USDA

U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

# SELECTED INFORMATION TECHNOLOGY GENERAL CONTROLS AT THE NATIONAL FINANCE CENTER NEED STRENGTHENING

**Report No.**
**11401-9-FM**
**March 2002**

USDA

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20250

DATE: March 18, 2002

REPLY TO<br>
ATTN OF: 11401-9-FM

SUBJECT: Selected Information Technology General Controls at the National Finance Center Need Strengthening

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

This report presents the results of our audit of (1) information technology (IT) application change controls over the financial and administrative systems developed and maintained by the National Finance Center (NFC) and (2) other IT general controls over NFC's Special Payroll Processing System. Your February 15, 2002, response to our draft report is included in its entirety in exhibit A, with excerpts incorporated in the findings and recommendations section of the report where appropriate.

Based upon this response, we agree with the management decisions for Recommendations Nos. 1-6, 8-10, 12, 14, 16-20, and 24. While you concurred with the remaining recommendations, additional information regarding the proposed corrective actions is needed before we can accept the management decisions for Recommendations Nos. 7, 11, 13, 15, and 21-23. Please refer to the OIG Response sections of the report for specific details.

In accordance with Department Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation for the cited recommendations where management decisions have not been reached. Please note that the regulation requires management decisions to be reached on all findings and recommendations within a maximum of 6 months from report issuance and final action is to be taken within 1 year of each management decision.

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

/s/

RICHARD D. LONG<br>
Assistant Inspector General<br>
for Audit

# EXECUTIVE SUMMARY

## U.S. DEPARTMENT OF AGRICULTURE
## SELECTED INFORMATION TECHNOLOGY GENERAL CONTROLS AT THE NATIONAL FINANCE CENTER NEED STRENGTHENING
## AUDIT REPORT NO. 11401-9-FM

## RESULTS IN BRIEF

The National Finance Center's (NFC) application change controls were not operating as effectively as needed to ensure that all modifications to applications maintained by its Application System Division (ASD) were properly tested and approved prior to implementation. These controls are important since they help prevent errors in software programming and the insertion of unauthorized computer program code into an application. In addition, without strengthened controls, incompletely tested or unapproved software could result in erroneous data being processed that, depending on the application, could lead to losses or incorrect outcomes in the payroll/personnel, administrative payments, accounts receivable, property management, and accounting systems that NFC maintains. In fiscal year 2001, these systems disbursed or authorized more than $43 billion in salary and administrative payments for both U.S. Department of Agriculture (USDA) and non-USDA agencies.

In prior Office of Inspector General audit reports, we have reported that modifications were made to application programs maintained by NFC without adequate authorization and testing, which resulted in data being processed incorrectly and caused subsequent modifications to be made to correct the erroneous information processed. We continued to find these kinds of problems. Specifically, we found that NFC needed to strengthen their controls in the following key areas (1) obtaining user approval of the functional requirements developed by ASD; (2) documenting software testing performed by ASD; and (3) performing acceptance testing, which determines if the software satisfies the requirements of the system owners, users, and operators, for certain application maintenance projects initiated by ASD. Also, NFC had not sufficiently limited "emergency" changes, which are high risk program modifications because full testing is waived prior to implementation. In addition, appropriate testing was not documented and user approval was not obtained for "emergency" changes within a reasonable period after implementation. Almost one-half (180 of 380) of ASD's software maintenance projects for which changes were implemented between October 1, 2000, and April 3, 2001, were classified as “emergency”. These projects accounted for about 20 percent of the programs changed during this period.

The types of application change control issues that we identified continue to persist mainly because the internal controls in place were either not adequately designed or not operating effectively. Consequently, we again found instances where data was processed incorrectly and/or subsequent modifications were required to correct errors because changes were either incomplete or not adequately tested. For example, we reviewed 11 “emergency” changes implemented between October 1, 2000, and April 3, 2001, to determine if any of these changes were made to fix errors caused by prior program changes that were made incorrectly. We found that six of the eleven, or 55 percent, were processed to fix problems resulting from previous changes that were either incomplete or had caused unintended consequences. Until NFC implements strengthened application change controls, it will continue to face increased risk of unauthorized and incorrect software changes and increased costs associated with making subsequent modifications to fix incorrect changes.

In addition to allowing changes to production software through the application maintenance process, NFC also permits production changes to be made through “special production processing.” These special processing routines allow changes to production data outside of the normal production methods and controls. This bypassing of established control techniques makes “special production processing” a high risk processing routine (e.g. production data could be inappropriately modified because the management controls built into the application maintenance process and individual applications are bypassed). In our audits of NFC internal controls for fiscal years 1996 and 1997, we reported material internal control weaknesses relating to “special processing” and that this process was commonly used to make changes to data files, which could result in inaccurate or unauthorized changes to records maintained by NFC.

NFC recognized that controls over “special production processing” needed improvement and strengthened controls over this area by issuing an updated directive in August 2001. The revised directive now requires user approval for “special production processing” requests, which should reduce the risk associated with this processing routine. We believe, however, that additional controls are necessary. For example, we found instances where “special production processing” was incorrectly used to perform routine processes because NFC had not established normal production programs and/or procedures that would have strengthened controls. We determined that over 1,000 “special production processing” requests were implemented for ASD applications between October 1, 2000, and May 15, 2001. Unless controls over “special production processing" are strengthened, the payroll/personnel, administrative payments, accounts receivable, property management, and accounting systems maintained by NFC will unnecessarily be placed at risk of unauthorized modifications to production data, which could ultimately lead to improper payments.

We found that NFC was not maintaining an adequate audit trail for "emergency" software change and "special production processing" requests. Consequently, NFC cannot appropriately ensure that "emergency" software change and "special production processing" requests can easily be traced from initiation to the final approval or from the change back to the initial user authorization.

We also identified weaknesses in certain general controls specific to the Special Payroll Processing System (SPPS). For example, access to SPPS and other information in the production payroll/personnel databases was not adequately restricted. We found that 78 of the 254 NFC employees that were granted update access to the quick service request, indebtedness, and death case functions of SPPS did not need this level of access to perform their job functions. This was caused mainly because SPPS had been designated as an "update only" system and "read only" access was not available for the indebtedness and death case functions. We also determined that four application programmers were unnecessarily allowed access to a powerful database utility that could be used to circumvent the security controls built into the payroll/personnel applications to improperly read and modify both SPPS data and other payroll/personnel information because NFC was not reviewing access to this powerful database utility to ensure that it was appropriate. As a result, NFC faces increased risk that certain payroll transactions may be improper or inaccurate and sensitive personnel information is vulnerable to inadvertent or deliberate unlawful disclosure.

In addition, we found computer security management weaknesses that could impact the effectiveness of information technology (IT) controls over not only SPPS, but other NFC applications as well. For example, NFC had not developed a security plan for the Payroll/Personnel System, which would encompass SPPS, or the other four major applications for which the center was responsible in fiscal year 2001.

## KEY RECOMMENDATIONS

To strengthen application change controls over ASD applications, we recommended that NFC establish controls and guidance to ensure that:

- user approval of the functional requirements documents developed by ASD is obtained,

- software testing performed by ASD is adequately documented, and
- acceptance testing is performed for all application changes.

We also made recommendations to improve controls over "emergency" changes to ASD applications. Specifically, we recommended that NFC:

- Establish controls to ensure that "emergency" changes are limited to those application changes that require immediate implementation,
- develop guidance that clearly defines the types of testing to be performed prior to implementation for "emergency" changes and documentation requirements for such testing, and
- implement controls to ensure that "emergency" changes are subsequently approved by user management within 30 days.

In addition, we made recommendations to:

- Help limit the number of "special production processing" actions related to ASD applications by (1) developing production programs and/or processes to perform these actions to accomplish routine actions, such as updating tables, that are currently performed through "special production processing" and (2) expanding current procedures to identify programming or systemic problems that need to be addressed to minimize the need for "special production processing" actions;
- ensure that "emergency" software change and "special production processing" requests can easily be traced from initiation to the final approval or from the change back to the initial user authorization;
- reduce the number of staff members allowed to perform SPPS transactions by allowing "read only" access to all SPPS functions and re-evaluate access to SPPS to ensuring that staff members are assigned the minimum level of access required to perform their job functions;
- begin performing periodic reviews of access to the powerful database utility that can be used to circumvent the security controls built into the payroll/personnel applications to ensure that such access remains appropriate; and
- prepare system security plans for NFC's major applications.

## AGENCY RESPONSE

The Chief Financial Officer responded to our official draft report dated, February 15, 2002. In this response, the Chief Financial Officer generally concurred with the conditions and recommendations presented in the report and specified corrective actions addressing them.

## OIG POSITION

Accomplishing the planned corrective actions outlined in the Chief Financial Officer's response to our draft report should further strengthen controls over changes to NFC applications and "special production processing", and other IT general controls over SPPS. Based on the information contained in the response, we were able to accept the management decisions for 17 recommendations in the report. In order to achieve management decision on the seven remaining recommendations, we need additional information as noted in the applicable findings.

# TABLE OF CONTENTS

# INTRODUCTION

## BACKGROUND

Establishing controls over the modification of application software is important to ensure that only authorized changes are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all program modifications are properly authorized, tested and approved. At the National Finance Center (NFC), the change control process is described in the following Management and Administrative Directives:

- Title VII, Chapter 11, Directive 48, Application System Life Cycle, dated July 24, 1995, which describes the standards, procedures, and responsibilities for development, operation, and maintenance of software during the Application System Life Cycle;
- Title VII, Chapter 11, Directive 47, Scheduled Software Maintenance, dated December 24, 1998, which defines the policy, standards, and responsibilities for the control and scheduling of application software changes; and
- Title VII, Chapter 11, Directive 37, Application Software Testing, dated April 7, 1998, which establishes the standards for performing and documenting tests of application software throughout the software life cycle.

The NFC Scheduled Software Maintenance directive defines three types of software changes: "routine," "emergency," and "mandated." "Routine" changes are approved modifications or enhancements of application software that can be planned for implementation in a scheduled release. "Emergency" changes require immediate implementation to correct an error in the existing version of application software. "Mandated" changes are any changes other than (1) "emergency" changes and (2) "routine" changes implemented as part of a scheduled release. Thus, "mandated" changes are not limited to changes mandated by legislative requirements.

For "routine" and "mandated" changes to Application Systems Division (ASD) applications, change requests are generally documented on the Production Software Change Request form (NFC-1133), which is completed by ASD requirements personnel after (1) the maintenance project has been assigned an ASD project number and entered into the Planning and Tracking System (PATS), which is used to track the status and scheduling of projects along with the staffing resources used in project development, and (2) the requirements for the maintenance project have been finalized. The Production Software Change Request form is used to document ASD authorization for the change and also serves as the approval vehicle for the software requirements document. [1]

Once the change request and associated requirements are approved, ASD forwards a copy to (1) Information System Quality Assurance Office (ISQAO) so that the responsible ISQAO analyst can begin planning for acceptance testing and the Financial Services Division Directives and Analysis Branch (DAB) so that DAB can determine if user procedures and/or bulletins need to be updated. Then ASD codes the change and performs unit, integration, and/or system testing. Once ASD has determined that the change is ready for acceptance testing or implementation, the division completes forms that identify the specific software components that need to be added and/or updated and approves the change in the Change Authorization Tracking System (CATS). At this point, NFC performs acceptance testing, which culminates in the final approval for implementation from users, database administrators, scheduling, security administrators, and other technical personnel outside of ASD. Upon approval, ISQAO moves the components specified by ASD into production using a standardized procedure that documents the changes in a library activity file.

“Emergency” changes to ASD applications are also initiated by an ASD programmer using the Production Software Change Request form. However, in the interest of expediency, the requirements are not formally documented in a software requirements document. In addition, the Scheduled Software Maintenance directive allows full testing to be waived for emergency changes. Once ASD forwards the forms identifying the specific software components that will be affected and approves the change for implementation in CATS, ISQAO moves the change into production. Like “routine” and “mandated” changes, “emergency” changes are also documented in the library activity file.

NFC also allows “special production processing” (previously referred to as production deviations), which bypasses normal production programs and/or procedures or otherwise makes changes to production data outside of the normal production methods. NFC’s Title VII, Chapter 11, Directive 23, Special Production Processing,” which is dated August 24, 2001, establishes management controls over this process and states that “special production processing” should only take place when a requirement cannot be met through standard methods. According to this directive, application programmers initiate “special production processing,” develop and test the special production process, and then complete a

[1] The ASD software requirements document is used to describe the purpose of the change and what needs to be accomplished with enough detail to enable programmers to satisfy the requirements and testers to ensure that the changes satisfy the requirements.

Special Production Processing Request form (NFC-644), which is approved by an application programming supervisor or branch chief and the data owner and then forwarded to the Operations Branch (OB) for processing. OB logs the request into the Special Production Processing database, processes the "special production processing" request, updates the Special Production Processing database, and files the Special Production Processing Request form.

Both application change controls and other categories of information technology (IT) general controls can be applied at the application system level. These application-specific general controls include:

- Entitywide security planning and management controls, which provide a framework for continually managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer controls;
- access controls, which limit or detect access to computer resources and protect these resources against unauthorized modification, loss, and disclosure;
- segregation of duties controls, which prevent one individual from controlling key aspects of computer-related operations that would allow unauthorized actions or improper access to assets or records; and
- service continuity controls, which ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed.

NFC, which is operated by the Department of Agriculture's (USDA) Office of the Chief Financial Officer (OCFO) in New Orleans, Louisiana, develops and operates USDA administrative and financial systems. At NFC, ASD maintains the computer applications that process data for the payroll/personnel, administrative payments, accounts receivable, property management, and certain accounting systems[2]. In fiscal year 2001, these systems disburse or authorize more than $43 billion in salary and administrative payments for both USDA and other agencies.

The Special Payroll Processing System (SPPS) is one of NFC's payroll/personnel applications that allows users to process:

- Quick service salary payments when an employee is not paid through the automated payroll/personnel system or manual payment process as a result of late time and attendance processing, a late personnel action, a late accession, no check mailing address, or other errors in the Personnel Action Processing System;

[2] ASD maintains USDA's Central Accounting System but not its Foundation Financial Information System (FFIS).

