U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Fiscal Year 2005 – Review of the Office of the Chief Financial Officer/National Finance Center General Controls

Report No. 11401-22-FM
November 2005

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

November 15, 2005

REPLY TO
ATTN OF: 11401-22-FM

TO: Patricia E. Healy
Acting Chief Financial Officer
Office of the Chief Financial Officer

THROUGH: Kathleen A. Donaldson
Senior Program Analyst
Office of the Chief Financial Officer
Planning and Accountability Division

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

SUBJECT: Fiscal Year 2005 – Review of the Office of the Chief Financial Officer/National Finance Center General Controls

This report presents the results of our review of the internal controls at the Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) as of July 30, 2005. The audit was conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States including the American Institute of Certified Public Accountants Professional Standards AU Sections 316, 319, and 324 as amended by applicable Statements on Auditing Standards (SAS), commonly referred to as a SAS 70 audit. The report contains a qualified opinion on the control objectives and techniques of OCFO/NFC (as identified by the center and documented in exhibit A to this report) during the period October 1, 2004, through July 30, 2005. Subsequent to July 30, 2005, OCFO/NFC officials asserted that they believed compensating controls have been implemented to mitigate the weaknesses we reported. However, due to the effects of Hurricane Katrina, we were unable to evaluate the effectiveness of the compensating controls; therefore, we offer no opinion on the effectiveness of those controls.

The accuracy and reliability of the data processed by OCFO/NFC and the resultant reports ultimately rests with the customer agency and any accompanying compensating controls implemented by such agency. The projections of any conclusions based on our audit findings to future periods are subject to the risk that changes may alter the validity of such conclusions. This report is intended solely for the management of OCFO/NFC, its customer agencies, and their auditors.

We appreciate the courtesies and cooperation extended to us during the audit.

Executive Summary

Fiscal Year 2005 - Review of the Office of the Chief Financial Officer/National Finance Center General Controls

This report presents the results of our review of the internal controls at the Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) as of July 30, 2005. While the center has taken significant corrective actions during the fiscal year, the report contains a qualified opinion on the internal control structure because certain control policies and procedures, as described in the report, were not suitably implemented and/or operating at the time of our review.

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

OCFO/NFC had progressed in its efforts to establish role-based security; however, we still found OCFO/NFC personnel had access to critical system files and a payroll application that exceeded what was required to perform their job functions. OCFO/NFC had also made progress in meeting Office of Personnel Management's requirements for assigning risk levels and performing background investigations; however, OCFO/NFC had not completed its process for all individuals with access to or significant responsibilities over critical applications and data. Finally, OCFO/NFC had taken additional steps to strengthen its controls over system software, including the implementation of a change control management system. OCFO/NFC was documenting change requests and approvals; however, we still found that OCFO/NFC needed to ensure that it completes documentation of change testing.

Recommendations In Brief

OCFO/NFC is in the process of implementing corrective actions on the weaknesses we identified based on prior Office of Inspector General recommendations. Therefore, we make no additional recommendations.

Agency Response

Subsequent to July 30, 2005, OCFO/NFC officials asserted that they believed compensating controls have been implemented to mitigate the weaknesses we reported.

OIG Position

Due to the effects of Hurricane Katrina, we were unable to evaluate the effectiveness of the compensating controls; therefore, we offer no opinion on the effectiveness of those controls. We will audit the general control environment at OCFO/NFC during fiscal year 2006, including any identified compensating controls.

Abbreviations Used in This Report

APF	Authorized Program Facility
FISCAM	Federal Information System Controls Audit Manual
HSPD	Homeland Security Presidential Directive
ID	Identification
IRMD	Information Resources Management Division
IT	Information Technology
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OMB	Office of Management and Budget
USDA	U.S. Department of Agriculture

Table of Contents

Background and Objectives

Background

The National Finance Center (NFC), located in New Orleans, Louisiana, is operated by the U.S. Department of Agriculture's (USDA) Office of the Chief Financial Officer (OCFO). The center operates administrative and financial systems that support the missions of USDA and other Federal Departments. Most importantly, the center is responsible for developing and operating the Payroll/Personnel System.

