U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Fiscal Year 2007 – Office of the Chief Financial Officer/National Finance Center General Controls Review

Report No. 11401-26-FM
September 2007

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 27, 2007

REPLY TO
ATTN OF: 11401-26-FM

TO: Charles R. Christopherson, Jr.
Chief Financial Officer
Office of the Chief Financial Officer

THROUGH: Kathleen A. Donaldson
Audit Liaison Officer
Office of the Chief Financial Officer

FROM: Robert W. Young /s/
Assistant Inspector General
for Audit

SUBJECT: Fiscal Year 2007 – Office of the Chief Financial Officer/National Finance Center General Controls Review

This report presents the results of our review of internal controls at the Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) for fiscal year 2007. The audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and American Institute of Certified Public Accountants Professional Standards AU Sections 316, 319, and 324, as amended by applicable Statements on Auditing Standards (SAS), which are commonly referred to as a SAS 70 audit. While OCFO/NFC has continued to improve its internal controls, the report contains a qualified opinion because certain control policies and procedures, as described in the report, had not consistently operated effectively from July 1, 2006, through June 30, 2007. As of August 30, 2007, OCFO/NFC had corrected or was in the process of correcting the exceptions we identified.

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 the 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.

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

Executive Summary

Fiscal Year 2007 – Office of the Chief Financial Officer/National Finance Center General Controls Review (Audit Report No. 11401-26-FM)

Results in Brief

This report presents the results of our review of internal controls at the U.S. Department of Agriculture's Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) for fiscal year 2007. While OCFO/NFC had continued to improve its internal controls, this report contains a qualified opinion because OCFO/NFC controls had not operated effectively to ensure that certain access control, awareness and training, audit and accountability, configuration management, contingency planning, and personnel security objectives were consistently achieved from July 1, 2006, through June 30, 2007. As of August 30, 2007, OCFO/NFC had corrected or was in the process of correcting the exceptions identified. The results of our tests and corrective actions taken by OCFO/NFC are described in exhibit B.

Our objectives were to perform procedures necessary to express opinions about whether (1) OCFO/NFC's description of controls in exhibit A presents fairly, in all material respects, the aspects of OCFO/NFC controls that may be relevant to a customer agency's internal control as it relates to an audit of financial statements; (2) the controls included and/or referenced were placed in operation and suitably designed to achieve the associated control objectives, if those controls were complied with satisfactorily, and customer agencies applied the controls specified in exhibit A; and (3) the controls we tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the associated control objectives were achieved during the period from July 1, 2006, through June 30, 2007.

Our audit disclosed that OCFO/NFC's description of controls presented fairly, in all material respects, the relevant aspects of OCFO/NFC controls. Also, in our opinion, the controls included and/or referenced in the description, as updated, were suitably designed to provide reasonable assurance that associated control objectives would be achieved if the described policies and procedures were complied with satisfactorily and customer agencies applied the controls specified in the OCFO/NFC description of controls.

Recommendations In Brief

OCFO/NFC corrected or was in the process of correcting the exceptions we identified. Consequently, we are not making additional recommendations.

Abbreviations Used in This Report

C&A	certification and accreditation
COOP	Continuity of Operations Plan
DRP	Disaster Recovery Plan
GESD	Government Employees Services Division
GSS	general support system
HRMS	Human Resources Management Staff
ID	identification
ISSO	Information System Security Office
ITSD	Information Technology Services Division
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
PMSO	Position Management System
PSD	Position Sensitivity Designation
SETS	Security Entry and Tracking System
SRM	security requirements matrix
SSP	system security plans
ST&E	security test and evaluation
USDA	United States Department of Agriculture

Table of Contents

Report of the Office of Inspector General

TO: Charles R. Christopherson, Jr.
Chief Financial Officer
Office of the Chief Financial Officer

We have examined the control objectives and techniques identified or referenced in exhibit A for the U.S. Department of Agriculture's Office of the Chief Financial Officer/National Finance Center (OCFO/NFC). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of OCFO/NFC controls that may be relevant to a customer agency's internal control as it relates to the audit of financial statements; (2) the controls included or referenced in the description had been placed in operation as of June 30, 2007; and (3) such controls were suitably designed to achieve the associated control objectives, if those controls were complied with satisfactorily and customer agencies applied the controls specified in the OCFO/NFC description of controls. The control objectives were specified by the National Institute of Standards and Technology.

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.

OCFO/NFC continued to improve its internal controls. However, certain access control, awareness and training, audit and accountability, configuration management, contingency planning, and personnel security objectives, as described in exhibit B, were not consistently achieved from July 1, 2006, through June 30, 2007. As of August 30, 2007, OCFO/NFC had corrected or was in the process of correcting the exceptions we identified.

