U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Fiscal Year 2006 – Office of the Chief Financial Officer/National Finance Center General Controls Review

Report No. 11401-24-FM
September 2006

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 28, 2006

REPLY TO
ATTN OF: 11401-24-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 2006 – 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 2006. 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 recovered from the disruptions caused by Hurricane Katrina and 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 operated effectively during fiscal year 2006.

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 2006 – Office of the Chief Financial Officer/National Finance Center General Controls Review (Audit Report No. 11401-24-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 2006. 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 entity-wide security program planning and management, access, application change, system software, and service continuity control objectives were consistently achieved from October 1, 2005 through June 30, 2006. This occurred mainly because of disruptions to normal operating procedures while OCFO/NFC recovered its operations and reconstituted its workforce in New Orleans, Louisiana, after Hurricane Katrina. While we also identified certain controls that were not adequately designed, OCFO/NFC updated its procedures during our review to address these issues. 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 control objectives specified in the description, 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 control objectives specified were achieved during the period from October 1, 2005 through June 30, 2006.

Our audit disclosed that OCFO/NFC's description of controls presented fairly, in all material respects, the relevant aspects of OCFO/NFC. 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

During our review, OCFO/NFC reinstituted control activities that were disrupted after Hurricane Katrina and updated its procedures to address the control weaknesses we identified. We make no additional recommendations.

Table of Contents

Executive Summary ..... **i**

Report of the Office of Inspector General **1**

Exhibit A – Office of the Chief Financial Officer/National Finance Center Description of Controls **3**

Exhibit B – Office of Inspector General - Review of Selected Controls **18**

Report of the Office of Inspector General

TO: Charles R. Christopherson, Jr.
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 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, 2006; and (3) such controls were suitably designed to achieve the control objectives in the description, 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 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.

OCFO/NFC continued to improve its internal controls. However, certain security program planning and management, access, application change, system software, and service continuity control objectives, as described in exhibit B, were not consistently achieved during the period when OCFO/NFC was recovering its operations and reconstituting its workforce in New Orleans, Louisiana, after Hurricane Katrina. While we also identified certain control practices that were not adequately designed, OCFO/NFC updated its procedures during our review to address our concerns.

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, 2006. Also, in our opinion, the controls included and/or referenced in exhibit A 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 control objectives included 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 that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in exhibit A were achieved during the period from October 1, 2005 through June 30, 2006.

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, 2006, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 2005 through June 30, 2006. 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

