewed every 5 years for personnel in high-risk positions, we are not making further recommendations.

Recommendation No. 1

OCFO/NFC should update its functional statements, management directives, and any applicable procedures to clearly define and delineate separation of security functions.

Section 2. Mainframe and Network Access Controls

Access controls, such as user identifications (ID) and passwords, protect network applications and data against unauthorized access. Network administrators should provide only authorized users access to network applications and data, and ensure that such access is limited to what is needed to perform the user's job functions. In addition, administrators need to ensure that network devices such as modems and firewalls are properly configured to ensure that access to network resources is protected against unauthorized or malicious access. Without strong access controls, privacy and financial data is subject to loss, disclosure, and unauthorized modification.

Finding 2 Access Controls to Payroll/Personnel Applications and Sensitive Data Requires Improvement

We found OCFO/NFC personnel and some of its clients had access to critical payroll and personnel applications that exceed what was required to perform their job functions. In some instances, the access provided also violated separation of duty controls. This occurred because OCFO/NFC had not adequately restricted access based on job responsibilities or complied with its prescribed guidance to monitor access for all its employees and external users. We also determined that OCFO/NFC had not adequately ensured that access to sensitive client information extracted from these systems was adequately protected from unauthorized disclosure. Inappropriate access increases the vulnerability of OCFO/NFC applications and the payroll/personnel system to fraudulent activity.

OCFO/NFC directives[9] state that OCFO/NFC employees should be granted access authority only to those resources required to carry out their jobs and that the number of employees with authorized access will be limited to the minimum number needed to effectively perform the required functions. OCFO/NFC directives[10] also state that the separation of functions will be used as an internal control to guard against personnel having the opportunity to commit and/or conceal intentional or unintentional alteration, destroy data or software, or view data that is outside the scope of the employees normal job assignments. In addition, if the separation of incompatible functions is not possible, compensating controls must be used.

[9] Title VII, Chapter 11, Management Directive No. 27.

[10] Title VII, Chapter 11, Directive 40.

Access to Payroll and Personnel Applications

We reviewed access reports provided by OCFO/NFC and found the following instances where access to payroll and personnel applications was not adequately restricted based on job responsibility or separation of duties principles:

- We found over 60 individuals at OCFO/NFC that had update access to critical payroll and personnel systems or data without a related job function need. We noted programmers who had access to update production data, individuals who retained update access from a previous assignment, and individuals who obtained update access that only required read access. OCFO/NFC agreed to change all of the inappropriate accesses identified during our review.

- We identified 68 individuals at OCFO/NFC that had the ability to update both payroll and personnel actions, and add positions and update tables within the payroll and personnel systems. This access could have allowed fraudulent transactions to be processed. Further, OCFO/NFC did not have effective compensating controls in place to detect possible fraudulent transactions that could have occurred due to this level of access. OCFO/NFC officials agreed to review these accesses and make changes where possible or implement compensating controls.

- We found users external to OCFO/NFC that had update access to four critical payroll and personnel applications. Having update access to these applications violates separation of duty controls. On one of its critical web-based systems, users both internal and external to OCFO/NFC could initiate incompatible transactions within the same system.

The above instances could have been avoided if OCFO/NFC had (1) adequately maintained access profiles based on job functions and separation of duties principles and (2) established an effective mechanism to periodically review access granted to employees to ensure that it remains consistent with job functions and separation of duties principles. OCFO/NFC directives[11] state that the OCFO/NFC will produce reports for division/staff security coordinators that show the scope of an employee's security access and/or lists of who has access to specific data and that the division/staff security coordinators will distribute monthly access authorization reports to the appropriate branch chiefs. Currently, OCFO/NFC does not periodically distribute reports of applications access, and based on our review, branch chiefs were not reviewing applications

[11] Title VII, Chapter 11, Directive 40.

access on a periodic basis. OCFO/NFC informed us that the ultimate solution to this problem might lie in the reengineering of OCFO/NFC access administration profiles into a role-based process.

Access to Other Sensitive Data

We also reviewed access to certain sensitive client information that had been extracted from payroll and personnel applications and found that that OCFO/NFC had not always adequately protected sensitive information from unauthorized disclosure.

For instance, we found that biweekly download files for one of OCFO/NFC's clients that contained sensitive information protected by the Privacy Act of 1974 had been posted to OCFO/NFC's Download Center, which was designed to contain only non-sensitive information. Consequently, the authentication and monitoring controls over this system were not adequately designed to protect sensitive information. This occurred because information posted to the download center was not controlled and monitored by the system owner.