- final payments for employees with debts not recorded in Administrative Billings and Collections System, such as educational loans, lost or stolen property, travel advances, and travel overpayments;
- unpaid compensation to the beneficiaries of a deceased employee; and
- manual payroll adjustment transactions for (1) employee details (i.e., grade, step, org, etc.), (2) check mailing and residence addresses and financial institution details, and (3) pay period details (i.e., payments, indebtedness, accounting, deductions, etc.).

## OBJECTIVES

Our audit objectives were to evaluate the design and test the effectiveness of (1) IT application change controls over applications developed and maintained by ASD, (2) management controls over "special production processing," and (3) selected IT general controls over SPPS.

## SCOPE

We reviewed controls established to ensure that (1) changes to the payroll/personnel, administrative payments, accounts receivable, property management, and accounting systems maintained by ASD and (2) changes to production data that were made through "special production processing" for the systems maintained by ASD were appropriately authorized, tested, and approved. To perform our testing, we selected samples of application changes made to ASD applications from October 1, 2000, through April 3, 2001. These samples were selected based upon a combination of judgmental and random selections. For each sample, we ensured that we included sample items that were directly related to SPPS were included and then randomly selected the remaining sample items from the universe associated with ASD applications. We also selected a sample of "special production processing" actions that affected ASD applications from October 1, 2000, through May 15, 2001, from production jobs that had the highest number of "special production processing" actions during this timeframe. In addition, we reviewed other general controls, such as security planning and management and access controls, as they applied specifically to SPPS.

We performed our work at NFC, which is located in New Orleans, LA, from March 2001 through August 2001 in accordance with generally accepted government auditing standards.

## METHODOLOGY

To accomplish our audit objectives, we (1) identified and reviewed NFC policies and procedures related to IT general controls and "special production processing;" (2) held discussions with NFC officials responsible for ASD application change controls, “special production processing,” and other IT general controls; and (3) conducted tests of controls in operation to determine whether IT general controls were in place, adequately designed, and operating effectively. As suggested by Office of Management and Budget (OMB) guidance on implementing the Government Information Security Reform Act, our evaluation was based on the guidance provided in General Accounting Office’s (GAO) Federal Information System Controls Audit Manual;[3] OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources;” and guidance issued by the National Institute of Standards and Technology (NIST).

[3] Federal Information System Controls Audit Manual, Volume I – Financial Statement Audits (GAO/AIMD-12.19.6, January 1999).

# FINDINGS AND RECOMMENDATIONS

## CHAPTER 1 APPLICATION CHANGE CONTROLS NEED STRENGTHENING

Controls over changes to application programs are critical in preventing unauthorized software programs or modifications to programs from being implemented. Key aspects of application change controls include ensuring that (1) software changes are properly authorized by the managers responsible for the program or operations that the application supports and (2) new and modified software programs are sufficiently tested and approved before they are implemented. We found that application change controls at NFC needed strengthening. As a result, NFC unnecessarily faces increased risk that incompletely tested or unapproved software changes could be implemented, resulting in erroneous data being processed that, depending on the application, could lead to losses or incorrect outcomes in the payroll/personnel, administrative payments, accounts receivable, property management, and accounting systems that NFC maintains. In fiscal year 2001, these systems disbursed or authorized more than $43 billion in salary and administrative payments for both USDA and non-USDA agencies.

In our fiscal year 1996 and 1997 reviews of NFC internal controls,[4] we reported that modifications were made to application programs without adequate authorization and testing, which resulted in data being processed incorrectly and subsequent modifications to correct the erroneous information. OCFO responded by stating that its initiative to move to Capability Maturity Model (CMM) Level 2[5] would ensure that necessary corrective action was accomplished. In our fiscal year 1998 review of NFC's internal control structure,[6] we reported that the application development and change control weaknesses we reported in fiscal years 1996 and 1997 still existed because NFC's CMM effort was halted during fiscal year 1998 because of other priorities. In NFC's description of its internal control structure as of September 30, 2000, the center reported several internal control structure and financial management system

[4] Audit Report No. 11401-2-FM, "Fiscal Year 1996 National Finance Center General Controls Review," dated March 1997 and Audit Report No. 11401-3-FM, "Fiscal Year 1997 National Finance Center Review of Internal Control Structure," dated March 1998

[5] The Software Engineering Institute, Capability Maturity Model (CMM) is an internationally recognized model for rating software development capabilities. CMM defines five levels of organizational maturity, with Level 5 being the highest. A Level 2 office has consistent project planning and execution, and through uniformity, the means to repeat software successes and avoid repeating software errors.

[6] Audit Report No. 11401-4-FM, "Fiscal Year 1998 National Finance Center Review of Internal Control Structure," dated September 1999.

weaknesses, including that it had not yet achieved CMM Level 2. NFC plans to achieve CMM Level 2 by September 30, 2003.

We continued to find problems with NFC's application change controls primarily because the controls in place were either not adequately designed or operating effectively. We reviewed user authorization, software testing, and approval controls for changes relating to 15 of the 200 "routine" and "mandated"[7] application maintenance projects for which changes were implemented from October 1, 2000, through April 3, 2001.[8] These projects were selected based on a combination of judgmental sampling to ensure that changes related to SPPS were included and random sampling among changes to the other ASD applications.

Our review disclosed that NFC was not adequately obtaining user approval of functional requirements;[9] documenting unit, integration, and system testing[10] performed by ASD; or performing acceptance testing[11] for "mandated" application maintenance projects initiated by ASD. These control problems continue to result in data being processed incorrectly and subsequent modifications to correct erroneous information. For example, six of the eleven "emergency" changes in our sample were required to fix problems resulting from previous application changes processed by ASD that were made incorrectly, incompletely, and/or had caused unintended consequences. (See Finding 4 for the results of our review of controls over "emergency" changes.) We also identified instances where (1) two "mandated" changes were needed to satisfy user requirements because the initial change was not done completely and (2) two of the "special production processing" requests that we reviewed were required to fix payroll/personnel data because a prior change did not function properly. Until NFC effectively implements improved application change controls, it will continue to face increased risk of unauthorized or incorrect software changes and increased costs associated with making subsequent modifications to fix the payroll/personnel, administrative payments, accounts receivable, property management, and accounting systems that ASD maintains.

[7] Title VII, Chapter 11, Directive 47, Scheduled Software Maintenance, dated December 24, 1998, defines three types of software changes: "routine," "emergency," and "mandated." "Routine" changes are approved modifications or enhancements of application software that can be planned for implementation in a scheduled release. "Emergency" changes require immediate implementation to correct an error in the existing version of application software and bypass testing controls prior to implementation. "Mandated" changes are any changes other than "emergency" changes and "routine" changes, which are not implemented as part of a scheduled release. Thus, "mandated" changes are not limited to changes mandated by legislative requirements.

[8] From October 1, 2000, through April 3, 2001, NFC implemented changes relating to 380 ASD application maintenance projects. These included 13 "routine," 187 "mandated," and 180 "emergency" changes. "Emergency" changes are discussed in Chapter 2.

[9] Functional requirements formally document all of the functions that the user requires the application to perform. At NFC, functional requirements for changes describe the purpose of the change and what needs to be accomplished.

[10] Unit testing checks individual program modules for typographic, syntactic, and logic errors. Integration testing is used to demonstrate that different software components work together properly. System testing covers the entire application and may include tests of both automated and manual processes.

[11] Acceptance testing determines if the software satisfies the acceptance criteria of the owners, users, and operators.

To improve the quality of its products and services, ASD has drafted a software inspection procedure and plans to test this process from September through November 2001. The goal of the software inspection procedure is to help identify and resolve potential issues and defects as close to their origin as possible. For major enhancements or program fixes, the software inspection process would consist of a combination of (1) technical reviews to evaluate design products such as requirements, functional specification, high level designs, and test plans and (2) inspections to assure that work products such as technical specifications, detail designs, code, and test cases conform to the design. If implemented effectively, a software inspection procedure could substantially improve the types of application change control weaknesses that we found.

## FINDING NO. 1

### FUNCTIONAL REQUIREMENTS FOR APPLICATION CHANGES WERE GENERALLY NOT APPROVED BY USERS

Changes to application software should generally be authorized by the managers responsible for the operations that the application supports (e.g., user management). As part of the application change process, ASD documents the functional requirements for each "routine" and "mandated" application maintenance project in a Software Requirements Document (SRD). NIST Special Publication 500-153, "Guide to Auditing for Controls and Security: A System Development Life Cycle Approach," states that the purpose of the requirements document is to provide a basis for mutual understanding of the software requirements between users and developers. However, neither ASD procedures nor the SRD template, which provides guidance and a consistent format for documenting the functional requirements contained in SRDs, include a requirement for obtaining user approval. Consequently, we found that NFC was not adequately obtaining user approval of the functional requirements developed by ASD, which is a critical control technique. It is important to obtain user approval to ensure that proposed changes meet the user needs. The functional requirements developed by ASD could also be improved if SRDs were expanded to include a summary of impacts to security, privacy, and internal control considerations as required by NIST Special Publication 500-153, "Guide to Auditing for Controls and Security: A System Development Life Cycle Approach." This control technique is not currently required by NFC. Without such an evaluation, NFC unnecessarily faces increased risks that software changes could create new security vulnerabilities or adversely impact other internal controls built into an application.

While we found some documentation (usually e-mails or letters from users) requesting the change for 13 of the 15 "routine" and "mandated" application maintenance projects that we reviewed, there was no evidence of user approval of the functional requirements relating to any of these projects. An NFC official advised us that ASD only requires user approval for application maintenance projects requiring more than 500 hours to complete. However, we found no evidence of user approval for any of the 5 projects that met this informal 500 hour requirement for user approval.[12] In addition, we do not believe that the need for user approval should be based solely on the hours needed to complete a project. For example, user approval of changes to software components that directly impact user communication with the system, such as input screens or reports, or other critical edits would generally be important regardless of the time estimates for completing the change.

Our tests also found that NFC does not require security, privacy, and/or internal control considerations to be specifically addressed in the functional requirements documents developed by ASD. This important control technique is required by NIST Special Publication 500-153. Consequently, we found that none of the functional requirements documents for 15 "routine" and "mandated" application maintenance projects that we reviewed discussed security, privacy, or internal control considerations of the proposed change. Such an evaluation is critical because changes to application systems could create new security vulnerabilities or render other internal controls ineffective if not adequately considered and addressed.

## RECOMMENDATION NO. 1

Modify OCFO procedures to require user approval of the functional requirements documents developed by ASD.

**OCFO Response**

The OCFO concurs with this recommendation. The NFC will develop criteria for when user approval of the requirements document is needed. The criteria will address the type of change being made, the magnitude of the change, the timeframe in which user approval should be obtained, and the method of documentation of the approval. The criteria will be developed by June 30, 2002, with implementation of the process on July 1, 2002.

**OIG Position**

We accept the management decision for this recommendation.

[12] The SRD template contains a section for documenting user approval, but does not contain guidance as to when this approval should be obtained.

## RECOMMENDATION NO. 2

Modify OCFO procedures to require NFC to specifically address the impact of the proposed change on existing security, privacy, and internal control considerations and whether the change mandates additional security, privacy, and/or internal control requirements in the functional requirements documents developed by ASD.

**OCFO Response**

OCFO concurs with this recommendation. NFC will modify the Software Requirements Document (SRD) template to include a section for security, privacy, and internal control considerations. The SRD will be modified by June 30, 2002. Beginning July 1, 2002, all SRDs will include statements addressing whether the change impacts security, privacy, and/or internal control requirements of the system.

**OIG Position**

We accept the management decision for this recommendation.

## FINDING NO. 2

### SOFTWARE TESTING WAS NOT ADEQUATELY DOCUMENTED

The President's Council on Integrity and Efficiency's (PCIE) Review of Application Software Maintenance in Federal Agencies, which was issued in September 1996, recognized that software testing is a critical component of software maintenance. The PCIE document also noted that insufficient testing and analysis of test results could result in programs that fail when introduced into the production environment. GAO's Federal Information System Controls Audit Manual states that the extent of software testing should generally vary depending on the type of modification. For major changes, testing should usually progress through a series of stages that include (1) testing individual program modules (unit testing), (2) testing groups of modules that must work together (integration testing), and (3) testing an entire system (system testing). Minor changes may require less extensive testing; however, even these changes should be carefully tested and approved since relatively minor program code changes, if done incorrectly, can have a significant impact on overall data reliability. Because testing is an iterative process that is generally performed at several levels, it is important that NFC adheres to a formal set of procedures or standards that include requirements for developing a detailed test plan for each change that defines the levels and types of tests to be performed, along with the responsibilities for the personnel involved in testing and approving software changes.

Our audit tests found that NFC was not adequately documenting the software testing performed by ASD, which includes unit, system, and integration testing. One reason we found for this lack of documentation and/or testing was that neither the NFC Application System Life Cycle directive nor the NFC Application Software Testing directive required test documentation to be maintained. In addition, we found that ASD was not following the Unit Test Plan format suggested in the NFC Application Software Testing directive, which provides a standard format for documenting test objectives, test procedures, including test cases, predicted results, evaluation criteria, actual results, and evidence of an independent review and approval. Without such test documentation, NFC will not be able to adequately assure that application software changes operate as intended and unauthorized changes are not introduced. This is critical since NFC maintains applications that disbursed and/or authorized over $40 billion in administrative and payroll payments in fiscal year 2001.

The NFC Application Software Testing directive requires full software testing (unit, integration, system, and acceptance) for development and/or maintenance projects that require over 500 staff hours. To test whether NFC was adhering to this directive, we requested test documentation for the five "routine" and "mandated" application maintenance projects included in our sample that exceeded the 500 hour limit. However, NFC officials were only able to provide test documentation for four of the five projects. Our review of these four found that none of the test documentation provided included complete test plans or evidence that test results were reviewed and approved. The documentation provided for three of the four projects was also not sufficient to determine if the testing performed was adequate to ensure that the modified programs were operating as intended.

- The test documentation provided for one of the projects included actual test results, but the documentation did not specify the test objectives, test procedures, test cases, predicted results, or evaluation criteria.
- In the second case, the test documentation provided did not describe the test procedures, test cases, predicted results, or evaluation criteria.
- In the third case, the test documentation provided included a document that specified test cases, actual results, and the person performing the testing, but did not describe the test objectives, test procedures, predicted results, or evaluation criteria.