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

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

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

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

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

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

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

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

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

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

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

Objectives

Our objectives were to perform testing necessary to express an opinion about (1) whether the control objectives and techniques in exhibit A for OCFO/NFC present fairly, in all material respects, the aspects of the OCFO/NFC policies and procedures in place and operating during the period October 1, 2004, through July 30, 2005; (2) whether this control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily; and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

Report of the Office of Inspector General

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

We have examined the control objectives and techniques identified in exhibit A for the U.S. Department of Agriculture's (USDA), Office of the Chief Financial Officer/National Finance Center (OCFO/NFC). Our examination included procedures to obtain reasonable assurance about (1) whether the control objectives and techniques of OCFO/NFC present fairly, in all material respects, the aspects of OCFO/NFC's policies and procedures in place and operating effectiveness during the period October 1, 2004, through July 30, 2005; (2) whether the control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily; and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives. The control objectives were specified by OCFO/NFC.

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

OCFO/NFC has made significant progress in fiscal year 2005 to address prior audit recommendations; however, OCFO/NFC needs to continue its improvements to ensure the effectiveness of its controls. We continued to identify weaknesses in OCFO/NFC's ability to ensure that access to its systems and applications were adequately controlled, required background investigations were conducted, and ensure that system software change control planning and testing was adequately documented.

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

Also, in our opinion, except as discussed above, the policies and procedures that were tested, as described in the exhibit, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified were achieved during the period from October 1, 2004, through June 30, 2005. The scope of this engagement did not include tests to determine whether control objectives not listed in exhibit A were achieved; accordingly, we express no opinion on achievement of controls not included in exhibit A.

Subsequent to July 30, 2005, OCFO/NFC officials asserted that they believed compensating controls have been implemented to mitigate the weaknesses we reported. However, due to the effects of Hurricane Katrina, we were unable to evaluate the effectiveness of the compensating controls; therefore, we offer no opinion on the effectiveness of those compensating controls. It is important to note that while various management, manual, and reconciliation controls help detect potential irregularities or improprieties, these types of compensating controls are not preventative controls. Thus the vulnerabilities we noted increase the risks of inappropriate disclosure and modification of sensitive data, destruction of data, or misuse or damage of computer resources.

The scope of this engagement did not include tests to determine whether control objectives not listed in exhibit A were achieved; accordingly, we express no opinion on achievement of controls not included in exhibit A. Further, the scope of this engagement did not include tests to determine whether control objectives were achieved subsequent to the natural disaster of Hurricane Katrina; accordingly, we express no opinion on the service center descriptions or achievement of control objectives subsequent to August 25, 2005. The OCFO/NFC service center description during its recovery efforts and subsequent operations is included as exhibit B.

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

The description of policies and procedures at OCFO/NFC is as of July 30, 2005, and covers the period from October 1, 2004, through July 30, 2005. Any projections of such information to the future are subject to the risk that, because of change, they may no longer portray the system in existence. The potential effectiveness of specific policies and procedures at OCFO/NFC is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. The projections of any conclusions, based on our findings, to future periods are subject to the risk that changes may alter the validity of such conclusions. Furthermore, the accuracy and reliability of data processed by OCFO/NFC and the resultant reports ultimately rests with the user agency and any compensating controls implemented by such agency.

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

/s/

ROBERT W. YOUNG
Assistant Inspector General
for Audit

July 30, 2005

Findings and Recommendations

Section 1. Access Controls and Background Investigations

Access controls, such as user identifications (ID) and passwords, protect applications and data against unauthorized access. Administrators should provide only authorized users access to applications and data, and ensure that such access is limited to what is needed to perform the user's job functions. In addition, managers need to ensure that appropriate background checks are performed on persons with significant control and responsibilities over applications and data. Without strong access controls and proper background checks, privacy and financial data is at increased risk to loss, disclosure, and unauthorized modification.

Finding 1

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

OCFO/NFC had progressed in its efforts to establish role-based security; however, we still found OCFO/NFC personnel had access to critical system files and a payroll application that exceeded what was required to perform their job functions. In some instances, the access provided also violated separation of duty controls. OCFO/NFC had not completed its corrective actions to review and limit system and application access based on job responsibilities through implementing a role-based access methodology. Inappropriate access increases the vulnerability of OCFO/NFC applications and its payroll/personnel systems to fraudulent activity.