OCFO/NFC informed us that they had removed the sensitive information from the Download Center and would ensure that the system owner approves all future information. OCFO/NFC also informed us that they are also evaluating the access controls over the Download Center.

Finally, we also found that sensitive information stored in two libraries used to share extracted payroll and personnel information between OCFO/NFC programming and support staff sections and with user organizations was not adequately protected from unauthorized disclosure. Our review disclosed that 603 users had access to sensitive information in one of these libraries, and 424 users had access to sensitive information in the other library. This occurred because, even though some of the files in these libraries contained sensitive information protected by the Privacy Act of 1974, access was generally granted to all files in these libraries regardless of their content.

Recommendation No. 2

Document and implement access profiles based on job responsibilities and separation of duties principles, and establish a process to periodically review user access to ensure that it remains consistent with job functions and separation of duties principles.

Recommendation No. 3

Document adequate justification and develop effective compensating controls for those branches that require update access to applications that violate separation of duty controls.

Recommendation No. 4

Establish controls to ensure that the system owner approves data loaded on the Download Center and access to that data.

Recommendation No. 5

Restructure access controls over the libraries used to share information extracted from OCFO/NFC payroll and personnel systems to provide greater protection of sensitive information.

Finding 3 Network Security and Monitoring Efforts Need Improvement

OCFO/NFC had not ensured that modems on its network were adequately tracked or properly secured, that its firewall configurations were appropriately maintained, or that logs were periodically reviewed on its Web and Unix servers. This occurred because OCFO/NFC had not established adequate controls or complied with its own guidelines to monitor and secure these critical network resources. As a result, OCFO/NFC's network is at unnecessary risk of intrusion and unauthorized access that may not be detected in a timely manner.

Modem Security

OCFO/NFC could not be adequately assured that its modems were properly secured. This occurred because OCFO/NFC's policies and procedures for tracking, detecting, and properly securing modems were inadequate and not always being followed by personnel. Modems pose a serious security risk because they provide "back door" points of entry into OCFO/NFC's network and bypass central protective devices such as the firewall. Potential attackers can use an unsecured modem to obtain unauthorized access to OCFO/NFC network and systems.

Departmental Regulations (DR)[12] require agencies to evaluate security measures in place on network gateways. Further, OCFO/NFC[13] established its own policy outlining responsibilities and procedures for requesting telephone lines for phones, fax machines, and modems. This directive requires a fax or modem request form be submitted for approval along with a description of how the modem would be secured. This directive also requires OCFO/NFC to maintain information regarding each request and assignment of phone numbers in a database, and requires that OCFO/NFC annually verify that modems are still needed.

In 2003, we reported[14] that OCFO/NFC had established procedures to identify active modem lines, but had not evaluated the security measures in place to ensure that modem phone lines were properly protected. In response, OCFO/NFC informed us that they had revised existing procedures to ensure that all modems are identified, properly secured, and reviewed on a monthly basis. However, since May 2003, OCFO/NFC performed only 2 evaluations. Further, we found that OCFO/NFC revised its procedures to only identify modems that were available during non-business hours. Consequently, only 12 modems phone lines were identified in its May/June 2004 evaluation while 76 were identified in its May 2003 evaluation when business hours were not specifically excluded. Finally, OCFO/NFC had not instituted a process to ensure that identified modems were properly secured.

We also reviewed the results of OCFO/NFC's evaluations and compared the results to its database of modems. We verified that OCFO/NFC had properly secured those modems. While none of the modems we selected had been improperly secured, we found that 2 of the 12 modem lines identified in one of its evaluations were not in the modem database. Further, we found modems in the database that were no longer needed or assigned to staff that had been relocated, reassigned, retired, or deceased. This occurred because users were not reporting changes needed to modem lines to the responsible unit of OCFO/NFC, and OCFO/NFC had not begun its annual review process. Two of these lines were deleted/disconnected from the phone system as the result of our inquiry.

In addition, we found that OCFO/NFC had not always maintained the proper authorizations for the modems in its database. We requested authorization forms for the first 10 modems on the database listing. However, OCFO/NFC had only three authorizations on file. Officials told us that the remaining seven were considered as "grandfathered-in" because they were in service prior to March 2001 when OCFO/NFC issued its telephone and fax/modem directive.