For development and/or maintenance projects that require less than 500 staff hours, the NFC Application Software Testing directive requires unit testing and a determination by ASD as to whether integration and system testing should be performed. We requested documentation for the 10 "routine" and "mandated" application maintenance projects included in our sample that required less than 500 hours to complete. The documentation provided by ASD included test documentation for three of these 10 projects. Our analysis showed that none of the documentation provided (1) included complete test plans or evidence that test results were reviewed and approved or (2) was sufficient to determine if the testing performed was adequate to ensure that the modified programs were operating as intended. Furthermore, the documentation provided for the 10 "routine" and "mandated" application maintenance projects included in our sample that required less than 500 hours to complete did not include evidence indicating that a determination regarding the need to perform integration and/or system testing had been made. We noted that 8 of the 10 changes appeared to involve multiple programs and/or applications, which would generally warrant integration and/or system testing to be performed. For example, one of the projects in our sample was established to implement a non-USDA agency into NFC's payroll/personnel systems and required modifications to 30 applications. While unit testing is required, it only checks the logic of an individual program. The performance of integration and system testing would be critical for this application maintenance project to ensure that changes did not adversely affect related software components or the operation of the Payroll/Personnel System as a whole. This is critical since NFC maintains applications that disbursed and/or authorized over $43 billion in salary and administrative payments for both USDA and non-USDA agencies in FY 2001.

The NFC Application Software Testing directive provides a suggested Unit Test Plan format that requires documentation of test objectives, test procedures, test cases, predicted results/evaluation criteria, actual results, and evidence of an independent review and approval. However, we found that none of the test documentation provided by ASD included all of the elements suggested in the Application Software Testing directive.

Another reason for the lack of adequate documentation relating to ASD software testing is that NFC's Application System Life Cycle directive does not clearly define project file documentation requirements for application changes. In addition, none of the NFC directives relating to application change control (1) provided specific guidance for determining when integration and/or system testing should be performed or (2) established a consistent format to document integration and system test plans, tests performed, test results, and review and approval. Furthermore, the Application System Life Cycle directive does not reference the other directives relating to application development and change control, such as the Scheduled Software Maintenance and Application Software Testing directives.

While our testing was not designed to identify processing irregularities or other concerns due to the absence of appropriate application change controls, we did discover examples where incomplete or inadequately tested changes resulted in data being processed incorrectly or the need for subsequent changes to effect the original change. For example, 6 of the 11 “emergency” changes that we reviewed were required to fix problems resulting from previous application changes. (Our review of controls over “emergency” changes is discussed in Finding No. 4.) In addition, two “mandated” changes had to be implemented because the initial change did not completely accomplish the user requirements. Furthermore, two “special production processing” requests that we reviewed were processed to fix payroll/personnel data because a prior change did not include important data edits. (Our review of controls over “special production processing” is discussed in Finding No. 5.)

## RECOMMENDATION NO. 3

Establish controls to assure that a standard test plan format is followed for all application changes processed by NFC. This format should include documentation of test objectives, test procedures, test cases for both valid and invalid conditions, predicted results/evaluation criteria, actual results, and an independent review and approval of the test plan/results.

### OCFO Response

OCFO concurs with this recommendation. NFC will establish guidance for documenting test procedures, which will include documentation of test objectives, test procedures, test cases for both valid and invalid conditions, predicted results/evaluation criteria, actual results, and an independent review and approval of the test plan/results. These procedures will be used in conjunction with the recently implemented ASD initiative, entitled the Software Inspection Process, to cover all phases of software development. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

### OIG Position

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 4

Establish specific guidance to identify when integration and/or system testing should be performed and the documentation required to support whether such tests are necessary.

### OCFO Response

OCFO concurs with this recommendation. NFC will document the procedures governing integration and system testing and the related approval authorities needed for when these tests do not have to be conducted. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**OIG Position**

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 5

Update applicable NFC directives to reflect changes implemented as a result of this audit, provide consistent guidance, and reference other directives associated with application development and change control.

**OCFO Response**

OCFO concurs with this recommendation. ASD will provide copies of the guidance developed as a result of the other recommendations to the Information Systems Policy and Control Staff (ISPCS). We will work with ISPCS to revise the applicable directives. Completion of the revised directives is expected by December 31, 2002.

**OIG Position**

We accept the management decision for this recommendation.

## FINDING NO. 3

### ACCEPTANCE TESTING WAS NOT ALWAYS PERFORMED

In addition to ensuring that application changes are properly authorized and tested, it is also important to obtain final acceptance by user management and other appropriate officials after testing is successfully completed and reviewed. Obtaining such approvals helps to ensure that the program changes, along with required database, security, and operational changes, are ready for implementation and meet user requirements. At NFC, approvals from users, database administrators, security administrators, and other appropriate personnel outside of ASD are obtained as part of the acceptance testing process described in NFC's Scheduled Software Maintenance and Application Software Testing directives. ISQAO's "Guide to Acceptance Testing" specifies guidance for developing the acceptance test plan, monitoring testing, and documenting and approving test results.

Our audit tests found that NFC had performed acceptance testing for the "routine" changes in our sample as required, but was not consistently performing acceptance testing for "mandated" changes. The 15 application maintenance projects in our sample included four "routine" and 11 "mandated" maintenance projects. Our review showed that NFC had performed acceptance testing for the four "routine" maintenance projects that were in our sample. However, NFC was unable to provide acceptance test documentation for 10 of the 11 "mandated" projects that we reviewed.[13] One reason that acceptance testing was not always performed for "mandated" changes was that NFC's Scheduled Software Maintenance and Application Software Testing directives provide conflicting guidance regarding acceptance testing.[14] Until NFC begins obtaining final approvals from users, database administrators, security administrators, and other appropriate personnel, the center will face increased risks that application changes will not meet user requirements or operate as intended.

In addition, the NFC Scheduled Software Maintenance directive requires acceptance testing to include regression testing. Such testing is used to ensure that unintended or unauthorized changes are not made to critical programs. The NFC Scheduled Software Maintenance directive also requires development and maintenance organizations, such as ASD, to develop a standard test deck or database that includes test transactions for regression testing. However, an ASD manager advised us that, except for the Payroll/Personnel System, which had a test bed of about 500 transactions, ASD had not yet developed such test transactions for any of its other applications. Consequently, even though NFC procedures require regression testing, we did not find any evidence of regression testing when acceptance testing was performed. Our review of application changes relating to the 15 "routine" and "mandated" application maintenance projects in our sample identified one instance where an application change error could have been prevented if NFC had performed the required regression testing. In this case, an emergency change was needed because an unrelated change had caused incorrect processing of depreciation records when the Property system master file was modified. NFC officials advised us that it is in the process of testing a tool that would facilitate the creation of test transactions for regression testing.

We also identified conflicting guidance between two NFC directives dealing with acceptance testing for application changes. For example, the Application Software Testing directive allows the option of not performing

[13] Three of the 10 "mandated" projects for which acceptance testing was not performed were estimated to require more than 500 hours of development division time, which would require acceptance testing per NFC's Application Software Testing directive.

[14] Although the Scheduled Software Maintenance directive requires ISQAO to perform acceptance testing for both "routine" and "mandated" changes, the Application Software Testing directive only requires user acceptance testing for changes that require over 500 hours of development division time.

user acceptance testing if approved by the Director of ASD. However, the Scheduled Software Maintenance directive does not allow for this exception. Regardless, we did not find any documentation to show that a waiver of acceptance testing was granted for the 10 “mandated” projects for which acceptance testing was not performed. While it could be acceptable to allow acceptance testing to be waived, this should not be approved unless regression testing for the change has been performed and the users and other technical personnel involved in acceptance testing approve the waiver.

## RECOMMENDATION NO. 6

Update NFC directives to provide consistent guidance that (1) requires acceptance testing for both “routine” and “mandated” changes and (2) only allows acceptance testing to be waived if approved by the users and other appropriate technical personnel after a review of ASD software testing.

### OCFO Response

OCFO concurs with this recommendation. ASD will work with ISPCS to develop a revised directive covering acceptance testing requirements and waiver procedures. We will issue the revised directive by December 31, 2002.

### OIG Position

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 7

Establish controls to ensure that regression testing is performed for “routine” and “mandated” changes to ensure that unintended or unauthorized changes are not made to critical programs.

### OCFO Response

OCFO agrees in part with this recommendation. In lieu of regression testing, which requires the duplication of voluminous amounts of data, NFC is currently instituting new requirements for system testing, integration testing, and acceptance testing designed to reduce any risk of unintended or unauthorized changes made to critical programs. The estimated completion date for the new requirements is December 31, 2002. Additionally, regression testing will be considered at a later time if the cost justifies any significant additional risk reductions.

### OIG Position

While the alternative procedures proposed by OCFO may accomplish the intent of our recommendation, we cannot consider the management decision to this recommendation until we review the alternative testing requirements to ensure that they adequately reduce the risk of unintended or unauthorized changes to critical programs. OCFO needs to provide us these alternative-testing requirements at the time they are completed so we can evaluate them.

# CHAPTER 2 APPLICATION CHANGE CONTROLS OVER "EMERGENCY" CHANGES WERE NOT SUFFICIENT

## FINDING NO. 4

Although applications may require changes to be made on "emergency" basis to ensure key systems continue to operate, NFC's procedures unnecessarily increased the risk of errors or unauthorized modifications. The NFC Scheduled Software Maintenance directive allows full application software testing for emergency changes to be waived. In addition, this directive does not require emergency changes to be fully tested and approved by users until the next scheduled release[15] for an application, which can be more than 3 years between releases.[16] Our audit tests also disclosed that "emergency" changes were not kept to a minimum. We found that almost one-half (180 of 380) of ASD software maintenance projects for which changes were implemented between October 1, 2000, and April 3, 2001, were initiated to implement "emergency" changes. These projects accounted for about 20 percent of the programs changed during this period. NFC is responsible for maintaining the application programs for the payroll/personnel, administrative payments, accounts receivable, property management, and certain accounting systems. In fiscal year 2001, these systems disbursed or authorized more than $43 billion in salary and administrative payments for both USDA and non-USDA agencies.

To perform our audit tests, we selected a sample of 11 of the 180 "emergency"[1] application maintenance projects for which changes were implemented from October 1, 2000, through April 3, 2001.[1] These projects were selected based on a combination of judgmental sampling to ensure that changes related to SPPS were included and random sampling among changes to the other ASD applications.

The NFC Scheduled Software Maintenance directive states that "emergency" changes require immediate implementation to correct an error in the existing version of application software. However, 2 of 11 did not appear to require immediate implementation. For example, one of the "emergency" changes that we reviewed was made to implement a change in the accounting code structure for a USDA agency. This change was implemented to fix a problem caused by a prior application change that

[15] The NFC Scheduled Software Maintenance directive defines a scheduled release as a regularly planned update of an application in which "routine" changes are combined with the "emergency" and "mandated" changes implemented since the last scheduled release.

[16] For 10 of the 15 systems affected by the application maintenance projects included in our samples, the time between the last scheduled release and the next scheduled release was at least one year. Three of these systems had not had a scheduled release in more than three years.

was not made properly. We questioned whether this change was critical enough to require immediate implementation. NFC officials agreed with our conclusions for the two changes that we questioned.

In addition, the NFC Scheduled Software Maintenance directive does not require emergency changes to be fully tested and approved by users until the next scheduled release for an application, which can be more than three years in the future. Although NFC officials told us that “emergency” changes were tested before implementation, we were able to obtain documentation supporting such testing for only one of the 11 “emergency” changes that we reviewed. Similarly, only one of the 11 “emergency” changes that we reviewed appears to have been approved by user management prior to the next scheduled release.

## RECOMMENDATION NO. 8

Establish controls to ensure that “emergency” changes are limited to those application changes that require immediate implementation.

### OCFO Response

OCFO concurs with this recommendation. ASD has informed their branch chiefs that “emergency” changes are authorized only for situations when program bugs have been detected. Other changes that need to be made in a short timeframe based on client needs are to be considered “mandated” changes. The branch chiefs and the division director are required to sign Form 1133 to ensure that all “emergency” changes made meet the above requirements. The estimated completion date for these corrective actions was January 1, 2002.

### OIG Position

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 9

Establish specific guidance that clearly defines the types of testing to be performed prior to implementation for “emergency” changes and documentation requirements for such testing.

### OCFO Response

OCFO concurs with this recommendation. The procedures that are being developed in conjunction with Recommendations 3 and 4 will also include specific guidance on documenting test procedures for “emergency” changes. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**OIG Position**

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 10

Establish controls to ensure that “emergency” changes are subsequently approved by user management within 30 days.

**OCFO Response**

OCFO concurs with this recommendation. As part of the guidance developed for testing and documenting “emergency” changes, ASD will include guidance covering user approval for these types of changes. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**OIG Position**

We accept the management decision for this recommendation.

# CHAPTER 3 “SPECIAL PRODUCTION PROCESSING” ROUTINES INCREASE RISK OF UNAUTHORIZED CHANGES TO DATA

## FINDING NO. 5

In addition to allowing changes to production software through its application maintenance process, NFC permits “special production processing”, which bypasses normal production programs and/or procedures or otherwise makes changes to production data outside of the normal production methods.[17] Because “special production processing” bypasses the management controls built into the application maintenance process and individual applications, it increases the risk of unauthorized changes being made to the systems. We have reported other control weaknesses with “special production processing” in our audits of NFC internal controls for fiscal years 1996 and 1997.

To perform our audit tests, we selected a sample of 18 of the 1,052 “special production processing” actions processed by NFC from October 1, 2000, through May 15, 2001 for ASD applications. These “special production processing” actions were judgmentally selected from the ASD production jobs that had the highest number of “special production processing” actions during this timeframe. The “special production processing” actions that we reviewed were generally required because ASD applications could not accomplish the required actions. We also found that NFC was not adequately (1) ensuring that “special production processing” was not used to perform routine processes, (2) documenting the testing performed to ensure that “special production processing” accomplished its intended purpose, or (3) effectively identifying programming or systemic problems that need to be addressed to minimize “special production processing.” Details of our review follow.