OCFO/NFC directives state that OCFO/NFC employees should be granted access authority only to those resources required to carry out their jobs and that the number of employees with authorized access will be limited to the minimum number needed to effectively perform the required functions.[3] OCFO/NFC directives also state that the separation of functions will be used as an internal control to guard against personnel having the opportunity to commit and/or conceal intentional or unintentional alteration, destroy data or software, or view data that is outside the scope of the employees normal job assignments.[4] In addition, if the separation of incompatible functions is not possible, compensating controls must be used.

In November 2003, we reported that OCFO/NFC personnel had access to operating system files and Authorized Program Facility (APF) library files in excess of what was needed to perform their job functions. As a result of that

[3] Title VII, Chapter 11, Management Directive No. 27.
[4] Title VII, Chapter 11, Directive 40.

audit, OCFO/NFC agreed to implement role-based access profiles to limit access to these critical system files. Our followup work this year found that Information Resources Management Division had not completed the process of refining their role-based access profiles. Therefore, we continued to find unnecessary access to 6 of the 17 sensitive operating system libraries and 42 of the 72 APF libraries that we reviewed. After we brought these unnecessary accesses to OCFO/NFC's attention, they began removing or limiting access on the instances we identified.

OCFO/NFC management informed us that they had implemented compensating controls in an effort to minimize the risk of unnecessary access to system files and critical payroll applications. These compensating controls included reports that monitored access to sensitive applications and system files. However, we were unable to test the compensating controls that OCFO/NFC officials had placed into operation; therefore, we offer no opinion about whether those compensating controls are operating effectively.

Since we have recommended that OCFO/NFC implement role-based access profiles in our prior audit, and OCFO/NFC is making progress in establishing these profiles, we are making no further recommendations at this time.

Finding 2 OCFO/NFC Has Made Significant Progress, but Not All Background Investigations Had Been Completed

OCFO/NFC has made progress in meeting Office of Personnel Management's requirements for assigning risk levels and performing background investigations; however, OCFO/NFC has not completed its process for all individuals with access to or significant responsibilities over critical applications and data. Until these requirements are met, OCFO/NFC faces the risk of exposing its information resources to loss or harm that could be caused by these individuals.

The Office of Management and Budget (OMB) requires that security-related responsibilities of offices and individuals throughout the entity should be clearly defined to include those of (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators.[5]

[5] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.

Further, Executive Order No. 10450, as amended, established general requirements that every competitive service position be designated at a risk level commensurate with the public trust responsibilities of the position, and be made subject to investigation.[6] In 1998, OCFO/NFC issued its own directive to implement the background investigation requirements.[7]

In response to our fiscal year 2004 audit, OCFO/NFC completed its risk rating and background investigations on the specific information technology specialists we reported as not having a proper background investigation. However, until final background investigations are completed, OCFO/NFC has implemented compensating controls, such as initial screening of new employees, which its management has indicated reduced their risk to an acceptable level. Due to the effects of Hurricane Katrina, we were unable to evaluate these compensating controls and offer no opinion on their effectiveness.

Since OCFO/NFC is in the process of implementing our prior recommendations, we are making no further recommendations at this time.

[6] Executive Order No. 10450, "Security Requirements for Government Employment," signed April 27, 1953.

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

Finding 3

Controls Over System Software Change Testing Need Improvement

OCFO/NFC has taken additional steps to strengthen its controls over system software, including the implementation of a change control management system. However, OCFO/NFC needs to strengthen its controls over documenting its testing results.[8] Although OCFO/NFC was documenting change requests and approvals, we still found that OCFO/NFC needs to ensure that it completes documentation of change testing. Despite its own policies to document approval and testing, OCFO/NFC had not adequately enforced its established guidance. Until these issues are addressed, OCFO/NFC will not be able to provide adequate assurance that system software changes have been sufficiently tested to ensure that they will operate as intended and not cause unforeseen adverse impacts.