In our opinion, OCFO/NFC's description of controls in exhibit A presents fairly, in all material respects, the relevant aspects of OCFO/NFC controls that had been placed in operation as of June 30, 2007. Also, in our opinion, the controls included and/or referenced in exhibit A, as updated, were suitably designed to provide reasonable assurance that the related control objectives would be achieved if the described controls were complied with satisfactorily and customer agencies applied the controls specified in the OCFO/NFC description of controls.

In addition, we performed tests to obtain evidence regarding the effectiveness of OCFO/NFC policies and procedures in meeting the controls included and/or referenced in exhibit A. The specific controls and the nature, timing, extent, and results of our tests are identified in exhibit B. This information has

been provided to customer agencies and their auditors to be taken into consideration, along with information about the internal control at customer agencies, when making assessments of control risk for customer agencies. In our opinion, except for the matters referred to above, the controls we tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the associated control objectives were achieved during the period from July 1, 2006, through June 30, 2007.

The relative effectiveness and significance of specific controls at OCFO/NFC and their effect on assessments of control risk at customer agencies are dependent on their interaction with the controls and other factors present at individual customer agencies. We did not evaluate the effectiveness of controls at individual customer agencies.

The description of controls at OCFO/NFC is as of June 30, 2007, and information about tests of the operating effectiveness of specific controls covers the period from July 1, 2006, through June 30, 2007. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at OCFO/NFC is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, 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. Finally, the accuracy and reliability of data processed by OCFO/NFC and the resultant reports ultimately rests with the customer 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.

/s/

Robert W. Young
Assistant Inspector General
for Audit

August 30, 2007

UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE CHIEF FINANCIAL OFFICER
NATIONAL FINANCE CENTER

DESCRIPTION

OF THE

INTERNAL CONTROL STRUCTURE

AS OF JUNE 30, 2007

Pages 4 through 19 are not being publicly released due to
the sensitive security information they contain.

Exhibit B – Office of Inspector General - Review of Selected Controls

This exhibit describes the results of our tests of operating effectiveness for the Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) controls specified and/or referenced in exhibit A. It is intended to provide customer agencies with information about OCFO/NFC control structure policies and procedures that may affect the processing of customer agency transactions and the operating effectiveness of the policies and procedures we tested. This report, when combined with an understanding and assessment of the internal control structure policies and procedures at customer agencies, is intended to assist customer agency auditors in (1) planning the audit of customer agency financial statements, and (2) in assessing control risk for assertions in customer agency financial statements that may be affected by OCFO/NFC control structure policies and procedures.

Our review was conducted through inquiry of key OCFO/NFC personnel, observation of activities, examination of relevant documentation and procedures, and other tests of controls. We also followed up on known control weaknesses identified in prior Office of Inspector General audits. We performed such tests as we considered necessary to evaluate whether operating and control procedures established by OCFO/NFC and the extent of compliance with them were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved. Our testing was not intended to apply to any procedures not included in this exhibit or to procedures that may be in effect at customer agencies.