September 21, 2006

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

DESCRIPTION

OF THE

INTERNAL CONTROL STRUCTURE

AS OF JUNE 30, 2006

Pages 4 through 17 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 OCFO/NFC control objectives specified 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 OCFO/NFC in exhibit A, 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. OCFO/NFC ensures its entity-wide security program planning and management control objectives are met by: a. Enforcing the security life cycle process in all phases of the information system's life; b. developing and maintaining system security plans to document current controls and address planned controls for information technology (IT) systems in support of the organization's mission; c. verifying that security controls and features are examined both periodically and on an event driven basis according to departmental standards for certification and accreditation (C&A) of IT systems and infrastructure; and d. authorizing the operation of organizational information systems and any associated information system connections.	OCFO/NFC C&A procedures, which address security documentation requirements throughout an information system's life cycle, establish roles and responsibilities for a three-phased C&A approach: • Phase 1, the precertification phase, consists of defining the system, including its security categorization, and the scope of the C&A effort; identifying existing security controls from the security controls compliance matrix, reviewing the system security plan, reviewing the initial risk assessment, and negotiating with participants. • Phase 2, the C&A phase, includes conducting a security test and evaluation (ST&E), updating the risk assessment with findings from the ST&E, updating the system security plan, documenting certification findings; and forwarding the certification findings to the designated accrediting authority for an accreditation decision. • Phase 3, the post-accreditation phase, consists of managing the configuration of the system to ensure that the that the security posture of the system is not threatened by hardware or software changes, the system security plan is kept current, and performing re-accreditation every three years or when the system changes significantly.	We reviewed the risk assessments, system security plans, ST&E reports, certification statements, and accreditation statements for OCFO/NFC's Payroll/Personnel System, Payroll Accounting System, System for Time and Attendance Reporting, and the associated general support systems. We randomly selected 15 of the 177 non-emergency projects associated with application changes that occurred between October 1, 2005 and March 15, 2006, and judgmentally selected 10 of the 222 general support system changes that were implemented between October 1, 2005, and March 4, 2006, and reviewed associated documentation provided by OCFO/NFC to determine if potential security impacts had been adequately assessed.	OCFO/NFC controls were suitably designed to achieve the control objectives. We also found that that security impacts associated with changes to applications and general support systems were assessed. However, OCFO/NFC had not updated its general support system risk assessments, security plans, certifications, or accreditations to reflect the changes that occurred when data center operations were transferred to the interim computing facility in Philadelphia, Pennsylvania, in January 2006. OCFO/NFC officials told us that they were operating under extraordinary circumstances and there was not time to establish a new data center and perform a full C&A within the timeframes under which they were required to migrate off of the equipment at the recovery operations center after Hurricane Katrina. According to OCFO/NFC management, the certification and accreditation process was started as soon as normal business operations were resumed in January 2006. On August 3, 2006, OCFO/NFC provided us with the updated risk assessments, system security plans, ST&E reports, and draft certification and accreditation letters that were submitted to U.S. Department of Agriculture's Office of the Chief Information Officer.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
2. OCFO/NFC ensures its entity-wide security program planning and management control objectives are met by conducting periodic reviews and assessments of implemented security controls to ensure that the controls remain necessary and effective.	The OCFO/NFC information security program requires division directors and staff chiefs to perform periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices on at least an annual basis. In addition, the Cyber Security Staff is responsible for ensuring that plans, procedures, and security controls are tested.	We interviewed OCFO/NFC personnel and reviewed the latest OCFO/NFC control self assessments for its major applications and general support systems.	OCFO/NFC controls were suitably designed and operating effectively to achieve the control objectives.
3. OCFO/NFC ensures its entity-wide security program planning and management control objectives are met by developing and implementing plans of action to correct any known or identified deficiencies and reduce or eliminate vulnerabilities in its information systems.	The OCFO/NFC information security program requires division directors and staff chiefs to prepare plans of action and milestones to remediate deficiencies and the Cyber Security Staff to ensure that remedial action plans for security deficiencies are implemented.	We interviewed OCFO/NFC personnel and reviewed the OCFO/NFC plan of action and milestones. OCFO/NFC also provided the March 2006 monthly update that was sent to the Associate Chief Information Officer for Cyber Security.	OCFO/NFC controls were suitably designed and operating effectively to achieve the control objectives.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