- Two of the 18 “special production processing” actions in our sample were initiated as part of a routine process for updating certain data even though NFC directives state that “special production processing” will only take place when standard methods cannot satisfy the requirement. For example, “special production processing” is the standard method used to update an automated table used by two key NFC payroll/personnel applications because NFC had not established normal production programs and/or procedures to accomplish this task.

[17] “Special production processing” differs from production software changes that are made through the application maintenance process in that (1) it can be used to make changes to changes to data and procedures in addition to programs and (2) changes made to production programs are affected by modifying the program temporarily rather than permanently.

- While the NFC Special Production Processing directive requires application programmers to test "special production processing" to ensure that it produces the expected results, this directive does not specify any documentation requirements. Consequently, we found that testing to ensure that "special production processing" produced the intended results and only accomplished authorized purposes was not adequately documented. Fourteen of the 18 "special production processing" actions that we reviewed were initiated to execute non-production programs, temporarily modify production programs, or copy files to update production data because the ASD application could not fix the problem encountered or accomplish the action requested.[18] The remaining four actions were processed to execute production jobs that had already been subjected to NFC application change controls. Although ASD programmers told us that they had tested each of the 14 "special production processing" actions that changed production data, documentation supporting the testing that had been performed was only provided for five of these 14 actions. In addition, none of the documentation provided was sufficient to determine if the testing performed was adequate or reviewed and approved. Without adequate test documentation that includes the test objectives, test procedures, test cases for both valid and invalid conditions, predicted results/evaluation criteria, actual results, and an independent review and approval of the test results, NFC cannot assure that "special production processing" actions will perform as intended and not cause any unintended consequences.

- Procedures established by NFC to identify programming or systemic problems that need to be addressed to minimize future "special production processing" need improvement. Currently, NFC personnel review a monthly report that identifies the number of "special production processing" requests processed for each application to identify programming or systemic problems that need to be addressed to minimize the need for future "special production processing". While the number of "special production processing" actions that occurred in a month may be one indicator of systemic problems, we identified examples of systemic system problems that would not be identified by the current analytical procedures. For example, two of the "special production processing" actions that we reviewed were implemented more than two months apart to fix similar data problems. Both of these "special production processing" actions were initiated by Software Problem Reports (SPR). Consequently, we analyzed the SPR

[18] The 12 "special production processing" requests that executed non-production programs to modify production data were generally required because an ASD application could not fix the problem or accomplish the requested actions. The remaining two "special production processing" requests (1) modified a production program to allow a non-production data file to be used as input to a production program and (2) updated production data by copying a non-production file into the production environment.

database to determine how many of the eight "special production processing" actions in our sample that were initiated by SPRs  were caused by recurring problems and found that four of these eight were due to recurring problems.

NFC recognized that controls over "special production processing" needed improvement and updated management controls in this area through the issuance of a directive released on August 24, 2001.  The revised directive now requires user approval for "special production processing" requests, which should reduce the risk associated with this processing routine, but does not address issues discussed above. Consequently, we believe additional controls are necessary.  We determined that over 1,000 "special production processing" requests were implemented for ASD applications between October 1, 2000, and May 15, 2001.  Unless controls over "special production processing" are strengthened, the payroll/personnel, administrative payments, accounts receivable, property management, and accounting systems maintained by ASD will unnecessarily be placed at risk of unauthorized modifications to production data, which could lead to improper payments.

## RECOMMENDATION NO. 11

Identify routine actions, such as updating tables, that are currently performed through "special production processing" and develop production programs and/or processes to perform these actions.

### OCFO Response

OCFO concurs with this recommendation.  NFC will develop procedures that will cover documentation of all "emergency" and "special production processing" projects.  A determination will be made as to whether the SPR process is the best method of documenting and analyzing the projects or if a different process should be used.  These procedures will be developed by June 30, 2002.  NFC will also establish controls to ensure that the present requirements for entering data into the SPR database are followed to ensure that all information is completely entered.

### OIG Position

While OCFO concurs with this recommendation, it is not clear that the proposed corrective actions will establish a method for identifying routine actions that are currently performed through "special production processing" and developing production programs and/or processes to perform these routine actions. Consequently, we cannot consider the management decision for this recommendation without additional information addressing NFC's plans to reduce these requests in the future.

## RECOMMENDATION NO. 12

Modify NFC procedures to include specific requirements for testing "special production processing" actions and the documentation that should be developed and maintained. This documentation should include test objectives, test procedures, test cases for both valid and invalid conditions, predicted results/evaluation criteria, actual results, and an independent review and approval of the test results.

**OCFO Response**

OCFO concurs with this recommendation. As part of the process of developing procedures for testing other types of changes, NFC will include guidance for testing "special production processing" changes as well. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**OIG Position**

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 13

Expand the current procedures used to identify programming or systemic problems that need to be addressed to minimize the need for future "special production processing" to include additional types of analytical review, such as evaluating the reason for performing "special production processing" to identify recurring problems that are fixed through "special production processing."

**OCFO Response**

OCFO concurs with this recommendation. NFC will develop procedures that will cover documentation of all "emergency" and "special production processing" projects. A determination will be made as to whether the SPR process is the best method of documenting and analyzing the projects or if a different process should be used. These procedures will be developed by June 30, 2002. NFC will also establish controls to ensure that the present requirements for entering data into the SPR database are followed to ensure that all information is completely entered.

**OIG Position**

While OCFO concurs with this recommendation, the proposed corrective actions do not address the types of analysis that will be used to identify programming or systemic problems that need to be addressed to minimize the need for future “special production processing.”  Consequently, we cannot consider the management decision without additional information showing NFC’s plans to identify programming or system problems for correction.

# CHAPTER 4 AUDIT TRAIL FOR CHANGES TO PRODUCTION SOFTWARE AND DATA NEEDS IMPROVEMENT

Another key element of controlling changes to NFC production software and data is developing and implementing a formal set of procedures or standards for documenting, ranking and scheduling changes to provide an adequate audit trail. However, we determined that ASD was not always tracking the initial request or documenting the change or processing that accomplished the initial requests for "emergency" software changes and "special production processing" requests. In addition, CATS the system that documents the final approval from ASD to implement a change to an existing program did not track the reason for or authorization of certain types of changes that could impact the operation of ASD applications. As a result, NFC cannot assure that "emergency" software change and "special production processing" requests can be easily tracked from initiation to the final approval or from the change back to the initial user authorization.

## FINDING NO. 6

### ASD WAS NOT ADEQUATELY DOCUMENTING THE INITIAL REQUEST FOR CERTAIN CHANGES

The NFC forms used to request production software changes (NFC-1133) and "special production processing" (NFC-644) both document ASD authorization of the change. In addition, the Special Production Processing Request form was modified in August 2001 to include a final user approval for the change. However, neither standard form includes or requires a reference to the initial user authorization. In March 1999, ASD implemented its SPR policy and an associated procedure, in part, to ensure that software maintenance requirements are documented and traceable from source to software. However, the current procedures do not ensure that "emergency" software change and "special production processing" requests can be tracked from authorization to the final approval or from the change back to the initial user request.

The current SPR policy allows software maintenance and customer assistance to be initiated through either SPRs or "other vehicles approved by ASD management". Consequently, we determined that ASD allows software maintenance and customer assistance requests to be initiated through several methods, including SPRs, letters, e-mails, and occasionally a phone call or visit. However, "emergency" change projects and "special production processing" requests initiated through methods other than an SPR are generally not tracked by other ASD systems. Only two of the 11 "emergency" software maintenance projects that we reviewed and less than one-half of the 18 “special production processing” requests that we reviewed were documented by an SPR.

To fully assure that NFC can trace “emergency” software change and “special production processing” requests from initiation to the final approval and from the change back to the initial user authorization, the SPR database should also be expanded to capture the type of output resulting from the SPR, along with the associated project number or “special production processing” request used to accomplish the output. While the SPR database contains fields for documenting the description of the problem, along with the cause and source of the problem, it does not include fields to (1) document the outcome or, (2) in the case of software modifications and data corrections, reference the project number or “special production processing” used to accomplish the outcome. Such information would allow NFC to trace both software changes and “special production processing” from initiation to final approval. Requiring “special production processing” and productions software change requests to reference the SPR that initiated the request would also permit NFC to easily trace code and other changes back to the initial requests.

In addition, the SPR requests were not always completely documented in ASD’s SPR database. While the SPR database appeared to adequately capture the information provided by the originator of the SPR, it did not always include information completed by ASD. For example, our analysis of the 871 SPRs initiated and completed in fiscal year 2001 as of August 15, 2001, showed that the priority assigned by the originator was captured for about 95 percent (833 of 871) of the SPRs, while the priority assigned by ASD was captured for less than 1 percent (5 of 871). In addition, the SPR database did not contain the source of the problem for more than half (486) of the 871 SPRs. Until all information about all software maintenance requests is entered into the SPR database, NFC will not be able to fully realize the other goals specified in the SPR policy, such as responding better to customers and providing a mechanism for evaluating, approving, and prioritizing maintenance workloads to more efficiently accomplish OCFO, NFC, and ASD goals and objectives.

## RECOMMENDATION NO. 14

Require all “emergency” application maintenance projects and “special production processing” requests to be documented by SPRs.

### OCFO Response

OCFO concurs with this recommendation. NFC will develop procedures that will cover documentation of all “emergency” and “special production processing” projects. A determination will be made as to whether the

Software Problem Report (SPR) process is the best method of documenting the projects or if a different process should be used. These procedures will be developed by June 30, 2002.

**OIG Position**

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 15

Expand SPRs to document the outcome and, where applicable, the resulting "special production processing" request or program change. Establish controls to ensure that SPR information is completely entered into the SPR database.

**OCFO Response**

OCFO concurs with this recommendation. NFC will develop procedures that will cover documentation of all "emergency" and "special production processing" projects. A determination will be made as to whether the SPR process is the best method of documenting the projects or if a different process should be used. These procedures will be developed by June 30, 2002. NFC will also establish controls to ensure that the present requirements for entering data into the SPR database are followed to ensure that all information is completely entered by June 30, 2002.

**OIG Position**

While OCFO concurs with this recommendation, the proposed corrective actions do not address expanding SPRs, or the information gathered through an alternative method, to document the outcome and, where applicable, the resulting "special production processing" request or program change. Consequently, we cannot consider the management decision for this recommendation without this additional information.

## RECOMMENDATION NO. 16

Begin referencing the SPR that initiated the change on Production Software Change and "special production processing" forms to ensure that changes can be traced back to the initial user authorization.

**OCFO Response**

OCFO concurs with this recommendation. NFC will begin referencing the applicable SPR or user request documentation on the Production Software Change and "special production processing" forms, as applicable. This procedure will become effective on April 1, 2002.

**OIG Position**

We accept the management decision for this recommendation.

## FINDING NO. 7

### CATS WAS NOT TRACKING ASD APPROVAL FOR CERTAIN TYPES OF CHANGES

NFC implemented CATS to facilitate the change control process. CATS system documentation states that it provides the ability to track changes to production software, but does not provide guidance regarding which types of changes should be tracked in CATS. According to an ISQAO manager, NFC uses CATS to track the final approval from ASD to implement a change to an existing program and the reason that the program was changed. However, CATS is not used to track the reason for or authorization of other changes, including changes to procedures (procs), specifications (specs), and copy members,[19] that could impact the operation of ASD applications. While changes to procs, specs, and copy members may not be as risky as changes to programs, if not properly controlled, such changes could still produce unintended results. For example, a change to a "proc" could be used to call the wrong production program, direct the operating system to open a file that does not exist, or not provide adequate operating system resources for the program to execute properly.

In addition, the General Purpose Library Maintenance Form, which is currently used to authorize changes to procs, specs, and copy members, does not require ASD to document the reason for the change or link the change to the maintenance project number prompting the change. While changes to procedures and/or specifications may not always be prompted by an ASD maintenance project, changes to copy members that are called by multiple programs should be formally coordinated within ASD to ensure that all affected applications are appropriately updated.[20] One "emergency" change in our sample was required to recompile programs to implement updates to agency and department codes in a table that was stored as a copy member. Without this change, the affected programs would have ended abnormally due to incorrect department codes.

## RECOMMENDATION NO. 17

Modify NFC procedures to begin tracking controls over changes to procs, specs, and copy members in CATS.

[19] Procedures (procs) are files that contain the execution Job Control Language (JCL) associated with a particular program, specifications (specs) are files that contain data to be included in the execution JCL, and copy members contain common code that is shared by more than one program.

[20] When a copy member is updated, each program that calls the copy member needs to be recompiled for the changes to take effect.

**OCFO Response**

OCFO concurs with this recommendation. Currently, an audit trail exists for these types of changes but no subsequent documentation on the reason for the change is required. NFC is developing a process to begin tracking controls over changes to procs, specs, and copy members in CATS. The new process will be implemented by April 1, 2002.

**OIG Position**

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 18

Update the General Purpose Library Maintenance Form to include the ASD maintenance project number or other reason for the change to a procedure, specification, or copy member.

**OCFO Response**

OCFO concurs with this recommendation. NFC is updating the General Purpose Library Maintenance Form to include the ASD maintenance project number or other reason for the change to a procedure, specification, or copy member. The estimated completion date for this corrective action is April 1, 2002.

**OIG Position**

We accept the management decision for this recommendation.

# CHAPTER 5 OTHER IT GENERAL CONTROLS WERE NOT EFFECTIVE

In addition to weaknesses in application change controls, we also identified weaknesses in other IT general controls that were applied specifically to SPPS. Access to SPPS and other information in NFC's payroll/personnel databases was not adequately restricted. As a result, NFC faces increased risk that certain payroll transactions may be improper or inaccurate. In addition, sensitive personnel information is vulnerable to inadvertent or deliberate unlawful disclosure.

OMB Circular A-130 establishes a minimum set of requirements to be included in Federal information security management programs, which are essential to ensure that appropriate computer controls are established and maintained. While reviewing security management controls that applied specifically to SPPS, we identified computer security management weaknesses that could impact the effectiveness of controls over not only SPPS, but other NFC applications as well. Specifically, NFC had not developed a security plan for the Payroll/Personnel System, which would encompass SPPS, or the other four major applications for which the center was responsible. We also found weaknesses in NFC's certification process.