The following table presents the control objectives specified by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, issued March 2006, related control activities established by OCFO/NFC, a description of our tests to determine if OCFO/NFC controls were operating with sufficient effectiveness to achieve the specified control objectives, and the results of those tests.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
1. Access Control Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	For OCFO/NFC employees, the network security policy states that individuals will be provided the least amount of access (within a defined role) necessary to perform his/her job and that access will be granted in accordance with OCFO/NFC management directives regarding data security access and internal controls for access to data and software. These management directives reiterate that OCFO/NFC employees will be authorized access only to the resources needed to perform his/her jobs and require separation of functions to guard against personnel having the opportunity to commit and/or conceal intentional or unintentional alteration, or destroy data or software. The data security access policy also refers to the OCFO/NFC role based security access policy for users that have been implemented into role-based security. Another OCFO/NFC management directive requires access to highly controlled resources, such as production data, special system software, special system and database utilities, etc., to be limited to staff members with an ongoing need. The OCFO/NFC role based security access policy assigns responsibilities and establishes procedures for requesting and maintaining role-based access. Desk procedures referred to by the role-based security directive specify procedures for adding and modifying access roles based on the OCFO/NFC security access form (NFC-1106) and a security requirements matrix (SRM) that is completed by the role owner and approved by the appropriate resource owners. The OCFO/NFC security access form is also used to add or remove users from access roles and delete access roles that are no longer needed. In addition, the role-based security access procedures contain requirements for reviewing all users assigned to each role annually and all resources assigned to each role every three years.	We randomly selected 30 of the 4,690 mainframe user identifications (ID) created from October 1, 2006, through May 1, 2007, for review to determine if the accounts had been appropriately authorized and the access granted had been restricted to that authorized by a security officer. We randomly selected 30 of the 165 Government Employees Services Division (GESD) and Human Resources Management Staff (HRMS) access roles defined as of June 18, 2007, for review to determine if access had been authorized and appropriately restricted to prevent users from having all of the necessary authority or information access to perform fraudulent activity without collusion. We reviewed access reports that identified users with the ability to update production application configuration management libraries as of May 2007. We reviewed access profiles that provided access to sensitive system libraries and access reports that identified staff members with access to sensitive programs. We randomly selected 15 of the 544 agency security officers as of May 1, 2007, and reviewed access reports that identified the administrative authorities assigned to agency security officers.	OCFO/NFC controls were operating effectively to provide reasonable assurance that access granted to user IDs created during fiscal year 2007 was limited to that authorized, inactive user IDs were disabled, mainframe security administrator activity was documented and reviewed, unsuccessful log in attempts were limited, and warning banners were displayed. However, OCFO/NFC controls had not operated effectively to consistently ensure that access roles provided the least amount of access necessary to perform job functions or that modems were properly protected before being placed in operation. For access roles, we found that 3 of the 30 roles we reviewed provided update access to the Position Management System (PMSO) even though only read access had been authorized on the role SRM. This access also unintentionally caused the access provided to the 92 GESD employees assigned these roles to violate separation of duties principles because the roles were authorized to process transactions in the Entry, Processing, Inquiry and Corrections System and either the Special Payroll Processing System, the System for Time and Attendance, and/or the Time & Attendance Online Suspense Correction and Document System. OCFO/NFC removed this unauthorized access on August 29, 2007. We also determined that one GESD and four Information Technology Services Division (ITSD) access roles included access to certain sensitive programs that were not needed to perform their job functions. OCFO/NFC subsequently removed this access.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
1. Access Control (continued)	For customer agency employees, the customer agency is responsible for designating personnel who are authorized to request user additions, deletions, and security level changes. OCFO/NFC then grants authority to access computer resources to individual users at the request of the customer agency security officer. Customer agency security officers are responsible for requesting access to applications in a manner that employs accepted separation of duty practices within their agency and ensuring the level of access assigned to a user remains appropriate over time. The OCFO/NFC network security policy also addresses suspending inactive user IDs, documenting and reviewing security administrator activity, limiting unsuccessful log in attempts, displaying warning banners, and controlling remote access.	We reviewed the logic for the OCFO/NFC program that disables inactive IDs and tested the logic using a listing of user IDs as of May 1, 2007. We interviewed OCFO/NFC personnel, reviewed desk procedures, and obtained examples of reports used to monitor administrative actions processed by security officers and others in the mainframe environment. We reviewed mainframe and Windows system documentation to determine if user IDs were locked after three unsuccessful sign-on attempts. We logged on to the OCFO/NFC mainframe (directly and remotely) and web-based applications available from OCFO/NFC's public web site to determine if a warning banner was displayed. We obtained a listing of dial up connections at the interim computing facility and attempted to connect to these modems using a Windows communication program (HyperTerminal).	