4. OCFO/NFC ensures its entity-wide security program planning and management control objectives are met by implementing personnel security controls, specifically background investigations and clearances, and ensuring adequate assignment of responsibilities.	OCFO/NFC had issued a management directive to define policy, responsibilities, and procedures for assigning risk levels, designating position sensitivity, and obtaining required background investigations for OCFO/NFC and contractor personnel. In May 2006, OCFO/NFC updated this directive to clearly require all employees to be assigned a position sensitivity designation, or risk level, and undergo the appropriate type of investigation. The updated directive also establishes requirements for re-evaluating risk levels when job responsibilities change or every two years.	We selected 10 OCFO/NFC employees hired into IT positions since May 2003 to review the process for assigning risk codes. We also judgmentally selected 36 IT employees in a manner that ensured that different OCFO/NFC organizations were represented to determine if assigned risk levels were appropriate. We reviewed documentation to determine if employees assigned the high and moderate risk levels for computer/ information system positions had completed required background investigations and periodic reinvestigations. We reviewed background investigation documentation for 10 contractors.	OCFO/NFC controls, as updated, were suitably designed to achieve the control objectives. However controls had not operated effectively to ensure that risk levels were accurate and appropriate background investigations, or reinvestigations, had been performed for OCFO/NFC employees. For example: • Thirteen of the 36 employees reviewed did not have risk levels that reflected current duties; • 46 of 180 employees assigned a high risk level for computer/information system positions did not show initial background investigations; an additional 10 did not have evidence of reinvestigations; and 39 only had limited or minimum background investigations even through a full background investigation was required; and • 47 of the 83 employees with a moderate risk for computer/information system positions did not show an initial background investigation. During our review, OCFO/NFC evaluated employee risk levels to ensure that proper background checks were initiated and updated its management directives to clarify personnel security responsibilities and specify risk level review requirements.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
5. OCFO/NFC ensures its entity-wide security program planning and management control objectives are met by conducting security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.	The OCFO/NFC information security program includes security awareness training to inform personnel, including contractors and other 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. The OCFO/NFC management directive for security awareness training requires new OCFO/NFC employees and contractor personnel to attend the OCFO/NFC New Employee Security Briefing before being given access to OCFO/NFC computer systems. For customer agency employees, the customer agency is responsible for ensuring users sign an agreement to abide by rules of behavior for accessing OCFO/NFC systems prior to requesting their access. The OCFO/NFC management directive for security awareness training also requires employees to complete annual security awareness training to renew their awareness of security responsibilities. This directive tasks the Cyber Security Staff with maintaining a security awareness program and division directors and staff chiefs with ensuring attendance. In addition, the OCFO/NFC management directive for individual development plans specifies a process for ensuring that employees receive training required to perform their job functions.	We interviewed OCFO/NFC personnel, reviewed the New Employee Security Briefing, and analyzed the security awareness tracking report as of April 26, 2006. We judgmentally selected a sample of 25 Government Employee Services Division and 25 Information Resources Management Division employees from organizational listings as of March 22, 2006, in a manner that ensured that staff members assigned to different organizational units would be selected. We reviewed the security awareness training status report as of April 30, 2006, and additional documentation to verify that they had completed the training.	OCFO/NFC controls were suitably designed to achieve the control objectives if customer agencies applied the controls specified in exhibit A. OCFO/NFC controls were also operating effectively to ensure that OCFO/NFC users were made aware of basic information system security concepts, but not OCFO/NFC-specific security responsibilities. While OCFO/NFC had planned for quarterly security awareness briefings addressing OCFO/NFC security-related directives, these briefings were not provided as planned because Hurricane Katrina disrupted the process. OCFO/NFC had plans to continue the quarterly security briefings.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
6. OCFO/NFC ensures its entity-wide security program planning and management control objectives are met by enforcing physical and logical security measures to prevent errors and irregularities and the possibility of loss of data or processing by limiting access to authorized users and restricting the types of transactions and functions that authorized users are permitted to exercise.	