## FINDING NO. 8

### ACCESS TO SPPS WAS NOT APPROPRIATELY LIMITED

NFC had not adequately restricted access to the payroll transactions and sensitive personnel information available through SPPS or a powerful database utility that could be used to circumvent the security controls built into the application to improperly read and modify both SPPS data and other payroll/personnel information. This was caused mainly because (1) SPPS had been designated as an "update only" system and "read only" access is not available for the indebtedness and death case functions of SPPS, (2) NFC's periodic reviews of access to SPPS had not identified employees that no longer needed access to SPPS due to changes in job responsibilities, and (3) NFC was not reviewing access to the Data Manipulation Language Online (DMLO) utility.

We reviewed access authorities and identified staff members that did not appear to require access to SPPS based on their job responsibilities. NFC verified that 78 of the 254 NFC employees that were granted update access to the quick service request, indebtedness, and death case functions of SPPS did not need this level of access to perform their job functions.

- Sixty-seven of the 78 NFC employees with update access to SPPS, including 44 Billings and Collections Branch and eight Human Resources Management Office employees, only needed the ability to read records in SPPS for research but were also permitted to update these records, which increases the risk of inadvertent errors and/or deliberate misuse, because “read only” access was not available.

- Although NFC performs periodic reviews of access to SPPS, as required by Title VII, Chapter 11, Directive 40, “Internal Controls for Access to Data and Software,” the remaining 11 NFC employees had access to perform updates to SPPS quick service requests, indebtedness, and death case transactions even though their access to SPPS was no longer needed due to changes in job responsibilities.

Our audit tests also disclosed that access controls over SPPS were not adequately enforcing segregation of duties principles.  Of the 254 NFC employees provided update access to SPPS, 18 were application programmers and seven were database management branch (DBMB) staff members.  This violates the basic segregation of duties principle that only users should process transactions and initiate changes to application data.  According to ASD and DBMB management, 16 of the 18 application programmers and three of the seven DBMB staff members did not require update access to SPPS.  The remaining two application programmers and four database management branch staff members need read access for research purposes and occasionally require update access to SPPS to solve problems.  While we agree that read access may be warranted, other techniques, such as emergency access identification, could be used to provide temporary update access authority in the special situations where additional access is required.  According to NFC officials, the center already has a process in place for granting temporary access to applications.

Finally, NFC had not adequately restricted access to DMLO.  NFC Title VII, Chapter 11, Directive 69, “Management of Online Database Utilities,” states that online database utilities, such as DMLO, will be restricted to “emergency” situations because these tools can subvert the normal controls applied to the update of production data.  We identified four ASD application programmers with permanent DMLO access to NFC’s payroll/personnel databases.  One of the programmers with DMLO access and the branch chief over the other three programmers with this access told us that they were not aware that they had DMLO access and that it was not necessary for their jobs.  One reason that unnecessary DMLO access to NFC’s payroll/personnel databases existed was because access to DMLO was not being reviewed to ensure that it remained appropriate. It appears that three of the four programmers with DMLO access to the payroll/personnel databases were inadvertently provided this access. The remaining programmer told us that he had requested access to DMLO to correct a specific problem more than a year ago and no longer needed this access. Consequently, effective periodic reviews of DMLO access would have allowed NFC to identify and correct this inappropriate access.

## RECOMMENDATION NO. 19

Establish a method to allow "read only" access to all SPPS functions and re-evaluate access to SPPS to ensure that staff members are assigned the minimum level of access required to perform their job functions.

### OCFO Response

OCFO concurs with this recommendation. The Special Payroll Processing System was developed with a "read only" capability. However, it was never implemented. NFC is in the process of testing the changes needed to implement the "read only" access and once implemented will ensure that access is granted to staff based on the minimum level of access needed for their job. We expect to implement the "read only" capability by October 1, 2002.

### OIG Position

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 20

Establish controls to ensure that application programmers and DBMB staff members are only provided read access to the applications that they maintain. Use NFC's process for granting temporary access to provide update access to application programmers and DBMB staff members on the occasions when this level of access is needed to solve problems.

### OCFO Response

OCFO concurs with this recommendation. NFC will use its current process for granting temporary access to provide update access once the corrective action described in Recommendation 19 has been completed.

### OIG Position

We accept the management decision for this recommendation.

## RECOMMENDATION NO. 21

Begin performing periodic reviews of access to DMLO to ensure that such access remains appropriate.

**OCFO Response**

OCFO concurs with this recommendation. ASD has asked ISPCS to revoke access to the Data Manipulation Language Online for all ASD programmers who presently have such access. In the future, programmers will receive only emergency access when needed.

**OIG Position**

While OCFO concurs with this recommendation, the proposed corrective actions do not address performing periodic reviews of access to DMLO to ensure that such access remains appropriate. Consequently, we cannot consider the management decision for this recommendation without this additional information and/or action.

## FINDING NO. 9

### SECURITY PLANS WERE NOT DEVELOPED FOR NFC'S MAJOR APPLICATIONS

OMB Circular A-130, which establishes a minimum set of controls to be included in Federal automated information security programs, requires agencies to prepare security plans for both general support systems and major applications. More specifically, NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," states that a system will be covered by an individual security plan if it has been designated as a major application. NFC had not developed individual security plans for the five major applications that it owns[21] because it interpreted USDA guidance as requiring the center to only prepare an overall plan and a plan for each of its general support systems. Without security plans for major applications, NFC faces increased risk that its systems are not secured in a manner that adequately prevents inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction of the financial transaction data and personnel information maintained by the payroll/personnel, billings and collections, administrative payments, accounting, and direct premium remittance systems that ASD maintains. In fiscal year 2001, these systems disbursed or authorized more than $43 billion in salary and administrative payments for both USDA and non-USDA agencies.

[21] The June 2001 NFC Security Plan identifies five major applications that are owned by NFC: Payroll/Personnel, Billings and Collections, Administrative Payments, Accounting Applications (other than FFIS), and the Direct Premium Remittance System.

OMB Circular A-130 also requires an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security. In this regard, the NIST guide for developing security plans states that risk assessments should be performed. In addition, GAO's May 1998 study of security management best practices pointed out that assessing risk is an important element of computer security planning because it provides the foundation for the other aspects of computer security management—implementing policies and controls to mitigate risks, promoting awareness of risks and responsibilities, and monitoring and evaluating the effectiveness of the computer security program. An effective risk assessment framework generally includes procedures that link security to business needs and provide for managing risk on a continual basis. GAO studied risk assessment practices at leading organizations[22] and identified the following success factors that were essential for effective risk assessment programs:

- Designating focal points to oversee and guide the risk assessment process and help ensure that organizationwide issues were appropriately addressed;
- defining procedures for conducting risk assessments and developing tools to facilitate and standardize the process;
- involving a mix of individuals with knowledge of business operations and technical aspects of the organization's systems and security controls;
- holding business units responsible for initiating and conducting risk assessments, as well as implementing risk reduction techniques;
- limiting the scope of individual risk assessments to particular business systems, facilities, or sets of operations while including provisions for considering risks shared throughout the organization; and
- documenting and maintaining risk assessment results so that managers could be held accountable for the decisions made.

We determined that NFC performs risk assessments and develops annual security plans for its general support systems. The June 2001 NFC Security Plan identifies eight major applications. However, we noted that NFC had not developed individual system security plans for the five major applications that NFC owns, including the Payroll/Personnel System, because NFC had interpreted the security plan guidance issued by USDA's Associate Chief Information Office for the Office of Cyber Security as only requiring NFC to prepare an overall plan and a plan for each of its general support systems. In addition, NFC had not performed security risk assessments, which are important to ensure that adequate, cost-effective security measures are included in security plans, for the five major applications owned by NFC. The last NFC information security risk

[22] Information Security Risk Assessment: Practices of Leading Organizations (GAO/AIMD-00-33, November 1999).

assessment covered risks relating to NFC general support systems, but did not address risks specific to the five major applications that are owned by NFC. An NFC official advised us that NFC plans to hire a contractor to perform another risk assessment during calendar year 2001, but had not yet set any specific guidelines or timeframes for this assessment.

Although general support system risk assessments and resulting security plans should include overall controls that provide some level of security over all the major applications that are maintained on the general support system and help to ensure that controls specific to individual applications cannot be rendered ineffective by circumvention or modification, important controls that apply specifically to the major application may be overlooked without security plans for major applications. For example, a general support system security plan would generally not include important segregation of duties controls that relate directly to the Payroll/Personnel system, such as not allowing the same person to perform (1) personnel actions that would establish an employee on the payroll database and (2) time and attendance, special payroll processing, or other transactions that could be used to generate payments to employees on the payroll database. Preparing security plans that are based on risk assessments for major applications would not only help ensure that these systems are properly secured, but would also facilitate ISPCS in ensuring that important security safeguards are evaluated during the application certification process described below.

In January 2001, we reported that USDA was unnecessarily vulnerable to fraudulent and erroneous payments due to the numerous material internal control weaknesses relating to NFC's miscellaneous payment (MISCPAY) system, which disburses or authorizes payments, etc. (e.g., letters of credit), in excess of more than $4.5 billion.[23] In fact, we identified potential fraudulent payments that could result in substantial losses to the government. This problem was attributed primarily to the absence of a structured risk assessment of the MISPAY system.

## RECOMMENDATION NO. 22

Immediately begin preparing system security plans for NFC's major applications, as required by OMB Circular A-130 and described in NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."

[23] Audit Report No. 50099-19-FM, "Review of Controls Over USDA Administrative Payment Systems," dated January 2001.

**OCFO Response**

OCFO concurs with this recommendation. NFC plans to contract out the development of a Security Plan for each major application owned by NFC: Payroll/Personnel, Billings and Collections, Administrative Payments, Accounting Applications (other than FFIS), and the Direct Premium Remittance System. The estimated completion date is December 1, 2003.

**OIG Position**

While we concur with the proposed corrective actions, OCFO does not plan to complete these actions within 1 year. Consequently, we cannot consider the management decision for this recommendation without a corrective action plan that identifies interim milestones and/or completion dates for each specific application security plan.

## RECOMMENDATION NO. 23

Establish a risk assessment framework for assessing risks associated with both general support systems and major applications that links security to business needs and provides for managing risk on a continual basis.

**OCFO Response**

OCFO concurs with this recommendation. NFC is dedicating specific resources to assess risks in a corporate approach. The proposed Risk Management Program, which will organizationally be under the Systems Review Office, will coordinate fragmented issues that weaken current risk management efforts, address risk assessment education, conduct and/or coordinate third party assessments, and coordinate NFC Management Control Manuals.

**OIG Position**

While OCFO concurs with this recommendation, the proposed corrective actions do not clearly specify how the risk assessment framework will address risks associated with both general support systems and major applications, link security to business needs, or provide for managing risk on a continual basis. Consequently, we cannot consider the management decision for this recommendation without this additional information.

## FINDING NO. 10

### CERTIFICATION PROCESS COULD BE IMPROVED

To ensure that agencies maintain adequate security over major applications, OMB Circular A-130 also states that such applications should be authorized by the management official responsible for the function supported by the application at least every three years. To fulfill this requirement, NFC issued Title VII, Chapter 11, Management Directive No. 36, “Certification of Sensitive ADP Applications”, which requires ISPCS to evaluate and certify the security safeguards of application software before it is used in an operational environment and, subsequently, after significant modification or at least every 3 years. To facilitate this process, ISQAO’s Standards and Certification Group developed procedures for performing certifications of mainframe production applications that were issued in May 1998. The Certification directive also states that the director of NFC will make the accreditation decision based on the certification report and the opinions of the Director’s staff.

During our review of the SPPS certification, we identified issues that could impact the effectiveness of NFC’s certification and accreditation process. For example, the ISQAO procedures for performing certifications do not include provisions for reviewing compliance with the application change controls as defined in the Scheduled Software Maintenance directive. Federal Information Processing Standards Publication 102 states that (1) all changes, however minor, should require a formal change request, authorization, testing and approval, (2) a record along with pertinent certification evidence, such as test results, must be kept, and (3) this record should be reviewed during recertification. ISQAO management told us that since the 1998 SPPS certification, the office had started reviewing compliance with the Scheduled Software Maintenance directive.

However, ISQAO procedures for performing certifications and the draft Certification Final Disposition matrix, which is used to determine if full, conditional, or no certification is warranted, had not yet been updated to reflect this review.

In addition, the draft matrix did not clearly document consideration of the application and access control reviews. Such controls are important in determining if full, conditional, or no certification is warranted. If access controls are not adequately restricted, NFC may not be adequately protected from unauthorized changes to application data and programs. In addition, application controls are important to ensure that application data is valid, properly authorized, and completely and accurately processed and reported. An ISQAO manager told us that results of the application and access control reviews performed as part of the certification are considered when determining if full, conditional, or no certification is warranted as part of the “Processing controls are adequate” section of the matrix. However, there was no documentation describing which reviews are included in this category.

Finally, an ISQAO manager told us that the NFC Director had designated the chief of ISPCS as the accreditation official. Consequently, the chief of ISPCS is both the certifying and accrediting official and the certification statement also serves as the authorization for processing. This appears to be contrary to OMB Circular A-130 guidance, which states that the management official responsible for the function supported by the application should authorize the application for processing. The intent of this requirement is to assure that the senior official whose mission will be adversely affected by security weaknesses in the application periodically assesses and accepts the risk of operating the application. According to an ISQAO manager, the application owner receives a copy of the draft certification report for comment. While it may not be as critical for the owner to separately reauthorize a system receiving a full certification (e.g., the certification review did not identify significant weaknesses), it is important for the application owner to formally authorize applications receiving a conditional certification for processing to acknowledge that that the owner is aware of the certification findings and accepts the risk of operating the application given these findings.

In October 2001, ISQAO issued updated procedures for performing application certifications that, among other things, includes a review of compliance with the Scheduled Software Maintenance and Application Software Testing directives and updates the certification matrix to clearly document consideration of the application and access control reviews when determining if full, conditional, or no certification is warranted. In addition, an ISQAO manager told us that her office plans to begin requiring the directors of both the division responsible for the function supported by the application and the application development organization to reauthorize applications that receive a conditional certification.

## RECOMMENDATION NO. 24

Require either the director or the management official responsible for the function supported by the application to reauthorize applications that receive a conditional certification.