The National Institute of Standards and Technology (NIST) requires organizations to document and control changes to information systems and recognizes that a configuration change control involves the systematic test/evaluation of proposed changes.[9] In January 2005, OCFO/NFC updated its directive that establishes policies, procedures, and responsibilities for making changes to its information technology (IT) infrastructure.[10] This directive also required that documentation be maintained on the tests performed in a test environment, the testing results, or the justification why no testing was performed. Further, OCFO/NFC's IT Infrastructure Change Management Desk Procedures reiterates that testing documentation related to the implementation of an approved IT change request must be recorded using one of the following methods:

- Attaching external documentation which validates or affirms that test results were captured and worked during the test phases in the test environment and/or validated during Quality/Assurance verification;

- documenting how testing was performed and the results of testing in the change request; or

[8] Audit Report No. 11401-9-FM, "Selected Information Technology General Controls at the National Finance Center Need Strengthening," dated March 2002; Audit Report No. 11401-15-FM, "Fiscal Year 2003 National Finance Center Review of Internal Controls," dated November 2003; Audit Report No. 11401-20-FM, "Fiscal Year 2004 – Review of the National Finance Center General Controls," dated October 25, 2004.

[9] NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," dated February 2005.

[10] Title VII, Chapter 11, Directive 59, "Information Technology Infrastructure Change Management (Revision 2)," January 6, 2005.

- relating the change request to other change requests that document testing.

We identified 244 system software changes that occurred between October 1, 2004, and June 16, 2005, on the UNIX, Windows, and Mainframe platforms. Using commercially available audit and analysis software, we judgmentally selected 15 system software changes, 5 from each of the 3 platforms. OCFO/NFC provided us the detailed records from their change management system for the 15 changes. Those detailed records showed that the 15 changes we selected were approved by management; however, only 9 of the 15 changes involved changes to production software that would have required testing.

OCFO/NFC did not maintain testing plans or results in its tracking system for seven of the nine changes that would have required testing. Subsequently OCFO/NFC was able to provide adequate documentation to support that three of the seven changes were evaluated by system users in a test environment. Out of the remaining four changes we sampled, OCFO/NFC officials informed us that two had been tested under a related change request, but failed to document this fact as required by OCFO/NFC operational procedures; while the remaining two had insufficient documentation to support the testing that occurred. Much of the documentation OCFO/NFC ultimately supplied was in the form of e-mails describing the steps taken to test the change. While we accepted this evidence in light of the center's improvements in this area, OCFO/NFC needs to ensure that future system software change testing be adequately documented.

In response to this audit, OCFO/NFC informed us that they believed that adequate documentation existed for the testing of our sampled changes; however, OCFO/NFC agreed that OCFO/NFC could enhance its change management process by including the testing documentation or at least reference to a summary of the test results in the change management ticket.

Since OCFO/NFC is in the process of implementing our prior recommendations, we are making no further recommendations at this time.

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

The objectives of our examination were to perform testing necessary to express an opinion about (1) whether the control objectives and techniques identified in this exhibit present fairly, in all material respects, the aspects of the Office of the Chief Financial Officer/National Finance Center's (OCFO/NFC) policies and procedures in place from October 1, 2004, through July 30, 2005; (2) whether the control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily; and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

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

Our testing of OCFO/NFC's control structure policies and procedures was restricted to the control objectives and the related policies and procedures listed in the matrices in this exhibit. Our testing was not intended to apply to any other procedures not included in the aforementioned matrices or to procedures that may be in effect at user organizations. Further, the scope of this engagement did not include tests to determine whether control objectives listed in the matrices or elsewhere were achieved subsequent to the natural disaster of hurricane Katrina; accordingly, we express no opinion on the achievement of control objectives subsequent to August 25, 2005.