For OCFO/NFC employees, the OCFO/NFC data security access policy directive states that access will be limited based on the minimum number of employees needed to effectively perform job functions, as determined by resource owners. This directive also establishes a standard process for requesting access to resources based on a standard form that documents the specific resources and access level required, the reason the access is needed, and both management and resource owner approvals. In June 2006, OCFO/NFC published a role-based security access policy and procedures for creating access roles, adding and removing staff members from existing roles, and modifying access authorities included in existing roles. In addition, the OCFO/NFC management directive for establishing internal controls over access requires separation of functions to guard against personnel having the opportunity to commit and/or conceal intentional or unintentional alteration, destroy data or software. If the separation of incompatible functions is not possible, branch chiefs are required to implement compensating controls. This directive also establishes procedures for ensuring that access remains appropriate over time. Division/staff office security coordinators are responsible for reviewing reports of personnel actions and branch chiefs are responsible for periodically reviewing their employee's access authorities to determine if access needs to be changed or removed. Furthermore, the OCFO/NFC management directive for completing its separation form (NFC 1267) requires the employee or their first line supervisor to hand carry the form to different organizations, including ISSO, on the employee's last working day. An ISSO representative signs the form to certify that mainframe access has been removed.	We interviewed Information Systems Security Office (ISSO) personnel regarding the processes used to manage information system accounts and observed the process for creating mainframe user identifications (ID) and passwords. For OCFO/NFC users, we reviewed listings that identified access permissions for sensitive payroll/personnel applications, production libraries related to mainframe application configuration management, and system resources. We also evaluated access permissions for 4 OCFO/NFC employees that transferred as of October 28, 2005, and 10 employees that separated after October 1, 2005. For customer agency employees, we reviewed access permissions for 14 judgmentally selected customer agency users whose accounts were created between October 1, 2005, and March 21, 2006. We also followed up on 13 employees that were either listed on a customer agency security officer listing or were assigned administrative access authorities consistent with customer agency security officer functions to determine if OCFO/NFC was accurately maintaining customer agency security officers. For inactive user IDs, we reviewed a listing provided by ISSO in March 2003 to identify and follow up on accounts that had not been used in 180 days, but were still active.	OCFO/NFC controls, as updated, were suitably designed to achieve the control objectives if customer agencies applied the controls specified in exhibit A. In addition, physical access controls were operating effectively to achieve the control objectives. However, logical access controls had not operated effectively to ensure that access to sensitive resources was appropriately limited. While OCFO/NFC had made substantial progress in implementing role-based access profiles, unnecessary access to payroll/personnel applications, application configuration management libraries, and sensitive system resources continued to exist. For example, 67 OCFO/NFC staff members were granted access to certain payroll and/or personnel applications even though it was not required to perform job functions. This included 16 staff members assigned to application development organizations that were granted access to process transactions through certain payroll and/or personnel applications, which violates segregation of duties principles. OCFO/NFC removed this unnecessary access when role-based access profiles were assigned to the staff members with unnecessary access. We also found that unnecessary access to sensitive system resources identified in our fiscal year 2005 review continued to exist. This included unnecessary access to 6 of 17 sensitive operating system libraries reviewed, 42 of 72 authorized program facility libraries reviewed, and a database utility that could be used to bypass normal controls.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
6. (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. These customer agency security officers are also responsible for ensuring the level of access assigned to a user remains appropriate over time. OCFO/NFC then grants authority to use (access) its facilities to individual users at the request of customer agency security officer. An additional management directive addresses the suspension/deletion of unused accounts and states that OCFO/NFC will use an automated process to delete user identifications after 150 days without use. The OCFO/NFC network security policy requires physical access to servers and related components to be limited to authorized personnel. The policy also requires servers, backup facilities, uninterrupted power supply, network switches, etc., to be installed in physically secured areas whenever possible.	For physical access controls, we judgmentally selected 10 of the 36 employees with access to the interim computer facility for review.	It appeared that the request to remove this access was not processed in the confusion after Hurricane Katrina. OCFO/NFC officials told us that the request had been resubmitted. In addition, 13 OCFO/NFC staff members were allowed to update certain production application configuration management libraries even though this access was not required to perform job functions. OCFO/NFC officials told us that this access would be removed. In April 2006, OCFO/NFC established procedures that require annual reviews of all users and resources assigned to role-based access profiles. In addition, we identified 10 OCFO/NFC employees that required access permissions that violated segregation of duties principles to perform their job functions. These access permissions provided the ability to create a fictitious employee position, enter payroll and personnel actions for the fictitious employee, and process payments for the fictitious employee for both USDA and other customer agencies. While OCFO/NFC had established controls to review manual payments for OCFO/NFC employees, it was not reviewing payments initiated by OCFO/NFC employees for customer organization employees. In addition, OCFO/NFC had not implemented controls to review other payroll and personnel actions entered by its employees.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