[12] DR 3140-1, "USDA Information System Security Policy," dated May 15, 1996.

[13] Management and Administrative Directives Manual, Chapter 12, "Telecommunications Management," Directive 2, "Requesting Telephone and Fax/Modem Lines", dated March 5, 2001.

[14] Audit Report No. 11401-15-FM, "Fiscal Year National Finance Center Review of Internal Controls," dated November 2003.

Firewall Documentation and Configuration Management Need Improvement

OCFO/NFC had not formally documented or adequately maintained support for its firewall configurations. This occurred because OCFO/NFC had not implemented a formal configuration management process for its firewalls. We also identified rules that were no longer needed but remained in the system because OCFO/NFC was not periodically reviewing its firewall configurations. As a result, OCFO/NFC does not have adequate assurance that its firewalls are properly configured.

NIST[15] and USDA's CIO[16] require that firewall rules be documented and periodically reviewed to ensure their accuracy. We found that OCFO/NFC was unable to provide supporting documentation for 15 of 17 firewall system rules selected for review. We also identified certain firewall rules that were no longer needed.

We also found that OCFO/NFC did not use a formal change control process for changing firewall rules. Officials informed us that the approval of changes to the firewall configuration occurs informally through e-mail. Maintaining supporting documentation in a personal e-mail account is not an efficient and effective system because generally only the account holder has access to the documentation, and does not ensure that all the appropriate personnel are made aware of the change. Without a formal change control process over its firewalls and conducting periodic reviews, OCFO/NFC cannot be assured that its firewalls are configured effectively, unnecessarily putting its network resources at risk of intrusion.

OCFO/NFC System Security Monitoring for Webservers and UNIX Servers Needs Improvement

OCFO/NFC had not adequately monitored user activity for security purposes on Webservers[17] and UNIX systems. This occurred because OCFO/NFC did not have a process in place to perform routine monitoring of these systems. The lack of a formal monitoring process reduces the possibility that security incidents involving Webservers or UNIX systems will be detected and corrected in a timely manner.

NIST[18] recognizes that routinely monitoring access can help identify significant problems and deter users from inappropriate and unauthorized activities. Because the volume of security information is likely to be too voluminous to review routinely, the most effective monitoring efforts are those that selectively target specific actions. These automated monitoring

[15] NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy," dated January 2002.

[16] Cyber Security Policy, CS-012, "Gateway and Firewall Technical Security Standards," dated January 22, 2002.

[17] These servers are the front-end interface servicing user's web/internet requests. These servers may use database connections to backend database but do not have database residing on them.

[18] NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," dated October 1995.

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.

Although OCFO/NFC had enabled logging[19] on its Web and UNIX systems and reviewed those logs as part of a security incident investigation, OCFO/NFC officials told us that they had not regularly generated system monitoring reports that would reveal suspicious access activity on these systems. OCFO/NFC recognized that this lack of monitoring was a security weakness and planned to implement monitoring software to correct this weakness.

Recommendation No. 6

Resume identifying modem phone lines during business hours, expand current procedures to ensure that the modems identified are adequately secured, survey its organizations to identify modems that are currently in use and authorized and update the database accordingly, and establish a process to annually verify that faxes/modems are still needed.

Recommendation No. 7

Document the current firewall configuration, establish a formal configuration change management process for the firewall, and perform periodic reviews of the firewall configuration.

Recommendation No. 8

Identify sensitive system resources that should be included in its active monitoring process; develop, test, and document system reports used in its monitoring process; and identify and document the types of unusual activity on these reports that should be investigated, for Webservers and UNIX systems.

[19] Recording of events made by a particular software package.

Finding 4 Application Software Change Controls Need Improvement

Despite prior recommendations,[20] we found that OCFO/NFC needs to strengthen its controls over application changes. Although NFC was documenting application software change requests and approvals, we found that OCFO/NFC needs to ensure that it (1) completes documentation of application change testing, (2) performs user acceptance testing on mandated application software changes, (3) obtains users' approval of application software requirements, and (4) notifies users of emergency changes for subsequent review. OCFO/NFC is currently in the process of implementing a new standardized change management system and process to support application changes. Despite its own policies to document approval and testing, OCFO/NFC was not adequately enforcing its established guidance. Until these issues are addressed, OCFO/NFC will face increased risk that application software changes may not meet user needs, not operate as intended, or cause unforeseen adverse impacts on the application.