We also determined that one ITSD role was permitted all access to application configuration management load and copy member libraries even though this level of access was not needed to perform the job functions. This unnecessary access was removed. OCFO/NFC officials told us that they are refining procedures for creating and maintaining roles and training new security developers/ administrators. OCFO/NFC is also verifying that SRMs are documented and appropriately authorized, application access is consistent with the SRM, and other resources are appropriate for the organization. We also determined that the 15 agency security officers we reviewed were granted an unnecessary administrative authority that could have allowed agency security officers to assign user schema had they had additional access permissions. OCFO/NFC removed this access. For remote access, we found that 3 of the 17 modems at the interim computing facility allowed connections without password protection. While these connections were allowed, additional passwords would have been required to access OCFO/NFC applications. In August 2007, we verified that one of these modems was disconnected and the other two were password-protected. OCFO/NFC told us they were in the process of updating procedures to ensure that security is addressed before modem lines are assigned.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
2. Awareness and Training Organizations must (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	The OCFO/NFC Information Security Program includes security awareness training to notify users of information systems that support the operations and assets of the agency of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In this regard, the OCFO/NFC management directive for security awareness training requires new employees and contractor personnel to attend the OCFO/NFC New Employee Security Briefing before they are given access to OCFO/NFC computer systems. OCFO/NFC updated its procedures during our review to require divisional security coordinators to maintain the signed briefing and attach it to the security access form (NFC-1106) when requesting access. For customer agency employees, the user organization is responsible for ensuring users sign an agreement to abide by rules of behavior for accessing OCFO/NFC systems prior to requesting access. NFC also requires employees and contractors to complete annual security awareness training that addresses basic U.S. Department of Agriculture (USDA) computer security concepts and provides quarterly security briefings that address OCFO/NFC-specific security responsibilities. For the basic security awareness training, division directors/staff chiefs are responsible for ensuring that all employees and contractor personnel in his/her organization complete annual security awareness training. The OCFO/NFC training coordinator provides reports to division coordinators to help them monitor completion rates for their organizations. USDA also provides OCFO/NFC Cyber Security staff with a monthly IT security scorecard that summarizes completion rates. The OCFO/NFC management directive for individual development plans specifies a process for ensuring that employees receive the training required to perform their job functions.	We randomly selected 15 of the 55 employees hired between October 1, 2006, and March 26, 2007, and requested the new employee security briefing for these employees to determine if it had been completed before access was granted to OCFO/NFC computer systems. We reviewed security awareness training records and associated documentation to determine if 44 OCFO/NFC contractors who were issued badges in December 2007 had completed annual basic security awareness training. We interviewed OCFO/NFC staff members and reviewed the quarterly security awareness briefings provided in December 2006 and March 2007. We also reviewed sign in sheets used to document attendance at quarterly security briefings.	OCFO/NFC procedures provided reasonable assurance that the Center provided quarterly security briefings that addressed OCFO/NFC-specific security responsibilities. However, OCFO/NFC controls had not operated effectively to ensure that employees consistently completed the OCFO/NFC New Employee Security Briefing before they were given access to OCFO/NFC computer systems or all contractors completed annual awareness training. For the new employee security briefing, OCFO/NFC did not provide a signed security awareness briefing for 7 of the 15 new employees we reviewed. Consequently, we could not determine whether access was granted before the briefing for these employees. We also determined that user IDs for two of the remaining eight employees were created before the employee received the security awareness briefing. During our review, OCFO/NFC updated its procedures to require divisional security coordinators to maintain the signed briefing and attach it when requesting access. For annual security awareness training, 33 of the 44 contractors we reviewed had taken the annual training as of June 30, 2007. OCFO/NFC officials told us that the remaining 11 contractors had not completed the training because they had not required contractors to sign up while OCFO/NFC was updating the security awareness training database (AgLearn). OCFO/NFC officials also told us that they are working with AgLearn technical support to enroll these contractors so they can complete the required training.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
3. Audit and Accountability Organizations must (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	The OCFO/NFC network security policy requires the following security events to be logged: all logons and log offs, all failed logons, all lockouts and unlocks, all server-based administrator activities, all unsuccessful attempts to access information resources, and all modifications to highly sensitive data and resources. The network security policy also requires server-based administrator activities and modifications to highly sensitive data and resources to be reviewed to identify and investigate unusual and/or inappropriate modifications. In this regard, OCFO/NFC had established an oversight committee to make policy decisions related to OCFO/NFC's logging, auditing, and monitoring program to ensure efficiency and compliance with Departmental and Federal regulations. In addition, the OCFO/NFC mainframe security plan states that audit trails are configured to support personal accountability by providing a trace of user actions and includes the following minimum requirements for audit trail records: date and time of event; source; type of event; success or failure of event; and name of program/file introduced, accessed, or deleted.	We interviewed NFC personnel. We also reviewed system documentation, configuration information, and access reports.	