6. (continued)			For transferred employees, OCFO/NFC had not appropriately adjusted access for 2 of the 4 users we reviewed that had transferred organizations. This occurred because requests to cancel access authority were not submitted when the employee transferred and OCFO/NFC was not producing a report of personnel actions that was intended to allow division office security coordinators to determine if access had been appropriately adjusted. During our review, OCFO/NFC established new procedures to ensure appropriate clearance of systems access, property, and other accountable items when employees transfer. These procedures include a control report that will be used to ensure that all transferred personnel have a completed transfer form. For separated employees, 8 of the 10 employees that we reviewed continued to have access to OCFO/NFC systems after their separation date. This occurred mainly because the separation form that triggers access removal was not consistently processed during the period when OCFO/NFC staff members were deployed in different locations after Hurricane Katrina. In addition, OCFO/NFC had not always removed access before signing the separation form. During our review, OCFO/NFC created desk procedures to ensure that access was appropriately removed.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
6. (continued)			During our review, OCFO/NFC expanded its existing procedures for reviewing manual payments to include transactions initiated by OCFO/NFC employees for customer agencies and created new reports to identify payroll and personnel actions initiated by its employees for review. For customer agency employees, OCFO/NFC officials could not locate the access requests for 4 of the 14 customer agency employees we reviewed. These accounts were created during October 2005 while OCFO/NFC was operating in disaster recovery mode after Hurricane Katrina. For 3 of the remaining 10, OCFO/NFC granted access based on requests from personnel that were not in the customer agency security officer listing. We also identified 2 instances where OCFO/NFC granted more access than was specified in the original request. During our review, OCFO/NFC created desk procedures for processing requests from customer agency security officers to ensure that the requestor is an authorized security officer and that access is appropriately granted based on the request.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
6. (continued)			We also found that OCFO/NFC had not maintained an accurate record of customer agency security officers. OCFO/NFC officials told us they were verifying current customer agency security officers. Also, OCFO/NFC updated its internal procedures and the procedures provided to customer agency security officers to ensure that customer agency security officers are accurately identified. For inactive user IDs, we determined that OCFO/NFC had implemented an automated process to delete mainframe user IDs after 150 days without use, but OCFO/NFC security officers and a certain type of customer agency security officer were not included in this process. OCFO/NFC updated its automated process to include these security officers in July 2006.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
7. OCFO/NFC ensures its access control objectives are met by enforcing controls to uniquely identify users, processes, and information resources and verifying the identity of a subject to ensure that it is valid.	The OCFO/NFC network security policy requires both user IDs and processes to be identified with an individual and to not be shared. This policy also requires each user account to have a password to ensure that users can be identified and authenticated.	We reviewed a list of mainframe user IDs and followed up on 42 user IDs that appeared generic. We also observed the process for creating user IDs and passwords and connected to servers to ensure that authentication was required.	OCFO/NFC controls were suitably designed and operating effectively to achieve the control objectives.
8. OCFO/NFC ensures its access control objectives are met by enforcing controls to monitor, analyze, investigate, and report on IT activity.	The OCFO/NFC network security policy states that the following events will be logged: logons and log offs; failed logons; lockouts and unlocks; server-based administrator activities; unsuccessful attempts to access information resources; and modifications to highly sensitive data and resources. The policy also requires the Information Systems Policy and Control Staff (ISPCS) to monitor logs for unusual security events, including unsuccessful access attempts to gain entry to systems or access sensitive information; deviations from access trends; unsuccessful attempts to access highly sensitive data and resources; highly sensitive/privileged access outside of normal operations; and access modifications made by non-security personnel. If further investigation is required, ISPCS documents the findings and if the event is found to be, or has the potential to be, a computer security incident, directs it to Cyber Security Staff. The policy also requires OCFO/NFC to develop and administer an intrusion detection program to reduce the risk of unauthorized access or hostile activity.	We interviewed OCFO/NFC personnel. We also reviewed system configuration information and monitoring reports.	OCFO/NFC controls were suitably designed, but not operating effectively to ensure that unusual or suspicious activity to certain sensitive mainframe resources was identified and investigated. OCFO/NFC's intrusion detection system was operating as intended and mainframe security events were being logged. However, some of the mainframe monitoring reports had not been consistently reviewed during fiscal year 2006. While it appeared that the security reporting processes were not interrupted after Hurricane Katrina, changes occurred in the way some reports were distributed and responsible parties were not always aware that the monitoring reports were being produced. OCFO/NFC performed a review of its mainframe monitoring reports that included documenting the current method of delivery, which should help ensure that reports are received by the appropriate staff member.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