To determine if application software changes were adequately documented, approved, and tested, we selected 25 of the 1,182 non-emergency changes and 15 of the 51 emergency changes to applications that were implemented between October 1, 2003, and March 31, 2004. The following summarizes the results of our review:

<u>Testing of Application Software Changes</u>

OCFO/NFC was unable to provide adequate documentation for 16 of the 25 non-emergency changes, and 8 of the 15 emergency changes we reviewed. Therefore, we could not determine if OCFO/NFC adequately tested application software changes. OCFO/NFC guidance for application software testing states that the programmer or project leader of an application change request must develop test plans and test results to reasonably ensure that proposed changes would function properly. These test plans and results must be maintained in the project folder.

OCFO/NFC officials informed us that they had begun using a contractor in one division to develop unit test plans for non-emergency changes to its payroll applications, and that they would begin enforcing this requirement for other applications and emergency changes. In addition, OCFO/NFC is in the

[20] Audit Report No. 11401-9-FM, "Selected Information Technology General Controls At The National Finance Center Need Strengthening," dated March 2002; Audit Report No. 11401-15-FM, "Fiscal Year 2003 National Finance Center Review of Internal Controls," dated November 2003.

process of implementing procedures for performing biweekly system testing for its payroll and personnel systems.

Acceptance Testing on Mandated Application Changes

OCFO/NFC officials informed us that acceptance testing was not performed for any of the 25 mandated changes that we reviewed. In addition, OCFO/NFC had not obtained waivers from users, development/maintenance organization, quality assurance staff, or other technical personnel. OCFO/NFC officials informed us that most of their systems are on a biweekly release schedule, which does not provide enough time to conduct formal user acceptance testing. As a result, OCFO/NFC faces increased risks that application changes will not meet user requirements or operate as intended.

The OCFO/NFC Scheduled Software Maintenance Directive[21] states that acceptance testing is required for mandated changes unless a waiver is approved by the users, development/maintenance organization, the quality assurance staff, and other technical personnel after a review of the development/maintenance organization's software testing. However, development organization testing guidance provides conflicting information on when acceptance testing is required.

OCFO/NFC informed us that it intends to include customer representatives in the system testing in the future.

User Review of Software Requirements and Other Application Changes

We found that OCFO/NFC had documented system requirements for 20 of the 25 non-emergency changes that we reviewed, but had not obtained user approval of these software requirements for any of these 20 changes. This occurred because OCFO/NFC was not complying with its own guidance that requires user sign-off on these system requirements. As a result, OCFO/NFC cannot be adequately assured that proposed changes meet user requirements.

The NFC's Application System Life Cycle[22] states that any modification, reconfiguration, or redevelopment would include user review of functional requirements. While OCFO/NFC had developed a template to guide the development of software requirements documents, officials stated that software requirement documents are at the discretion of the programmer and are not required. Each software requirement document must have a sign-off sheet, which documents approval by OCFO/NFC officials and a customer representative.

[21] Title VII, Chapter 11, Directive 47, Scheduled Software Maintenance (Revision 2), November 14, 2003

[22] Title VII, Chapter 11, Directive 48, Application System Life Cycle (Revision 2), November 14, 2003

We also found that OCFO/NFC had not established a process to notify the designated customer representative of emergency changes for subsequent review. OCFO/NFC officials informed us that they had begun meeting with the customer representative for one of its systems on a bi-weekly basis to discuss emergency changes, and would begin a similar process for the other applications.

Recommendation No. 9

Develop a process to ensure that adequate testing has been performed and properly documented by the development organization before its approving official signs the change request.

Recommendation No. 10

Establish controls to ensure that acceptance testing is performed or a waiver is obtained prior to implementation for all mandated changes.

Recommendation No. 11

Establish controls to ensure that software requirements for application modifications, reconfigurations, and redevelopments are properly documented and approved by a customer representative.

Exhibit A – Office of Inspector General, Review of Selected Controls

The objectives of our examination were to perform testing necessary to express an opinion about (1) whether the control objectives and techniques identified in this exhibit present fairly, in all material respects, the aspects of the Office of the Chief Financial Officer (OCFO) National Finance Center (OCFO/NFC)'s policies and procedures in place from October 1, 2003, through June 30, 2004, (2) whether the control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily, and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

This report is intended to provide users of OCFO/NFC with information about the control structure policies and procedures at OCFO/NFC that may affect the processing of user organizations' transactions and to provide users with information about the operating effectiveness of the policies and procedures that were tested. This report, when combined with an understanding and assessment of the internal control structure policies and procedures at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations' financial statements, and (2) in assessing control risk for assertions in user organizations' financial statements that may be affected by policies and procedures at OCFO/NFC.