OCFO/NFC controls were operating effectively to provide reasonable assurance that mainframe audit records were created and protected and the actions of information system users could be traced. However, OCFO/NFC controls had not ensured that unusual and/or inappropriate modifications to certain sensitive system resources and application configuration management libraries would be identified and investigated. For sensitive system resources, OCFO/NFC had instituted a tracking system to ensure that reports were reviewed, expanded its definition of critical security resources, and established a requirement to produce and distribute reports that document access activity associated with sensitive system resources that could impact security regularly. However, these processes had not been fully implemented. As of June 30, 2007, OCFO/NFC was regularly reviewing monthly usage reports for two programs identified as critical system resources in the mainframe environment. In August 2007, OCFO/NFC incorporated reports that identified updates to certain critical mainframe data sets and usage of eight additional sensitive programs into its tracking system. Monitoring reports for 21 programs added as critical mainframe security resources could not be produced because these programs were not protected by the mainframe access control software. OCFO/NFC officials told us that they plan to refine the list of sensitive programs; protect these programs; and begin distributing requested reports.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
3. Audit and Accountability (continued)			However, this effort will not begin until after the data center relocation to the primary computing facility. For application configuration management libraries, OCFO/NFC had implemented automated processes to identify unusual and/or suspicious access activity, but certain production libraries were not included in the monitoring report as of June 30, 2007. In August 2007, OCFO/NFC expanded the monitoring report to include the remaining production configuration libraries.
4. Certification, Accreditation, and Security Assessments Organizations must (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	OCFO/NFC certification and accreditation (C&A) procedures require an independent security test and evaluation (ST&E) to determine the effectiveness of the security controls. The designated approving authority decides whether or not to authorize the system for processing based on the ST&E results and residual risk. This accreditation decision, along with the supporting documentation and rationale, are included in the final accreditation package. OCFO/NFC C&A procedures require systems to be re-accredited every 3 years or when significant changes occur. OCFO/NFC C&A procedures also require agreements that specify security responsibilities for inter-agency or inter-department information system connections. In addition, the OCFO/NFC Information Security Program requires (1) testing and evaluating the effectiveness of information security policies, procedures, and practices at least annually; and (2) planning, implementing, evaluating, and documenting remedial action to address identified deficiencies. OCFO/NFC division directors/staff chiefs are responsible for performing the security control testing and preparing plans of action and milestones to remediate deficiencies. In addition, OCFO/NFC Cyber Security staff is responsible for ensuring that security assessments are conducted and remedial action plans for security deficiencies are implemented.	We interviewed OCFO/NFC personnel and reviewed OCFO/NFC assessments, along with system detail and task reports, documented in the Automated System Security Evaluation and Remediation Tracking system. We also reviewed OCFO/NFC general support system test and evaluation reports, the tracking matrix that documented weaknesses identified and their resolution, and the certification and accreditation statements for the OCFO/NFC general support systems at its interim computing facility. In addition, we evaluated interconnection security agreements for 3 of the 15 organizations with direct connections to the OCFO/NFC interim computing facility.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the associated NIST controls would be achieved.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
5. Configuration Management (CM) Organizations must (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	The OCFO/NFC general support system (GSS) configuration and change management directive specifies policy, responsibilities, and procedures for managing the configuration of and controlling both emergency and routine changes to the OCFO/NFC GSS, which includes all hardware, firmware, system software, and supporting components (cables, connectors, etc.) that make up the entire data center environment. This directive establishes requirements for: • Maintaining both an online configuration management repository and an online change management system; • documenting, testing, approving, validating, and specifying the outcome of each change request; • ensuring that the configuration repository is updated when changes are completed; and • performing an annual review to ensure that the information included in the repository is accurate. NFC management directives also require all services not needed for applications and basic administration of the server to be turned off and an annual configuration review of all OCFO/NFC GSS components to ensure that all unnecessary functions, ports, protocols, services, etc., are identified and eliminated. For applications, OCFO/NFC uses library management software to maintain application baselines throughout the system development lifecycle. The OCFO/NFC management directive for scheduled software maintenance requires all changes to be documented on a program change request form, tested according to development organization guidelines, and approved prior to implementation. Once all approvals have been received, either the library management software or OCFO/NFC staff members independent of the application developers implement the proposed change.	For GSSs, we interviewed NFC personnel and reviewed system documentation. For applications, we interviewed NFC personnel and reviewed system documentation. We also randomly selected 15 of the 217 mandated application change projects and 10 of the 26 emergency changes that were implemented between October 1, 2006, and April 30, 2007, for GESD mainframe applications and reviewed associated documentation for each of the selected changes.	OCFO/NFC controls were operating effectively to provide reasonable assurance that changes to its applications were authorized, documented, and controlled. However, OCFO/NFC had not yet performed planned annual reviews to ensure that its component baseline was accurate and that all unnecessary functions, ports, protocols, services, etc., had been identified and eliminated. In February 2007, OCFO/NFC had updated its policies and procedures to establish requirements for maintaining an online configuration management repository of GSS components and conducting an annual configuration review to ensure that the GSS configuration repository is accurate and that all unnecessary functions, ports, protocols, services, etc., are identified and eliminated. While OCFO/NFC had also established the Data Center Organizer as the official configuration management repository in February 2007, the Center had not conducted a review to determine if the information was accurate or to ensure that only required functions, ports, protocols, services, etc. were available on its GSS components. OCFO/NFC officials told us that they had purchased a tool that would allow them to automate this review and planned to implement the tool after the data center relocated to its primary computing facility.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