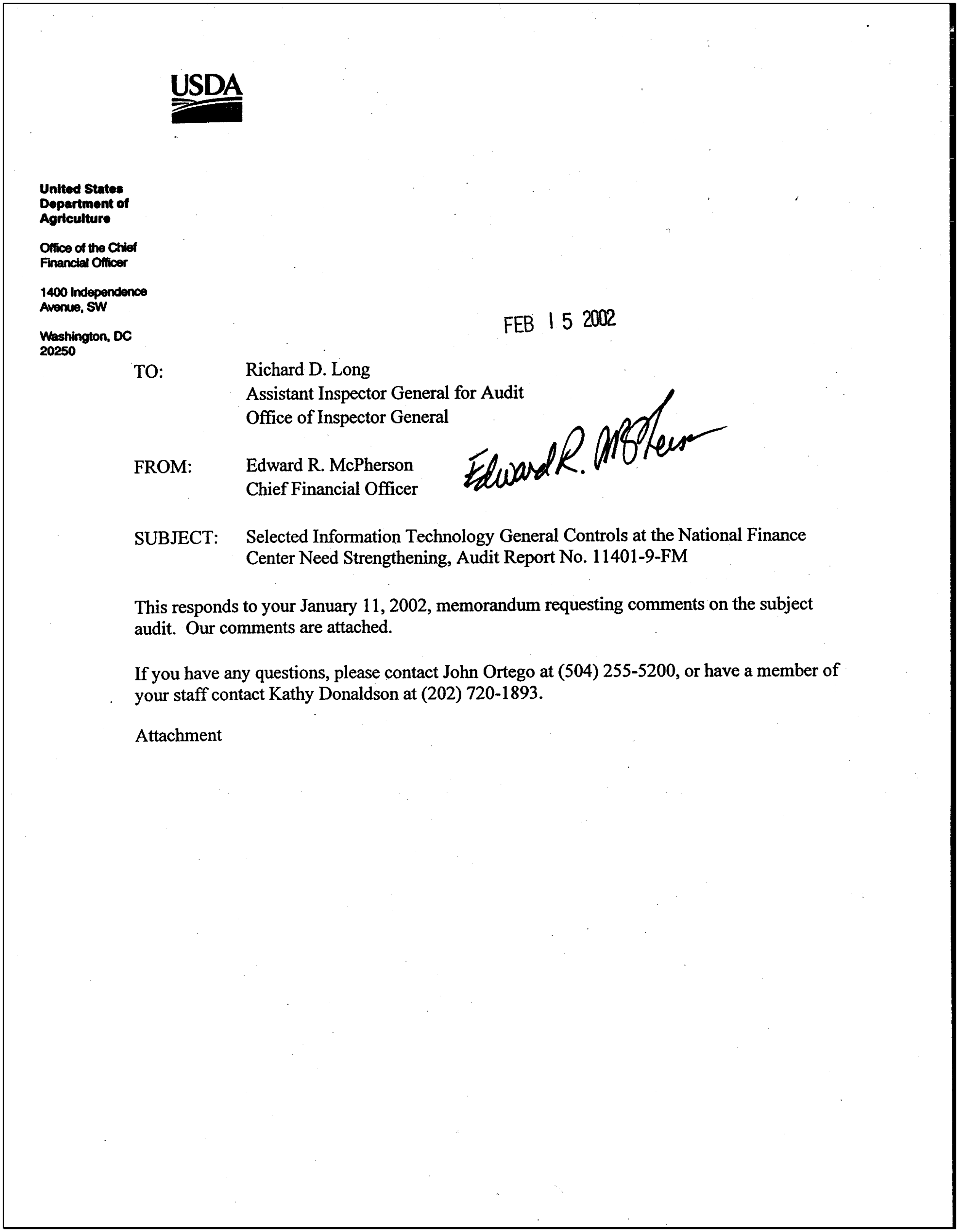
### OCFO Response

OCFO concurs with this recommendation. The Certification Process has been modified to include the signature of the responsible management official for all conditional certifications. The implementation of this process began with the fiscal year 2002 certifications.

**OIG Position**

We accept the management decision for this recommendation.

# EXHIBIT A –CFO'S RESPONSE TO THE DRAFT REPORT



USDA

United States
Department of
Agriculture

Office of the Chief
Financial Officer

1400 Independence
Avenue, SW

Washington, DC
20250

FEB 15 2002

TO: Richard D. Long
Assistant Inspector General for Audit
Office of Inspector General

FROM: Edward R. McPherson
Chief Financial Officer

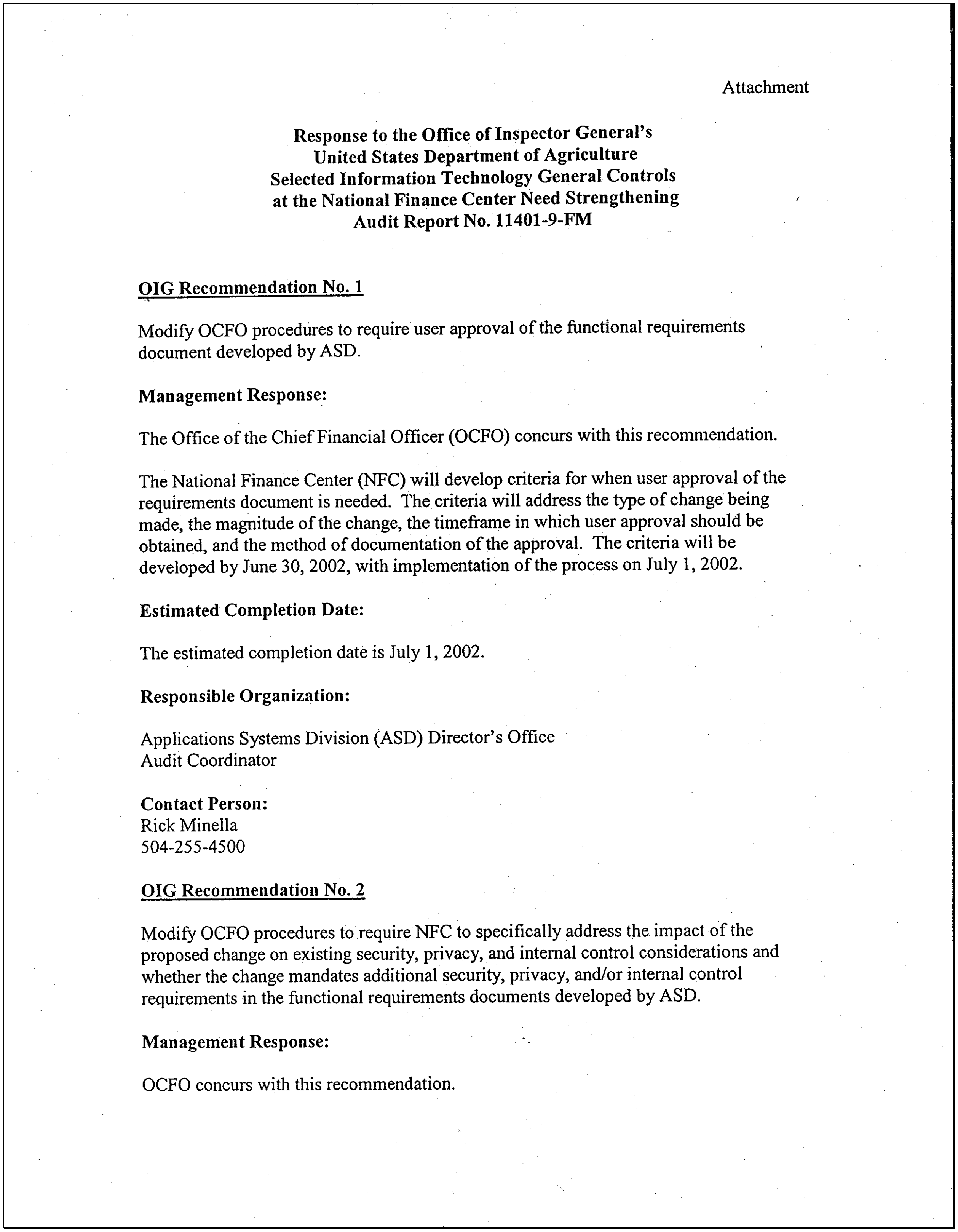
Edward R. McPherson

SUBJECT: Selected Information Technology General Controls at the National Finance Center Need Strengthening, Audit Report No. 11401-9-FM

This responds to your January 11, 2002, memorandum requesting comments on the subject audit. Our comments are attached.

If you have any questions, please contact John Ortego at (504) 255-5200, or have a member of your staff contact Kathy Donaldson at (202) 720-1893.

Attachment



Attachment

**Response to the Office of Inspector General's**
**United States Department of Agriculture**
**Selected Information Technology General Controls**
**at the National Finance Center Need Strengthening**
**Audit Report No. 11401-9-FM**

**<u>OIG Recommendation No. 1</u>**

Modify OCFO procedures to require user approval of the functional requirements document developed by ASD.

**Management Response:**

The Office of the Chief Financial Officer (OCFO) concurs with this recommendation.

The National Finance Center (NFC) will develop criteria for when user approval of the requirements document is needed. The criteria will address the type of change being made, the magnitude of the change, the timeframe in which user approval should be obtained, and the method of documentation of the approval. The criteria will be developed by June 30, 2002, with implementation of the process on July 1, 2002.

**Estimated Completion Date:**

The estimated completion date is July 1, 2002.

**Responsible Organization:**

Applications Systems Division (ASD) Director's Office
Audit Coordinator

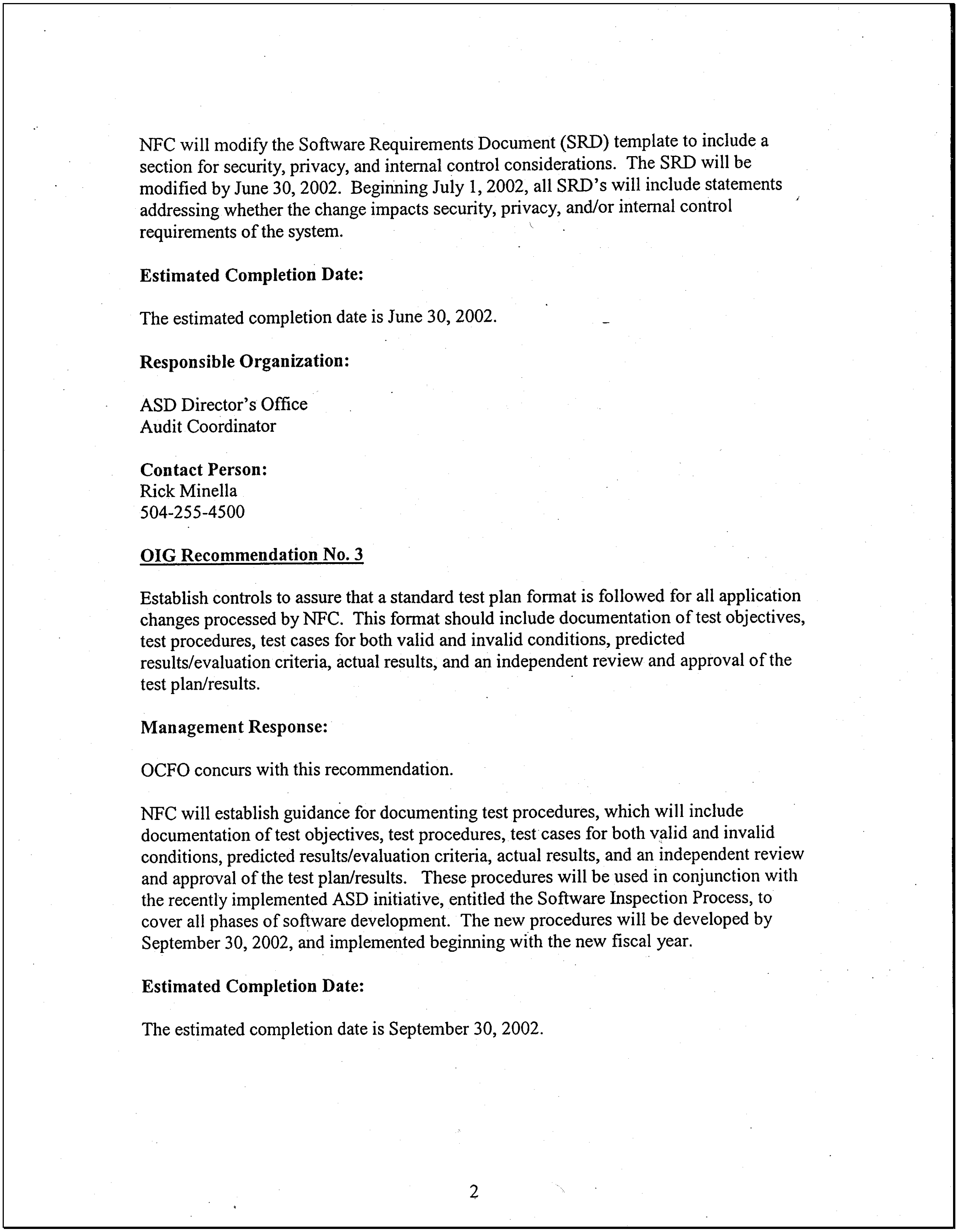
**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 2</u>**

Modify OCFO procedures to require NFC to specifically address the impact of the proposed change on existing security, privacy, and internal control considerations and whether the change mandates additional security, privacy, and/or internal control requirements in the functional requirements documents developed by ASD.

**Management Response:**

OCFO concurs with this recommendation.



NFC will modify the Software Requirements Document (SRD) template to include a section for security, privacy, and internal control considerations. The SRD will be modified by June 30, 2002. Beginning July 1, 2002, all SRD's will include statements addressing whether the change impacts security, privacy, and/or internal control requirements of the system.

**Estimated Completion Date:**

The estimated completion date is June 30, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**OIG Recommendation No. 3**

Establish controls to assure that a standard test plan format is followed for all application changes processed by NFC. This format should include documentation of test objectives, test procedures, test cases for both valid and invalid conditions, predicted results/evaluation criteria, actual results, and an independent review and approval of the test plan/results.