9. OCFO/NFC ensures its access control objectives are met by: a. Enforcing controls to monitor and control communications at the external boundary of the information system and at key internal boundaries with the system; b. preventing public access into the internal networks; c. only permitting connections to the Internet through controlled interfaces; and d. allocating publicly accessible information system components to separate sub-networks with separate, physical network interfaces.	The OCFO/NFC firewall policy 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. The firewall policy also 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 that permit http and https services and only allow administrative protocols through the internal network. The OCFO/NFC network security policy requires all modems connected to the OCFO/NFC network be documented and approved. The OCFO/NFC management directive for modem phone lines establishes procedures for requesting, approving, and performing an annual validation of authorized modem lines. In addition, OCFO/NFC runs a quarterly phone scan to identify unauthorized modems. OCFO/NFC procedures also prohibit employees from connecting devices to the network. Employees must submit Form NFC-1155. If approved, OCFO/NFC ensures that the device is appropriately protected before connecting it to the network.	We interviewed OCFO/NFC staff. We also obtained OCFO/NFC firewall rules and reviewed the system test and evaluation report for the mainframe general support system and other system documentation for the interim computing facility. We reviewed the results of OCFO/NFC phone scans performed in March 2006. We tested the modems identified by the OCFO/NFC phone scans and 16 modem lines at the interim computing facility to ensure that they were adequately secured. We also reviewed documentation associated with connecting devices to the OCFO/NFC network.	OCFO/NFC controls were suitably designed and operating effectively to achieve the control objectives.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
10. OCFO/NFC ensures its access control objectives are met by protecting the physical facility to prevent unauthorized access to the computers, printers, terminals, telecommunications equipment, and storage media.	The OCFO/NFC network security policy states that physical access to the network server and related components is limited to authorized personnel. The policy also requires servers, backup facilities, uninterrupted power supply, network switches, etc., to be installed in physically secured areas whenever possible. OCFO/NFC implemented security procedures for gaining access to the interim computing facility in January 2006. In July 2006, OCFO/NFC updated these procedures to include periodically reviewing the access control listing to ensure that access was still appropriate and analyzing physical access logs to identify unusual or suspicious attempts to access OCFO/NFC controlled areas at the interim computing facility.	We interviewed OCFO/NFC officials, reviewed documentation describing how physical access points are controlled, and observed physical security access points and processes at the interim computing facility. We judgmentally selected 10 of the 36 employees with access to the interim computing facility as of April 24, 2006, for review to determine if their access was appropriately authorized. We reviewed access logs that documented denied attempts to access OCFO/NFC controlled areas at the interim computing facility from January 2006 through April 2006. We observed OCFO/NFC procedures for escorting and monitoring visitor activity and reviewed associated visitor access logs.	OCFO/NFC controls, as updated, were suitably designed and operating effectively to achieve the control objective.
11. OCFO/NFC ensures its environmental protection control objectives are met by maintaining a secure, conditioned space with redundant uninterruptible power source, physical event monitoring, and available onsite assistance in order to minimize potential damage to or interruption of information systems.	The OCFO/NFC network security policy requires critical application network components have air conditioning and humidity control systems to maintain temperatures within manufacturer specifications. In addition, the policy states that the network and its components should be protected from the effects of static electricity, power surges, dust, smoke, water, and other particulate matter. In this regard, critical applications are required to reside on systems with a backup power supply that includes both power surge protection and line conditioning/filtering capabilities. In addition, OCFO/NFC operates, maintains, and tests emergency power generators for use during commercial power outages.	We interviewed personnel, observed both OCFO/NFC and the interim computing facility, and reviewed associated documentation.	OCFO/NFC controls were suitably designed and operating effectively to achieve the control objectives.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