6. Contingency Planning Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.	The OCFO/NFC Information Security Program includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. OCFO/NFC Cyber Security staff are responsible for ensuring that a Continuity of Operations/Disaster Recovery Program is implemented, maintained, and tested according to NIST guidance. In addition, division directors/branch chiefs are responsible for providing plans and procedures in coordination with OCFO/NFC central recovery plan and developing, testing, and maintaining continuity of operations plans for their business units. In this regard, the OCFO/NFC Continuity of Operations Plan (COOP) relies on the OCFO/NFC Disaster Recovery Plan (DRP) for recovery of the computer processing capability if an event impacts the interim computing facility and Business Unit Plans that are documented separately to restore the business aspects of critical business unit functions. The OCFO/NFC COOP also states that OCFO/NFC conducts semi-annual tests (drills) at its recovery operations center and alternate work sites to train and exercise its business resumption capabilities as well as its recovery capability. In addition, the OCFO/NFC COOP states that the Center's continuity of operations plans should be updated to reflect lessons learned during these tests. In addition, OCFO/NFC management directives require critical data on servers to be backed up regularly. System administrators are responsible for developing documented procedures for backup and recovery of data on the servers for which they are responsible. Critical application backups and operating system backups are tested at least annually as a part of the division/staff's disaster recovery drill to ensure that such backups support network/workstation recovery and restore procedures.	We interviewed OCFO/NFC personnel. We also reviewed the OCFO/NFC COOP, OCFO/NFC DRP, documentation associated with OCFO/NFC DRP desktop reviews, and the results of a review of information system backups at the NFC offsite storage facility.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the OCFO/NFC COOP and the associated plan for recovering computer operations (DRP) had been updated to reflect the current operating environment and information system backups were created and stored at an off-site facility. However, as of June 30, 2007, OCFO/NFC had not tested its updated recovery procedures to ensure that information system could be recovered from its backups and reconstituted to a known secure state after a disruption or failure. In fiscal year 2006, we reported that OCFO/NFC had not yet updated its procedures for recovering computer operations (DRP) to reflect changes that occurred with the move to the interim computing facility or tested recovery of operations at its new recovery operations center. While OCFO/NFC had updated its DRP based on desktop reviews, the center had not tested recovery of computer operations based on the updated procedures as of June 30, 2007. OCFO/NFC performed a disaster recovery test where it used backup information from its interim computing facility to recover its systems at the primary computing facility during the week of July 29, 2007. OCFO/NFC officials told us that they plan to update the recovery plan and procedures based on these results and perform an additional test in November when the backup computing facility is established in New Orleans.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
7. Identification and Authentication Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	For OCFO/NFC employees, the OCFO/NFC network security policy states that user IDs and processes will be identified to an individual, have a password, and not be shared. This policy also states that if a process cannot be specifically tied to an individual, then the password lifetime will be issued for the period of the session. In addition, the network security policy requires initial passwords to be communicated in confidence and set to expire and force a new password selection on the user's first sign-on to the system. Additional desk procedures provide guidance on resetting passwords. The OCFO/NFC network security policy states that passwords should: • Be at least six characters; • consist of alphabetic and numeric characters; • not be stored in clear text on any medium; • not be the same as any of the five previous passwords; • not be identical to the user's ID; • be set to expire at least every 90 days; • be controlled via a restricted password list when possible; and • be protected from eavesdropping during network transmissions. The network security policy also requires default passwords to be changed when the hardware or application is implemented. In addition, this policy states that whenever access is to be gained by remote methods, passwords will be supplemented with personal identification numbers, tokens, smart cards, or some other trusted authentication device or procedure. For customer agency employees, the customer agency is responsible for designating personnel (agency security officers) who are authorized to request user additions, deletions, and security level changes. Agency security officers are also responsible for ensuring the level of access assigned to a user remains appropriate over time.	We interviewed OCFO/NFC personnel. We also reviewed a listing of user IDs and mainframe password settings. In addition, we accessed the NFC mainframe and web-based applications available from the NFC web site to determine if NFC systems obscured feedback of authenticator information.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the associated NIST controls would be achieved.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