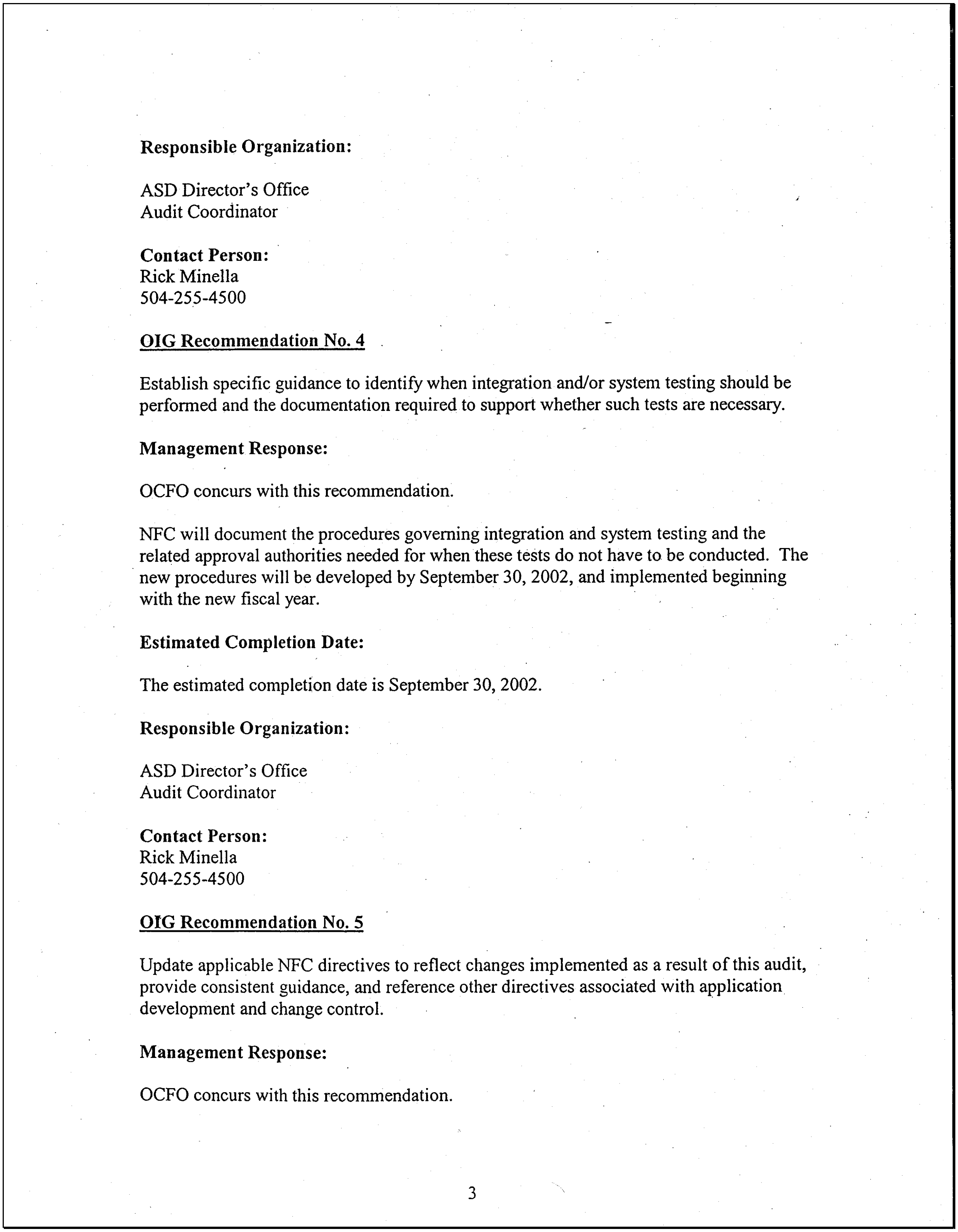
**Management Response:**

OCFO concurs with this recommendation.

NFC will establish guidance for documenting test procedures, which will include documentation of test objectives, test procedures, test cases for both valid and invalid conditions, predicted results/evaluation criteria, actual results, and an independent review and approval of the test plan/results. These procedures will be used in conjunction with the recently implemented ASD initiative, entitled the Software Inspection Process, to cover all phases of software development. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**Estimated Completion Date:**

The estimated completion date is September 30, 2002.



**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

<u>**OIG Recommendation No. 4**</u>

Establish specific guidance to identify when integration and/or system testing should be performed and the documentation required to support whether such tests are necessary.

**Management Response:**

OCFO concurs with this recommendation.

NFC will document the procedures governing integration and system testing and the related approval authorities needed for when these tests do not have to be conducted. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**Estimated Completion Date:**

The estimated completion date is September 30, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

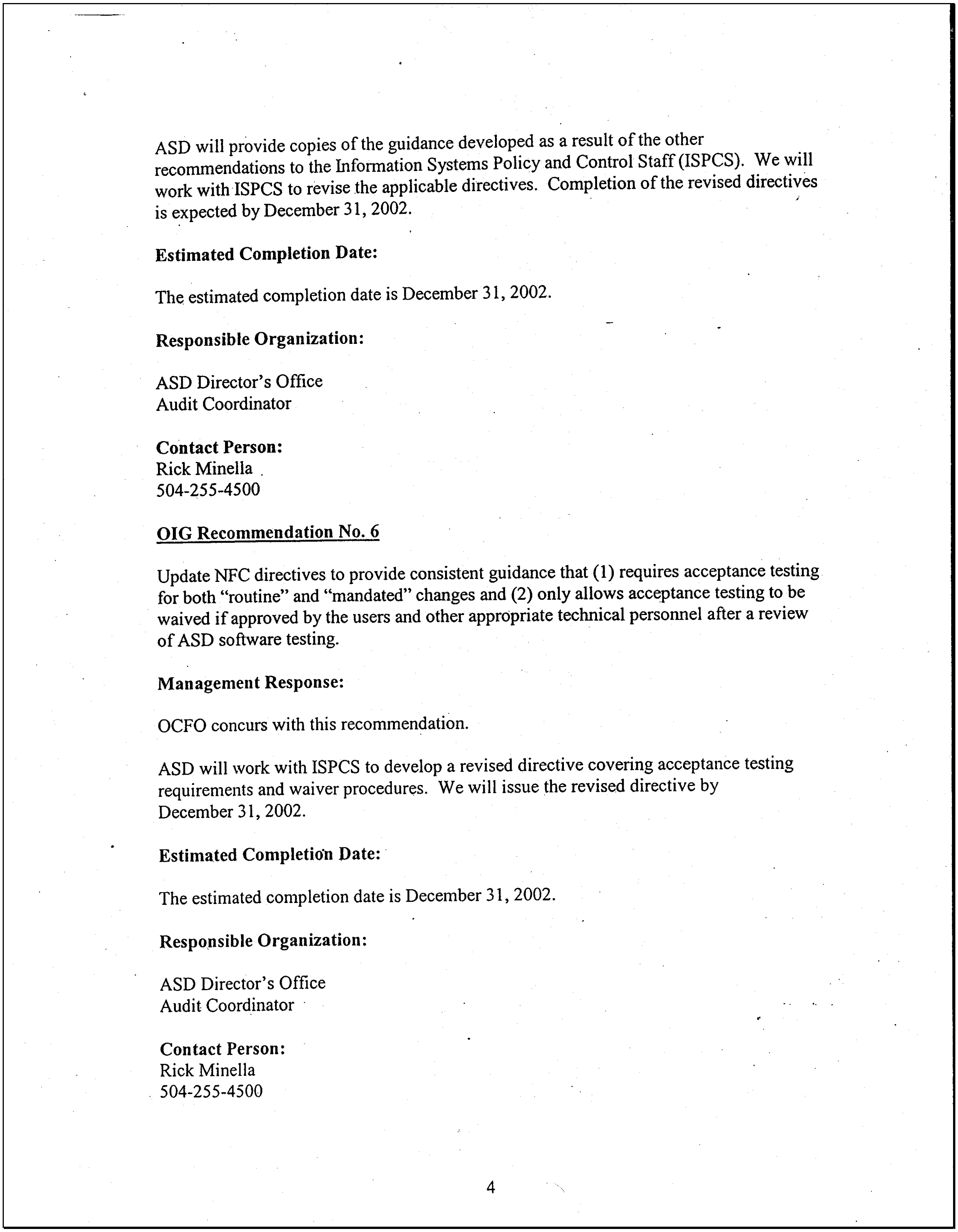
**Contact Person:**
Rick Minella
504-255-4500

<u>**OIG Recommendation No. 5**</u>

Update applicable NFC directives to reflect changes implemented as a result of this audit, provide consistent guidance, and reference other directives associated with application development and change control.

**Management Response:**

OCFO concurs with this recommendation.



ASD will provide copies of the guidance developed as a result of the other recommendations to the Information Systems Policy and Control Staff (ISPCS). We will work with ISPCS to revise the applicable directives. Completion of the revised directives is expected by December 31, 2002.

**Estimated Completion Date:**

The estimated completion date is December 31, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 6</u>**

Update NFC directives to provide consistent guidance that (1) requires acceptance testing for both "routine" and "mandated" changes and (2) only allows acceptance testing to be waived if approved by the users and other appropriate technical personnel after a review of ASD software testing.

**Management Response:**

OCFO concurs with this recommendation.

ASD will work with ISPCS to develop a revised directive covering acceptance testing requirements and waiver procedures. We will issue the revised directive by December 31, 2002.

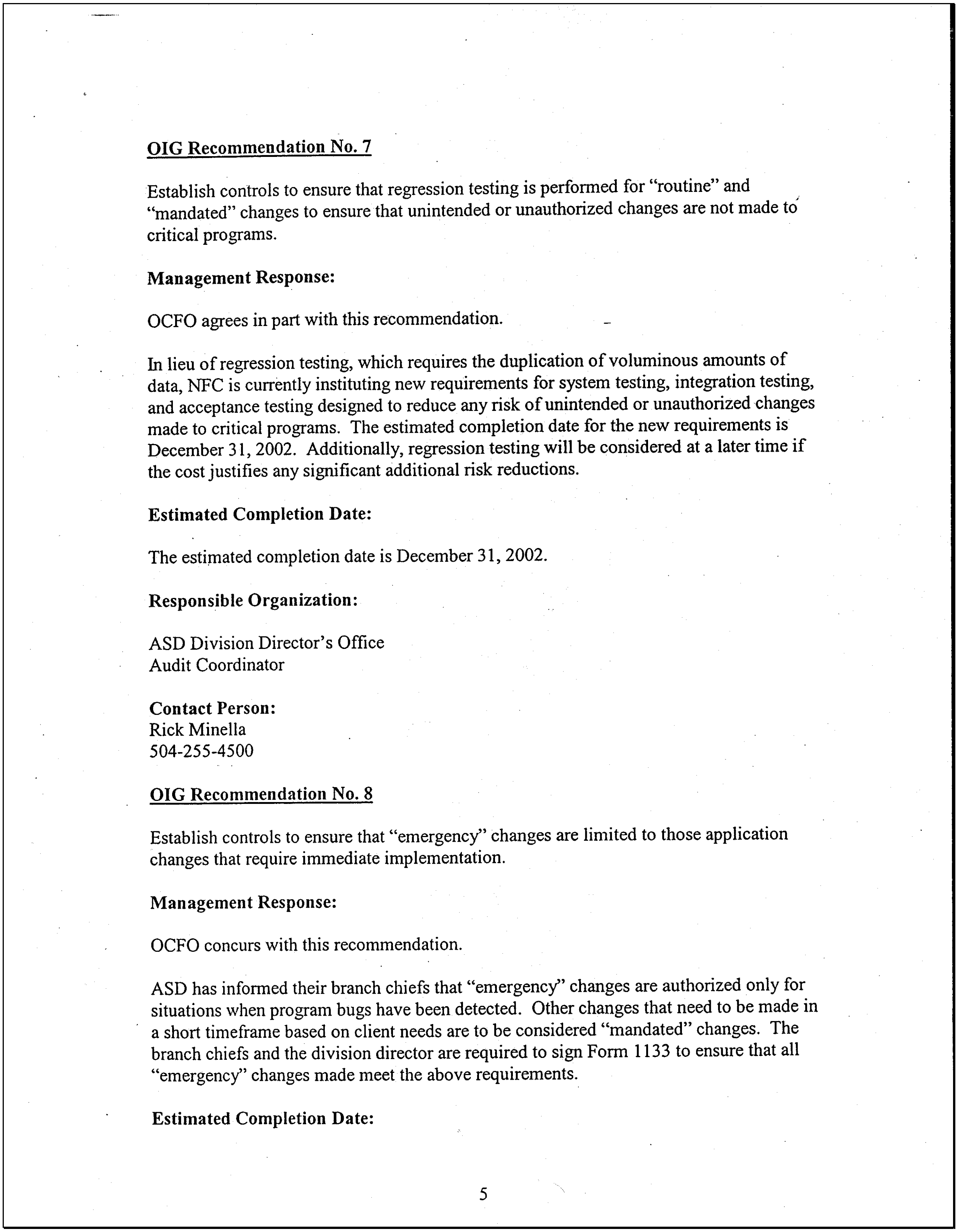
**Estimated Completion Date:**

The estimated completion date is December 31, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500



**OIG Recommendation No. 7**

Establish controls to ensure that regression testing is performed for "routine" and "mandated" changes to ensure that unintended or unauthorized changes are not made to critical programs.

**Management Response:**

OCFO agrees in part with this recommendation.

In lieu of regression testing, which requires the duplication of voluminous amounts of data, NFC is currently instituting new requirements for system testing, integration testing, and acceptance testing designed to reduce any risk of unintended or unauthorized changes made to critical programs. The estimated completion date for the new requirements is December 31, 2002. Additionally, regression testing will be considered at a later time if the cost justifies any significant additional risk reductions.

**Estimated Completion Date:**

The estimated completion date is December 31, 2002.