Our testing of OCFO/NFC's control structure policies and procedures was restricted to the control objectives and the related policies and procedures listed in the matrices in this exhibit. Our testing was not intended to apply to any other procedures not included in the aforementioned matrices or to procedures that may be in effect at user organizations.

Our review was performed through inquiry of key OCFO/NFC personnel, observation of activities, examination of relevant documentation and procedures, and tests of controls. We also followed up on known control weaknesses identified in prior OIG audits. We performed such tests as we considered necessary to evaluate whether the operating and control procedures described by OCFO/NFC and the extent of compliance with them are sufficient to provide reasonable, but not absolute, assurance that control objectives are achieved.

The description of the tests of operating effectiveness and the results of those tests are included in the following section of this report.

Control Objective	Control Techniques	Tests Performed	Conclusions
1. Ensure the necessary controls are in place to mitigate and/or reduce the potential for fraud, waste, and abuse of IT information assets.	1. Implement and maintain an effective security program by assuring: a. Risk assessments are performed. b. Security plans are developed and maintained. c. Policies and procedures to reduce risks are implemented. d. Periodic security awareness training is provided. e. Testing and evaluation of plans, procedures, and security controls are conducted. f. Security incident response capability is maintained.	Verified that OCFO/NFC had developed risk assessments and security plans for its major applications and general support systems. Reviewed the departmental guidelines for certification and accreditation for general support systems and major applications. Obtained security awareness database as of end of fiscal year 2003 and performed analysis to determine the number of employees who did/did not take the security awareness training. Reviewed NIST SP 800-18. Reviewed control self assessments for OCFO/NFC business units. Interviewed OCFO/NFC officials and reviewed NFC Directives.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and operating effectively, except as noted below. OCFO/NFC had revised its certification and accreditation process in accordance with departmental guidelines. However, it had not completed the certification and accreditation of its general support systems and major applications for the period under review. The C&As were completed by September 30, 2004. (See Finding No. 1.)
2. Ensure that reimbursement agreements developed between NFC and user agencies for provision of services and cost development are accurate.		Selected a sample of Memorandum of Understandings (MOU) for two agencies.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and were operating effectively.
3. Ensure that requirements for information systems are developed, documented, and maintained and that they satisfy user needs.	a. Develop requirements documentation that is in compliance with Title VII, Chapter 11, Directive 48, Application System Life Cycle. b. Submit requirements package to the user for feedback and prepare adjustments to the package, if necessary. c. Obtain user sign off on requirements packages, when appropriate.	Interviewed OCFO/NFC personnel and reviewed applicable directives and procedures. Selected and reviewed mandated application changes that were implemented between October 1, 2003, and March 31, 2004.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and were operating effectively, except as noted below. OCFO/NFC was not obtaining user approval of software requirements. We found that OCFO/NFC had documented system requirements for 20 of the 25 non-emergency changes that we reviewed, but had not obtained user approval of these software requirements for any of these 20 changes. (See Finding No. 4.)

Control Objective	Control Techniques	Tests Performed	Conclusions
4. Ensure that NFC's application software systems are developed to minimize invalid, lost, or corrupted data, and to maintain data security and integrity.	a. Established, as dictated by requirements documentation and/or users' requests, systems checks, and edits to verify the validity of data processed in and interfaced between NFC systems. b. Restrict developer access to data on an "as needed" basis. c. Adhere to acceptable standard development practices for specifications, coding, security, and testing of software at each phase along the development lifecycle. d. Adhere to NFC's policy for software configuration control as documented by ISPCS.	Observed OCFO/NFC personnel process. Reviewed OCFO/NFC procedures for the selected applications. T&A's, reviewed access reports for Table Management System.. Selected and reviewed mandated application changes that were implemented between October 1, 2003, and March 31, 2004. Randomly selected emergency application changes implemented between October 1, 2003, and March 31, 2004. Interviewed responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and operating effectively, except as noted below. OCFO/NFC officials told us that acceptance testing is performed for all application changes that are classified as routine; however, we found that OCFO/NFC was not performing acceptance testing application changes that are classified as mandated. (See Finding No. 4.) We also found that OCFO/NFC had not sufficiently documented the software testing for the application change requests. Consequently, we could not always determine if adequate testing had occurred. (See Finding No. 4.) We noted that individuals at OCFO/NFC had update access to applications that was not within the scope of their job function. (See Finding No. 2.)