12. OCFO/NFC ensures that change control objectives for production application systems are met by: a. Planning, developing, implementing, and directing a software quality assurance program that includes configuration management and user acceptance testing; b. providing configuration management by identifying and defining the configuration items in a system, controlling the release and change of these items through the system life cycle, and recording completeness and correctness of configuration items; c. maintaining baseline configurations and inventories of organizational information systems; and d. utilizing state-of-the-art change control tools for migration of program changes from development environments to quality assurance and production environments.	The OCFO/NFC management directive for scheduled software maintenance defines policy, responsibilities, and procedures for controlling application software changes. This directive requires all changes to be documented on a program change request form, tested according to development organization guidelines, and approved prior to implementation. Also, it includes a step for updating associated procedure documentation. Supplemental guidance for completing program change request forms states that the form serves as a cover sheet for requirements documentation and should be prepared and approved. Also, there is agreement on software requirements as documented by requirements analysts or the customer agency. Supplemental guidance for application software testing requires both emergency and non-emergency program changes to undergo unit testing and additional testing for non-emergency changes, which are classified as either mandated or routine. Mandated changes undergo user acceptance testing in a simulated production environment, unless specifically waived by the operations manager or the user requesting the change; while routine changes undergo more formal quality assurance acceptance testing unless specifically waived by the development organization, users, and other technical personnel. Test plans that include test cases and expected results; test results; and the associated approvals are required to be documented and maintained.	We interviewed OCFO/NFC officials and reviewed system documentation. We randomly selected 15 of the 177 non-emergency projects and 5 of the 24 emergency projects associated with application changes that were implemented between October 1, 2005 and March 15, 2006, and reviewed associated documentation provided by OCFO/NFC. We eliminated one of the non-emergency projects selected because it was an emergency project that was miscoded.	OCFO/NFC controls were suitably designed and operating effectively for emergency changes, but not for non-emergency changes. OCFO/NFC had adequately documented and approved the 14 non-emergency projects we reviewed. However, OCFO/NFC did not provide complete requirements and/or unit test documentation for 5 of the 14 projects. Three of these projects occurred while OCFO/NFC was deployed after Hurricane Katrina. The two additional projects with incomplete documentation appear to have been caused by human error rather than a control deficiency. In addition, OCFO/NFC had not performed user acceptance testing during fiscal year 2006 due to staffing deficiencies and large backlogs caused by Hurricane Katrina. However, user acceptance testing had been reinstated in August 2006.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
13. OCFO/NFC ensures its systems software are updated and protected from malicious code by: a. Giving particular attention to the process utilized to build, change, or implement the system and b. maintaining a flaw remediation process with patch management, malicious code screening, and checks, along with personnel supervision, procedural reviews.	OCFO/NFC C&A procedures recognize the importance security-related documentation, including a trusted facility manual that explains how to operate the system in the most secure manner. These procedures also state that standard operating procedures may be included in this manual or maintained separately. The OCFO/NFC management directive for IT infrastructure changes specifies responsibilities and procedures for changes to hardware and operating system software. This directive requires the requestor to submit a change request; test the change in a test environment and document the results or the reason the change was not tested; and provide a method of validation to ensure that the change operates as intended in the production environment. Branch chiefs verify that testing was performed, review the method of validation, and approve the request. OCFO/NFC management directives and other guidance also establish policies and procedures for preventing information system vulnerabilities by requiring anti-virus software, prohibiting users from installing unauthorized software, and implementing network system security patches. In addition, the OCFO/NFC management directive for network vulnerability self assessments requires vulnerability scans to be performed at least quarterly. 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 within 45 days of identification.	We interviewed OCFO/NFC officials and reviewed system configuration documentation. We judgmentally selected 10 of the 222 non-emergency and 5 of the 41 emergency general support system changes that were implemented between October 1, 2005, and March 4, 2006, and reviewed OCFO/NFC documentation associated with the changes. We reviewed vulnerability scan reports from March through June 2006 and documentation identifying vulnerabilities classified as false positives or acceptable risks.	OCFO/NFC controls were suitably designed to achieve the control objectives. In addition, OCFO/NFC controls were operating effectively to ensure that system software change requests were appropriately documented, tested and approved. However, OCFO/NFC controls had not consistently ensured that identified vulnerabilities were resolved in a timely manner. We identified 84 easily exploitable vulnerabilities that were identified in March 2006, but remained open in June 2006. As of July 8, 2006, 15 of these had been declared as either false positives or acceptable risks, 68 were included in action plans, and 1 remained open. The 15 declarations for false positives or acceptable risk occurred, on average, more than 85 days after their identification. We also identified 68 additional easily exploitable vulnerabilities that were identified in January 2006 but not resolved until April 2006. OCFO/NFC officials told us that the delay in executing declarations and addressing vulnerabilities was due, in part, to the limited number of staff available after Hurricane Katrina and the increased downtime associated with traveling to and from the interim computing facility. OCFO/NFC began rerunning scans on a weekly basis in May 2006. In addition, the monthly plan of actions and milestones reporting process began tracking the resolution of items noted.