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

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

Control Objective	Control Techniques	Tests Performed	Conclusions
1. Ensure that systems function according to the requirements documentation and are user friendly.	a. Participate in the development of system implementation plans, system testing plans, and acceptance testing plans.	Interviewed OCFO/NFC personnel and reviewed applicable directives and procedures. Selected and reviewed system software changes that were implemented between October 1, 2004, and June 16, 2005.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed in operation and were operating effectively, except as noted below. OCFO/NFC was still not able to provide adequate testing documentation to support all sampled changes. (See Finding No. 3.)
2. Ensure that entries added to table management are valid and comply with Treasury, OMB, and other applicable Government regulations and management policies to minimize errors, fraudulent entries, and unauthorized data.	a. Restrict access to specific personnel to process, add, change, or delete data in table management to minimize possible adverse impact on processing.	Reviewed access to a critical payroll system. Made inquiries to responsible OCFO/NFC programmers. Reviewed applicable OCFO/NFC directives.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed in operation, but not operating effectively. OCFO/NFC personnel had access to critical Payroll/Personnel Systems that was not within the scope of their job functions. (See Finding No. 1.) We found that OCFO/NFC had made significant progress in completing background investigations; however, it had not fully implemented its corrective actions. (See Finding No. 2.)

Control Objective	Control Techniques	Tests Performed	Conclusions
3. Ensure that manually processed salary payments are accurate and timely, and comply with regulations.	a. Assign Form AD-343, Payroll Action Requests, Document Tracking System External, Special Payroll Processing System (SPPS), Quick Service Wires, or other requests for manual payments promptly to unit accounting technicians, payroll technicians, and clerks to ensure timely processing in SPPS.	Reviewed Federal guidelines regarding need for unique login identifiers. Reviewed access controls over Special Payroll Process System. Made inquiries to responsible OCFO/NFC personnel.	The control structure policies and procedures were not suitably designed to achieve the control objective specified. We found access control weaknesses that violate separation of duties controls, and excessive access that was not needed to perform the user's job functions. (See Finding No. 1.) We found that OCFO/NFC had made significant progress in completing background investigations; however, it had not fully implemented its corrective actions. (See Finding No. 2.)
4. Develop and maintain an effective information systems security program in compliance with OMB Circular No. A-130, Departmental Regulation 3140, Federal Information Processing Standards, Federal Information Security Management Act (FISMA), and NIST.	a. Control access to resources.	Interviewed responsible OCFO/NFC personnel. Performed vulnerability assessments on selected servers and network devices. Reviewed applicable OCFO/NFC policies and procedures.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation, and were operating effectively.

Control Objective	Control Techniques	Tests Performed	Conclusions
5. Ensure that access to online systems is controlled.	a. Define and implement policies and procedures for issuing user ID and password administration. b. Develop security which restricts access to defined data and programs that are necessary to perform a specific job function. c. Reports of incidents of suspected inappropriate access are produced and reviewed. d. Monitor user activity and provide reports to management for inactive accounts. e. Provide access through secure connectivity with approved security form.	Reviewed the mainframe security software control options that impact password administration. Requested and obtained listings of user IDs from OCFO/NFC and selected client agencies to determine whether user IDs were granted only to employees whose job responsibilities required such access. Reviewed access reports for a sensitive payroll application to identify individuals granted inappropriate access and separation of duty based on their job function. Reviewed the results of a commercially available software product that was used to identify vulnerabilities in operating systems that use Transmission Control Protocol/Internet Protocol. Interviewed responsible OCFO/NFC personnel for selected activities and functions reviewed.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed in operation but not operating effectively. We found access control weaknesses that violate separation of duties controls, and excessive access that was not needed to perform the user's job functions. (See Finding No. 1.) We found that OCFO/NFC had made significant progress in completing background investigations; however, it had not fully implemented its corrective actions. (See Finding No. 2.)

Control Objective	Control Techniques	Tests Performed	Conclusions
6. Ensure that access to data is controlled to minimize unauthorized access.	a. Provide access to sensitive or critical data only when needed for processing.	Reviewed monitoring reports, and applicable procedures. Reviewed access reports for a sensitive payroll application to identify individuals granted inappropriate access and separation of duty based on their job function. Interviewed responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed in operation, but were not operating effectively. We found access control weaknesses that violate separation of duties controls, and excessive access that was not needed to perform the user's job functions. (See Finding No. 1.) We found that OCFO/NFC had made significant progress in completing background investigations; however, it had not fully implemented its corrective actions. (See Finding No. 2.)
7. Ensure that OCFO/NFC provides security, confidentiality, integrity, and availability of software and data on mainframe and personal computers.	a. Inform employees of the Automated Data Processing security program and their responsibilities.	Reviewed OCFO/NFC organization chart, security directives, functional statements, and made inquiries to OCFO/NFC personnel to determine actual procedures in place. Reviewed applicable OMB and FISMA requirements.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed in operation to ensure confidentiality, but not operating effectively. We found access control weaknesses that violate separation of duties controls, and excessive access that was not needed to perform the user's job functions. (See Finding No. 1.) We found that OCFO/NFC had made significant progress in completing background investigations; however, it had not fully implemented its corrective actions. (See Finding No. 2.)