Control Objective	Control Techniques	Tests Performed	Conclusions
5. Ensure that entries added to table management are valid and comply with Treasury, OPM, and other applicable Government regulations and management policies to minimize errors, fraudulent entries, and unauthorized data.	a. Restrict access to specific personnel to process, add, change, or delete data in table management to minimize possible adverse impact on processing.	Reviewed access reports for the Table Management System. Made inquiries to responsible OCFO/NFC programmers. Reviewed applicable OCFO/NFC directives.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation but not operating effectively. The table management application has controls in place to prevent inappropriate updates to the tables; however, we found individuals at OCFO/NFC had access to critical Payroll/Personnel Systems that was not within the scope of their job function. (See Finding No. 2.)
6. Ensure that time and attendance documents (T&A’s)are received and processed timely, accurately, and according to Government regulations.	a. Ensure accuracy, validity of the information, and compliance with regulations. b. Verify the receipt and status of agency contact and running of T&A reports. c. Correct and reprocess suspended T&A's. Research multiple employee T&As, to identify the block, batch, and sequence number of the suspended T&As. Correct duplicate T&As to ensure that each employee is paid only once for the current pay period. Establish a Special Payroll Processing System record for an indebtedness and/or death case if T&A is marked final or termination action applies.	Reviewed relevant application documentation and made inquiries of system programmers. Reviewed various payroll/personnel exception reports. Observed OCFO/NFC processing of T&A's. Reviewed OCFO/NFC procedures for correcting T&A's and other relevant directives. Reviewed relevant system reports. Made inquiries to responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and operating effectively.

Control Objective	Control Techniques	Tests Performed	Conclusions
7. Ensure that manually processed salary payments are accurate and timely, and comply with regulations.	a. Assign Form AD-343, Payroll Action Requests, Document Tracking System External, Special Payroll Processing System, Quick Service Wires, or other requests for manual payments promptly to unit accounting technicians, payroll technicians, and clerks to ensure timely processing in Special Payroll Processing System.	Reviewed Federal guidelines regarding need for unique login identifiers. Reviewed criteria for AD343 authorizations. Compared list of Special Payroll Process System transactions to list of those authorized to process AD343s for one agency. Reviewed OCFO/NFC reports designed to identify employees updating their own payroll and personnel transactions. Made inquiries to responsible OCFO/NFC personnel.	The control structure policies and procedures were not suitably designed to achieve the control objective specified. We found access control weaknesses that violate separation of duties controls, and excessive access that was not needed to perform the user's job functions. Also, we found weak access controls over OCFO/NFC's Download Center. (See Finding No. 2.)
8. Ensure that new and current clients are adequately trained to effectively and efficiently use the applicable NFC system, including electronic access applications.	a. Provide comprehensive user training on applicable system applications.	Reviewed application documentation for applicable systems. Made inquiries to responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and were operating effectively.

Control Objective	Control Techniques	Tests Performed	Conclusions
9. Ensure that NFC systems, including new and revised electronic systems, are user friendly.	a. Review recommendations for modifications to screen designed and/or data field names to ensure ease of operations, user friendliness, and consistency with other screens and/or systems.	Reviewed OCFO/NFC procedures for the selected applications. Tested and evaluated the software used to input payroll/personnel information. Made inquiries to responsible OCFO/NFC personnel. Interviewed timekeepers.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and were operating effectively.
10. Ensure Individual Development Plans (IDPs) are properly developed and executed in compliance with applicable laws, regulations, and policies.	a. Prepare IDPs in accordance with NFC Directives. b. Assess needs of employees to determine training required to successfully perform present duties. c. Provide employees with activities to enhance their skills so that they may perform and advance to their highest potential.	Obtained training records for a sample of employees with significant security responsibilities. Reviewed training records to determine whether training was adequate.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and operating effectively.