CONTROL OBJECTIVE	CONTROL ACTIVITIES	TESTS PERFORMED	CONCLUSION
14. OCFO/NFC ensures its service continuity control objectives are met by: a. Providing continuity of support and developing, testing, and maintaining the continuity of operations plan to provide for business resumption and to ensure continuity of operations during emergencies or disasters. This control also includes the backup capability available for system recovery; b. establishing an incident response capability to prepare for, recognize, report, and respond to the incident and return the IT system to operational status; and c. controlling access to and disposal of data media.	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. Division directors and 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 states that OCFO/NFC conducts semi-annual tests at the recovery operations center and alternate work sites. In addition, OCFO/NFC management directives also define standards, procedures, and responsibilities for preparation, implementation, and maintenance of disaster recovery backup and restore jobs for the mainframe environment that require daily backups and storage at an offsite location. The OCFO/NFC Information Security Program also 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. In addition, the OCFO/NFC management directive for sanitizing storage media containing sensitive data requires either degaussing or shredding data storage media that will not be used again and either degaussing or overwriting for data storage media that will be transferred, donated, stored, or reused.	We interviewed OCFO/NFC personnel, and reviewed the OCFO/NFC Continuity of Operations Plan. We also reviewed the OCFO/NFC Computer Incident Handling Guide and ST&E for the mainframe general support system.	OCFO/NFC controls were suitably designed to achieve the control objectives. We also concluded that OCFO/NFC controls were operating effectively except to ensure continuity of operations during emergencies or disasters. While OCFO/NFC had updated its Continuity of Operations Plan to reflect their current operating environment, it had not yet completed updates of the associated procedures for recovering computer operations to ensure that architectural changes that occurred with the move to the interim computing facility or tested recovery of operations at the new recovery operations center. OCFO/NFC officials estimated that they would complete the disaster recovery procedure update by September 30, 2006, after performing a limited test to validate the new recovery site set up and equipment. OCFO/NFC officials also told us they had scheduled another test for May 2007.