8. Incident Response Organizations must (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.	The OCFO/NFC Information Security Program includes procedures for detecting, reporting, and responding to security incidents. In this regard, the OCFO/NFC *Computer Incident Handling Guide* establishes policy, responsibilities, and procedures for addressing computer security incidents. These procedures address detecting potential incidents; documenting and analyzing the potential incidents to determine if an incident has occurred and, if so, the appropriate steps regarding containment, eradication and recovering from the incident; and documenting, tracking, and promptly reporting information security incidents to the appropriate authorities.	We interviewed NFC personnel and reviewed the NFC *Computer Incident Handling Guide*, along with sign in sheets for incident response training that was provided to ITSD Operations Security Center staff members.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the associated NIST controls would be achieved.
9. Planning Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.	The OCFO/NFC Information System Security Program requires division directors/staff chiefs to prepare and maintain system security plans (SSP) that provide adequate information security for system resources under their responsibility. In this regard, OCFO/NFC certification and accreditation procedures require the existing SSP to be reviewed to ensure that it describes the most current system configuration, specifies all security controls included in the system, and was prepared according to NIST guidance. These procedures also require SSP updates when changes that impact security are implemented. In addition, USDA requires agency heads to submit system security plans and attest to their accuracy and completeness annually. In addition, the OCFO/NFC management directive for security awareness training requires new employees and contractor personnel to attend the OCFO/NFC New Employee Security Briefing, which includes rules of behavior, before they are given access to OCFO/NFC computer systems. For user organization employees, the user organization is responsible for ensuring users sign an agreement to abide by rules of behavior for accessing OCFO/NFC systems prior to requesting their access.	We interviewed NFC personnel and reviewed the final system security plans for the NFC GSS' associated with payroll/personnel services, along with the *Security Access Manual* provided to agency security officers.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the associated NIST controls would be achieved.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
10. Personnel Security Organizations must (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.	The OCFO/NFC personnel security and suitability program directive, which applies to all OCFO employees, contractors, and consultants located at OCFO/NFC, requires all positions to be assigned a Position Sensitivity Designation (PSD) level in accordance with its potential to have an adverse effect on the USDA mission and national security and each person to undergo the appropriate type of personnel security investigation based on the position sensitivity or risk level designation. This directive also requires each PSD to be reviewed when job responsibilities change or every 2 years. In addition, the OCFO/NFC management directive for completing its separation (NFC-1267) and transfer (NFC-1366) forms provides a means to ensure that organizational information systems are protected when terminations and transfers occur. Furthermore, the OCFO/NFC management directive specifying information system user responsibilities requires OCFO/NFC managers to consult with the HRMS regarding the appropriate disciplinary action to take against employees for not complying with the responsibilities specified.	We interviewed OCFO/NFC personnel and reviewed Security Entry and Tracking System (SETS) information as of May 29, 2007, along with the results of OCFO/NFC's 2006 PSD review. We randomly selected 15 of the 107 employee transfers that occurred from October 1, 2006, through April 6, 2007, for review. For each of the selected transfers, we reviewed the transfer (NFC-1366) form and the access permissions associated with the transferred employee's user ID. We randomly selected 15 of the 47 employee separations that occurred from October 1, 2006, through March 16, 2007. For each of these separations, we reviewed the separation (NFC-1267) form, a listing of mainframe user IDs, and Information System Security Office (ISSO) documentation to determine when access was disabled.	OCFO/NFC controls were operating effectively to provide reasonable assurance that organizational information systems were protected when transfers occurred and to ensure that appropriate disciplinary actions would be taken if employees fail to comply with information system user responsibilities. While OCFO/NFC had improved its control processes, we found that controls were not operating with sufficient effectiveness to ensure that employee PSDs were accurately reflected in SETS, suitable personnel security investigations were requested, or separation forms were consistently completed before employees separated. For employee PSDs, even though OCFO/NFC had instituted a quarterly PSD review to help ensure that PSDs remain accurate, we determined that SETS did not contain accurate PSDs for more than 20 percent of the employees (7 of 33) whose SETS PSD did not match the results of the NFC PSD review. This occurred because one division had not performed its PSD review while its security officer was temporarily reassigned. While the employees' background investigations were suitable based on the correct PSD, OCFO/NFC had identified these employees as needing higher level background investigations. To prevent this type of problem from recurring, OCFO/NFC officials told us that they plan to begin requiring the security officers to report the results of their quarterly review even if no changes are required.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
10. Personnel Security (continued)			For personnel security investigations, we determined that the appropriate level of background investigation had not been requested for about 6 percent of OCFO/NFC employees (55 of 847) in SETS as of May 29, 2007. While these employees had undergone the minimum required investigation for Federal employees, OCFO/NFC procedures required a more stringent investigation based on the employee's PSD. OCFO/NFC officials told us that they had performed a manual review of SETS information in March and April 2007 to identify employees that did not have appropriate background investigations for their current PSD and were in the process of scheduling the needed investigations. This manual review occurred because SETS does not provide a reporting mechanism that allows users to easily identify employees with unsuitable investigations based on their current PSD. OCFO/NFC officials confirmed with a USDA Personnel and Document Security Division official that the new version of SETS, which is scheduled for implementation on or about November 2007, will include a report that should help organizations ensure that investigations are appropriate. In addition, OCFO/NFC officials told us that they plan to begin requiring an OPM worksheet to be submitted for PSD changes. These forms will be assigned a control number and forwarded to the appropriate organizations to ensure that the PSD change is made in PMSO and additional background investigation requirements are identified in a timely manner.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