Control Objective	Control Techniques	Tests Performed	Conclusions
11. Ensure that all OCFO/NFC and contractor personnel have the appropriate position sensitivity codes, clearances, and background investigations as directed by USDA, OPM, and OMB guidelines.	a. Obtain appropriate background checks or investigations for selected/appointed individuals prior to their being placed in the designated position. b. Monitor suspense dates for completed investigations for high-risk positions to ensure that investigative actions are taken within 30 days of the 5-year anniversary.	Obtained a status report and performed an analysis to determine whether if progress had been made relating to the background investigations and reinvestigations cited in the fiscal year 2003 General Controls report.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation but not fully operating effectively. We identified 27 high-risk computer/information systems positions that either did not have a background investigation or did not have a re-investigation within the required 5-year period. (See Finding No. 1.)
12. Develop and maintain an effective IS security program in compliance with OMB Circular A-130, Departmental Regulation (DR) 3140, FIPS, FISMA, and NIST.	a. Control access to IS resources.	Interviewed responsible OCFO/NFC personnel, reviewed rules for firewall system, and evaluated supporting documentation for selected rules. Performed vulnerability assessments on selected servers and network devices. Reviewed applicable OCFO/NFC policies and procedures.	The control structure policies and procedures were not suitably designed to achieve the control objective specified. OCFO/NFC has made significant improvements to comply with Federal regulations; however, we found that OCFO/NFC had not updated its directive and functional statements to clearly define security responsibilities after its 2002 reorganization. Finally, OCFO/NFC had not completed all required background investigations for individuals in high-risk positions. OCFO/NFC had not ensured that modems on its network were adequately tracked or properly secured, that its firewall configurations were appropriately maintained, or that logs were periodically reviewed on its Web and Unix servers. (See Finding Nos. 1 and 3.)

Control Objective	Control Techniques	Tests Performed	Conclusions
13. Ensure adequate testing of new and modified applications.	a. Develop system testing procedures and standards as specified in NFC directives that include: 1) Testing prior to implementation of new and modified applications and scheduled releases. 2) Use of comprehensive test data and nonproductive copies of live files. 3) Participation by users and other groups involved with the application, including preparation of test data by users. 4) Testing various combinations of conditions, realistic volumes, and infrequent processing. 5) Testing the application's interface with other systems. 6) Providing for review and approval of test results by users and developers prior to moving into production. 7) Develop and implement acceptance testing plans in accordance with NFC standards prior to placing in production. 8) Document results of acceptance tests and resolve problem areas.	Interviewed OCFO/NFC personnel and reviewed applicable directives and procedures. Selected and reviewed application changes that were implemented between October 1, 2003, and March 31, 2004. Selected and reviewed emergency application changes implemented between October 1, 2003, and March 31, 2004.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation but were not operating effectively. We found that OCFO/NFC had documented system requirements for 20 of the 25 non-emergency changes that we reviewed, but had not obtained user approval of these software requirements for any of these 20 changes. We found that OCFO/NFC had not performed acceptance testing for application changes that are classified as mandated. (See Finding No. 4.)

Control Objective	Control Techniques	Tests Performed	Conclusions
14. Ensure that program changes are authorized and accurately implemented to reduce the potential for errors or irregularities.	a. Establish an independent quality assurance group to process program changes to ensure program integrity. b. Develop and implement a formal procedure for transferring new and modified application programs into production libraries. c. Produce reports of program changes and provide the reports for management review upon request. d. Maintain a history of program changes in accordance with General Services Administration retention schedule.	Reviewed system documentation for OCFO/NFC library management software and change control system. Interviewed responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and were operating effectively.
15. Ensure that application programs and related documentation are physically and logically secure.	a. Maintain a program library management software system to restrict update access to production versions of application modules to a designated group of authorized individuals. b. Deny developers update access to production programs.	Obtained and reviewed access reports for the OCFO/NFC mainframe production program source code, load and procedure libraries.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and were operating effectively.