Control Objective	Control Techniques	Tests Performed	Conclusions
8. Ensure that access to resources and records is limited to authorized individuals, and accountability for custody and use of resources is assigned and maintained.	a. Maintain adequate segregation of duties to prevent an individual from performing two or more incompatible functions.	Reviewed access reports for a sensitive payroll application to identify individuals granted inappropriate access and separation of duty based on their job function.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed in operation, but were not operating effectively. We found access control weaknesses that violate separation of duties controls, and excessive access that was not needed to perform the user's job functions. (See Finding No. 1.) We found that OCFO/NFC had made significant progress in completing background investigations; however, it had not fully implemented its corrective actions. (See Finding No. 2.)
9. Ensure that sensitive data that contain personal identifiers are adequately protected in compliance with the Privacy Act and Directive 55.	a. Verify that access to items or reports containing personal identifiers is restricted to only authorized persons who need the data to perform their job functions.	Reviewed access reports for a sensitive payroll application to identify individuals granted inappropriate access and separation of duty based on their job function. Made inquiries to responsible OCFO/NFC personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed in operation, but were not operating effectively. We found access control weaknesses that violate separation of duties controls, and excessive access that was not needed to perform the user's job functions. (See Finding No. 1.) We found that OCFO/NFC had made significant progress in completing background investigations; however, it had not fully implemented its corrective actions. (See Finding No. 2.)

Exhibit B – Service Center Description During Hurricane Recovery

National Finance Center's
Revised Service Center Description
Changes in Operations as a Result of
Hurricane Katrina

The United States Department of Agriculture's (USDA) Office of the Chief Financial Officer's (OCFO) National Finance Center (NFC) operated from its location in New Orleans, Louisiana for fiscal year 2005 from October 1, 2004 through August 28, 2005. As a result of Hurricane Katrina, the OCFO/NFC implemented its Disaster Recovery Plan (DRP). On Friday, August 26, the OCFO/NFC began implementing the DRP, which included the organized shut-down of operations, including the running of nightly cycles, running back-up tapes of data and concurrently dispatching advance teams to the Alternate Work Sites (AWS). Advance teams were dispatched to Philadelphia, PA for computer operations and to Grand Prairie, TX for the operational staffs. According to the OCFO/NFC's DRP and the Continuity of Operations Plan (COOP), the OCFO/NFC successfully completed re-establishing computer operations during the following week and successfully operated its Payroll/Personnel System (PPS) for Pay Period 17 without interruption to its customers. Currently, OCFO/NFC is continuing to operate under the COOP and successfully completed year-end closing of the fiscal year.

During the month of September 2005, OCFO/NFC operated under unusual circumstances, curtailing many non-critical operations while maintaining critical operations with controls for these operations remaining in place and operational. OCFO/NFC maintained operating the PPS. As of Pay Period 17, OCFO/NFC implemented two new organizations into the PPS increasing the number of Federal employees payroll processed by OCFO/NFC to more than 560,000 employees. OCFO/NFC continued operating all USDA systems, financial and administrative payment systems and customer specific systems, such as, for the Thrift Investment Board, the Thrift Savings Plan operations, for the Office of Personnel Management, the Direct Premium Remittance System and the Federal Employees Health Benefits Centralized Enrollment Clearinghouse System. For these and other systems, internal controls remained operational. However, some operations were curtailed, such as, system enhancements and customer requested system changes. Under current operations and limited personnel resources, OCFO/NFC is processing only legally mandated system changes. These systems changes follow OCFO/NFC change request procedures as when in operation at New Orleans. System testing, supervisory review and approval along with the involvement of the Information Systems Quality Assurance Office are still established controls in place during OCFO/NFC's COOP operations.