10. Personnel Security (continued)			As of August 24, 2007, OCFO/NFC had made corrections for about half (26 of 55) of the unsuitable investigations we identified by either submitting requests to update background investigations or reclassifying PSDs to more accurately reflect the employee's duties. OCFO/NFC officials told us that they planned to provide additional education regarding PSDs and continue submitting requests to update background investigations for employees based on their correct PSDs. For separations, the OCFO/NFC separation form (NFC-1267) was not processed on or before the employee's separation date for 5 of the 15 separated employees that we reviewed. In each of these cases, the employee's supervisor had not ensured that the form was completed and delivered to HRMS by the separation date. ISSO personnel processed these forms from 11 to 57 days after the actual separation date, which increases the risk of improper activity after separation. However, we verified that this control weakness had not resulted in improper mainframe activity. We also noted that four of these five instances occurred before OCFO/NFC updated its procedures in December to require the employee's immediate supervisor to ensure that the OCFO/NFC separation form is completed and delivered to HRMS no later than close of business on the effective date of the separation.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
11. Risk Assessment Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	The OCFO/NFC Information System Security Program requires periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets, and tasks division directors/staff chiefs with ensuring that these risk assessments are prepared and maintained. In this regard, OCFO/NFC C&A procedures require the risk assessment to contain a security categorization based on the FIPS 199 guidance, to be reviewed to ensure that it identifies all apparent threats and vulnerabilities in the information technology system and is consistent with the NIST guidance, and to be updated each time there is a change to the security controls on the system that might affect the residual risk to the system. In addition, OCFO/NFC currently performs monthly scans to identify network vulnerabilities. The OCFO/NFC management directive for network vulnerability self assessments requires the identified vulnerabilities to be analyzed and eliminated or documented if the vulnerability is required for production processes. While the directive does not specify a timeframe for resolution, it requires approved action plans for vulnerabilities that are not resolved or documented within 45 days.	We interviewed NFC personnel and reviewed the final C&A documentation, including risk assessments, for the NFC GSS' associated with payroll/personnel services. We also evaluated the NFC vulnerability scanning process, including the cumulative vulnerability report as of June 21, 2007. In addition, we reviewed 8 of the 48 vulnerabilities that had been classified as either a false positive or an acceptable risk.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the associated NIST controls would be achieved.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
12. System and Communications Protection Organizations must (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	The OCFO/NFC network connects its resources to the Internet, to the general USDA network, to other US Government agencies, and to financial institutions. The OCFO/NFC firewall policy establishes a requirement for a demilitarized zone between the Internet and OCFO/NFC's internal network to support applications that require publicly accessible network servers. The demilitarized zone is protected by firewalls on both sides. The OCFO/NFC firewall policy also requires all direct connections to the Internet or other networks to occur through an OCFO/NFC managed firewall that denies all inbound and outbound protocols unless specifically permitted and identifies the source and destination for each protocol. NFC procedures for connecting laptop computers and other devices to the OCFO/NFC network prohibit employees from connecting devices to the network without approval. If approved, OCFO/NFC ensures that the device is appropriately protected before connecting it to the network.	We interviewed NFC personnel and reviewed system documentation, including NFC firewall rules.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the associated NIST controls would be achieved.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
13. System and Information Integrity Organizations must (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	NFC management directives and other guidance establish policy, responsibilities, and procedures for reviewing advisory alerts and implementing network system security patches required for OCFO/NFC systems, requiring the use of anti-virus software, and prohibiting users from installing unauthorized software on their computers. The OCFO/NFC management directive for network vulnerability self assessments also requires vulnerability scans to be performed at least quarterly and states that identified network vulnerabilities will be analyzed and eliminated or documented if the vulnerability is required for production processes. While the directive does not specify a timeframe for resolution, it requires action plans to be documented and approved for vulnerabilities that are not resolved or documented within 45 days. In addition, OCFO/NFC network security policy states that the Center will develop and administer an intrusion detection program to reduce the risk of unauthorized access or hostile activity.	We interviewed NFC personnel and reviewed system configuration information. We also evaluated the NFC vulnerability scanning process, including the cumulative vulnerability report as of June 21, 2007. In addition, we reviewed 8 of the 48 vulnerabilities that had been classified as either a false positive or an acceptable risk.	OCFO/NFC controls were operating effectively to provide reasonable assurance that the associated NIST controls would be achieved.