Control Objective	Control Techniques	Tests Performed	Conclusions
16. Ensure that access to online systems is controlled.	a. Define and implement policies and procedures for issuing user ID and password administration. b. Develop security which restricts access to defined data and programs that are necessary to perform a specific job function. c. Reports of incidents of suspected inappropriate access are produced and reviewed. d. Monitor user activity and provide reports to management for inactive accounts. e. Provide access through secure connectivity with approved security form.	Reviewed the mainframe security software control options that impact password administration. Also, tested selected servers for certain password vulnerabilities. Requested and obtained listings of user IDs from OCFO/NFC and selected client agencies to determine whether user IDs were granted only to employees whose job responsibilities required such access. Reviewed access reports for selected applications and a sensitive dataset file to identify individuals granted inappropriate access and separation of duty based on their job function. Reviewed monitoring reports and procedures. Obtained a file of mainframe user IDs that included the date of last use and identified user IDs that had not been used in more than 150 days. Reviewed the results of a commercially available software product that was used by OCFO/NFC to identify security risks posed by modems, compared the modems identified to the modems database, and verified that the identified modems were properly secured. Interviewed responsible OCFO/NFC personnel for selected activities and functions reviewed.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation but not operating effectively. We found individuals within OCFO/NFC and external to OCFO/NFC with access to update personnel/payroll applications although their current job function did not require access. We found individuals with access that violated separation of duty controls. (See Finding No. 2.) We found some OCFO/NFC staff that had access to confidential data that exceeds what was required to perform their job duties. (See Finding No. 2.) OCFO/NFC had not ensured that modems on its network were adequately tracked or properly secured, that its firewall configurations were appropriately maintained, or that logs were periodically reviewed on its Web and Unix servers. . (See Finding No. 3.)

Control Objective	Control Techniques	Tests Performed	Conclusions
17. Ensure that access to data is controlled to minimize unauthorized access.	a. Provide access to sensitive or critical data only when needed for processing.	Reviewed monitoring reports, and applicable procedures. Reviewed identification/authentication for selected applications and the Download Center. Obtained and reviewed a copy of the files on the Download Center. Reviewed access reports for one sensitive dataset file used to store sensitive data when submitted to the OCFO/NFC for processing. Interviewed responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation but were not operating effectively. OCFO/NFC is not adequately controlling the accesses to the systems we selected for review. (See Finding No. 2.) We found some users within OCFO/NFC and external to OCFO/NFC that had update access to selected applications although their current job function did not require such access. In some instances, the access violated separation of duty controls. (See Finding No. 2.) We found that there were inadequate access controls to the Download Center, which could lead to the disclosure of sensitive information covered by the Privacy Act of 1974. (See Finding No. 2.)

Control Objective	Control Techniques	Tests Performed	Conclusions
18. Ensure that NFC provides security, confidentiality, integrity, and availability of software and data on mainframe and personal computers.	a. Inform employees of the ADP security program and their responsibilities.	Reviewed OCFO/NFC organization chart, security directives, functional statements and made inquiries to OCFO/NFC personnel to determine actual procedures in place. Reviewed applicable OMB and FISMA requirements.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation to ensure confidentiality but not operating effectively. We found that the security responsibilities are not accurately assigned because the responsibilities have not been updated to reflect organizational changes. Furthermore, security responsibilities are not clearly defined in some OCFO/NFC directives and functional statements because procedures at OFCO/NFC have not been updated to clearly delineate security functions. (See Finding No. 1.) We found some users within OCFO/NFC and external to OCFO/NFC that had update access to selected applications although their current job function did not require such access. In some instances, the access violated separation of duty controls. (See Finding No. 2.)

Control Objective	Control Techniques	Tests Performed	Conclusions
19. Ensure that access to resources and records is limited to authorized individuals, and accountability for custody and use of resources is assigned and maintained.	a. Maintain adequate segregation of duties to prevent an individual from performing two or more incompatible functions.	Reviewed compensating controls for separation of duties for individuals who had access to process transactions on one critical application.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had placed in operation but were not operating effectively. We found OCFO/NFC personnel and some of its clients had access to critical payroll and personnel applications that exceed what was required to perform their job functions. In some instances, the access provided also violated separation of duty controls. (See Finding No. 2.)
20. Ensure that sensitive data that contain personal identifiers are adequately protected in compliance with the Privacy Act and Directive 55.	a. Verify that access to items or reports containing personal identifiers is restricted to only authorized persons who need the data to perform their job functions.	Reviewed data backup files. Reviewed OCFO/NFC procedures and directives relating to privacy act and confidentiality. Reviewed OMB guidance relating to privacy. We requested and obtained listings of user IDs from OCFO/NFC and selected client agencies to determine whether user IDs were granted only to employees whose job responsibilities required such access. Made inquiries to responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation and not operating effectively. We found that some OCFO/NFC personnel have access to confidential data that exceeds that is required to perform their job duties. (See Finding No. 2.)