**Responsible Organization:**

ASD Division Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**OIG Recommendation No. 8**

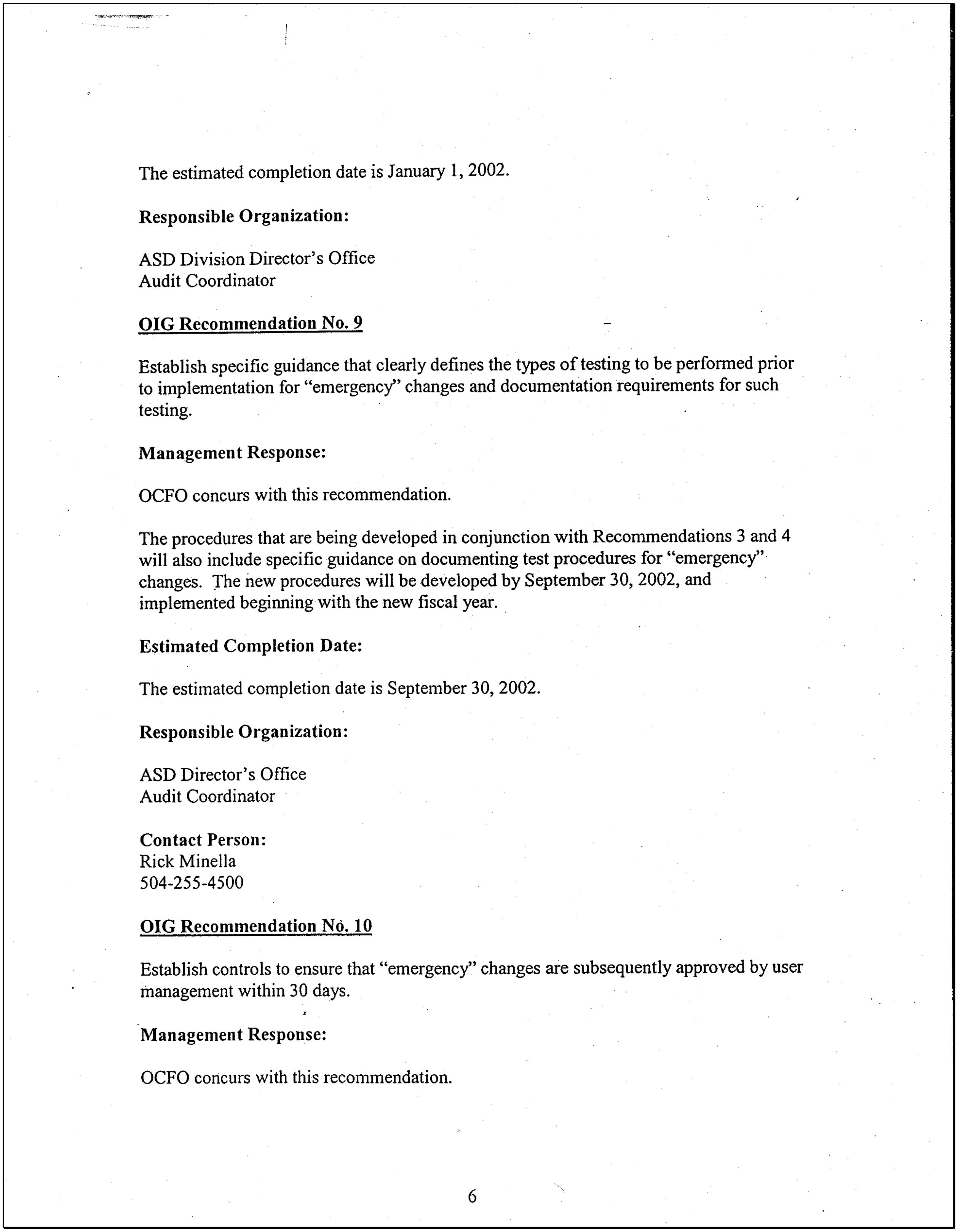
Establish controls to ensure that "emergency" changes are limited to those application changes that require immediate implementation.

**Management Response:**

OCFO concurs with this recommendation.

ASD has informed their branch chiefs that "emergency" changes are authorized only for situations when program bugs have been detected. Other changes that need to be made in a short timeframe based on client needs are to be considered "mandated" changes. The branch chiefs and the division director are required to sign Form 1133 to ensure that all "emergency" changes made meet the above requirements.

**Estimated Completion Date:**



The estimated completion date is January 1, 2002.

**Responsible Organization:**

ASD Division Director's Office
Audit Coordinator

**OIG Recommendation No. 9**

Establish specific guidance that clearly defines the types of testing to be performed prior to implementation for "emergency" changes and documentation requirements for such testing.

**Management Response:**

OCFO concurs with this recommendation.

The procedures that are being developed in conjunction with Recommendations 3 and 4 will also include specific guidance on documenting test procedures for "emergency" changes. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**Estimated Completion Date:**

The estimated completion date is September 30, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**OIG Recommendation No. 10**

Establish controls to ensure that "emergency" changes are subsequently approved by user management within 30 days.

**Management Response:**

OCFO concurs with this recommendation.

As part of the guidance developed for testing and documenting "emergency" changes, ASD will include guidance covering user approval for these types of changes. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**Estimated Completion Date:**

The estimated completion date is September 30, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

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

Identify routine actions, such as updating tables that are currently performed through "special production processing" and develop production programs and/or processes to perform these actions.

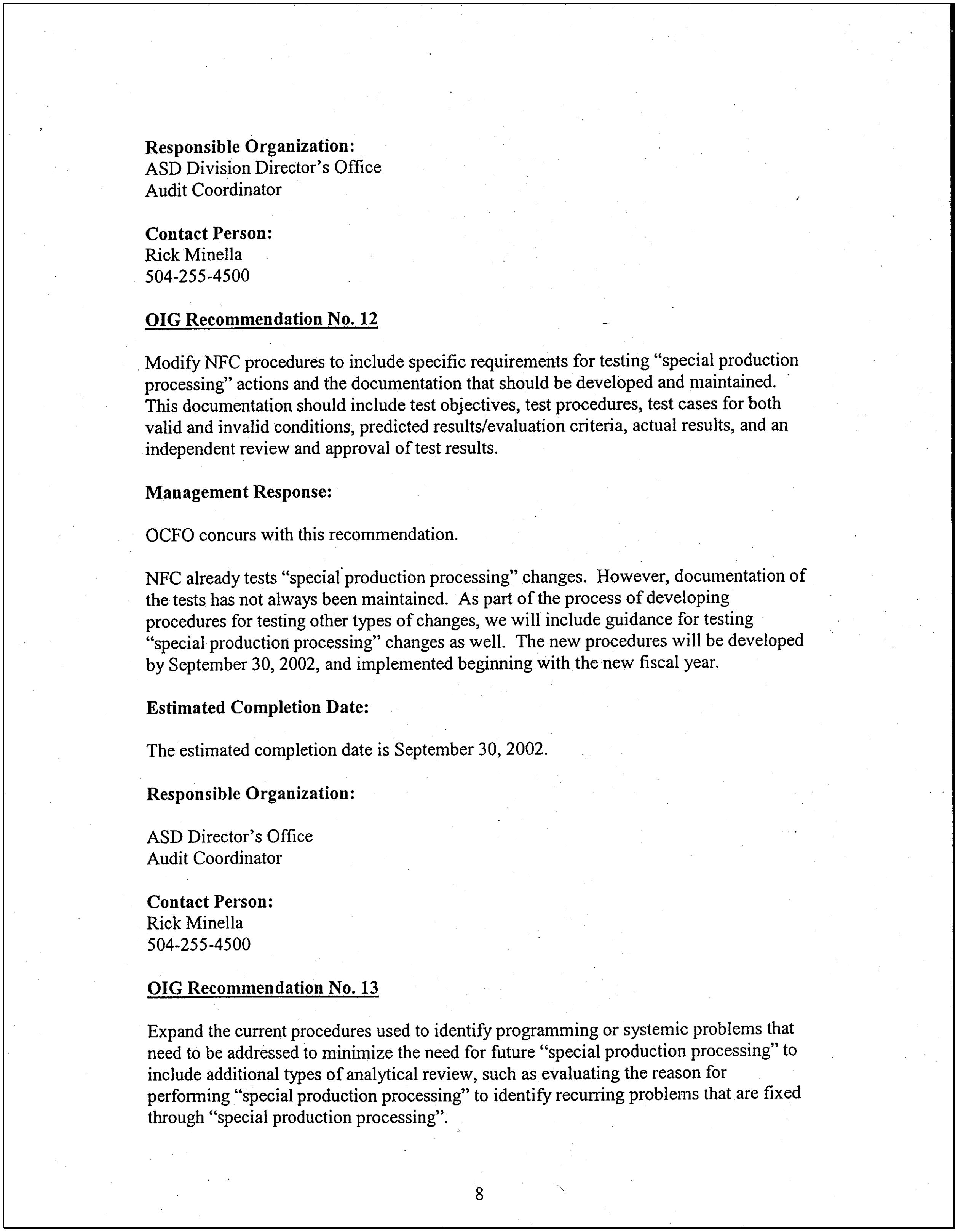
**Management Response:**

OCFO concurs with this recommendation.

NFC will develop procedures that will cover documentation of all "emergency" and "special production processing" projects. A determination will be made as to whether the SPR process is the best method of documenting and analyzing the projects or if a different process should be used. These procedures will be developed by June 30, 2002. NFC will also establish controls to ensure that the present requirements for entering data into the SPR database are followed to ensure that all information is completely entered.

**Estimated Completion Date:**

The estimated completion date is June 30, 2002.



**Responsible Organization:**
ASD Division Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 12</u>**

Modify NFC procedures to include specific requirements for testing "special production processing" actions and the documentation that should be developed and maintained. This documentation should include test objectives, test procedures, test cases for both valid and invalid conditions, predicted results/evaluation criteria, actual results, and an independent review and approval of test results.

**Management Response:**

OCFO concurs with this recommendation.

NFC already tests "special production processing" changes. However, documentation of the tests has not always been maintained. As part of the process of developing procedures for testing other types of changes, we will include guidance for testing "special production processing" changes as well. The new procedures will be developed by September 30, 2002, and implemented beginning with the new fiscal year.

**Estimated Completion Date:**

The estimated completion date is September 30, 2002.

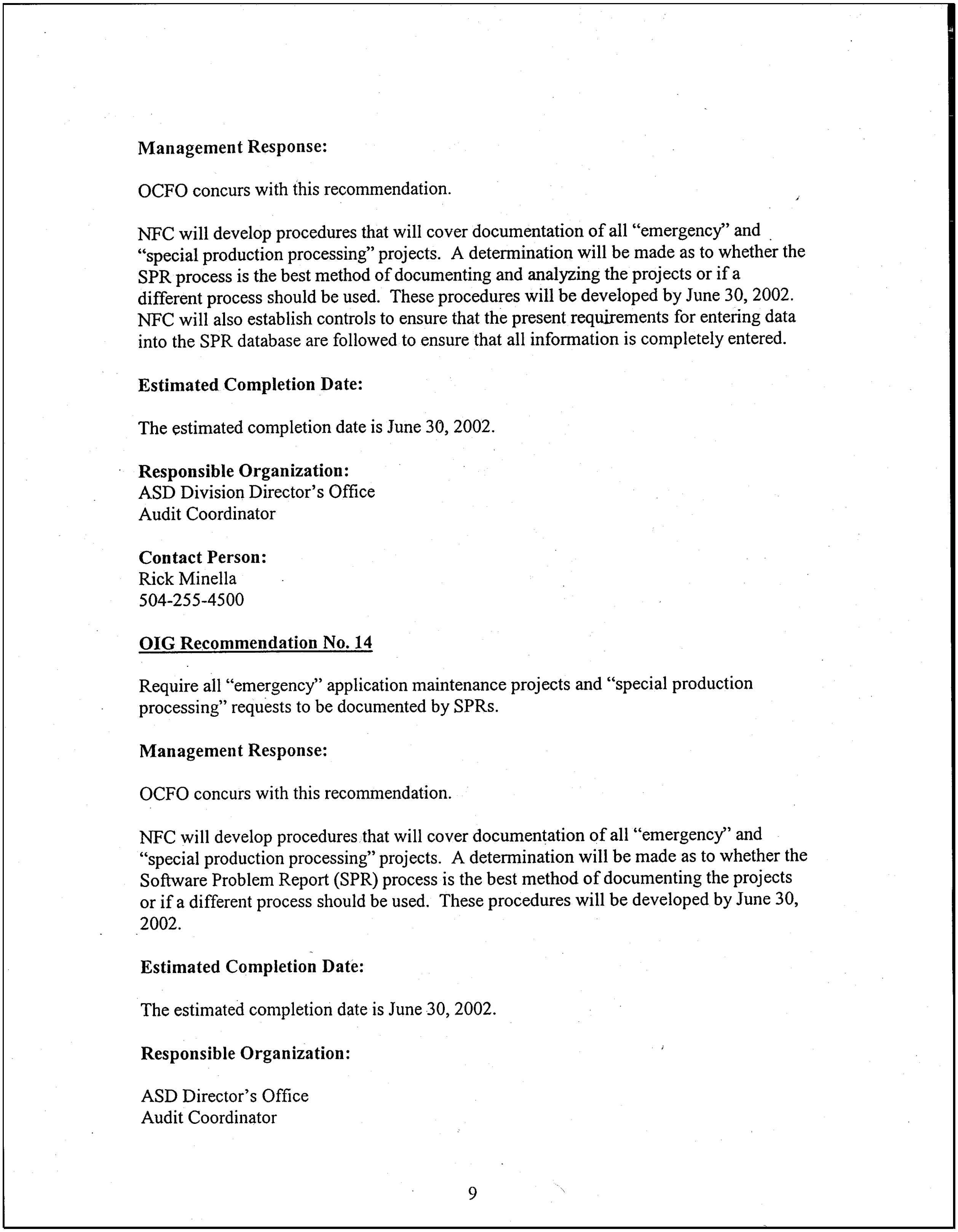
**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 13</u>**

Expand the current procedures used to identify programming or systemic problems that need to be addressed to minimize the need for future "special production processing" to include additional types of analytical review, such as evaluating the reason for performing "special production processing" to identify recurring problems that are fixed through "special production processing".



**Management Response:**

OCFO concurs with this recommendation.

NFC will develop procedures that will cover documentation of all "emergency" and "special production processing" projects. A determination will be made as to whether the SPR process is the best method of documenting and analyzing the projects or if a different process should be used. These procedures will be developed by June 30, 2002. NFC will also establish controls to ensure that the present requirements for entering data into the SPR database are followed to ensure that all information is completely entered.

**Estimated Completion Date:**

The estimated completion date is June 30, 2002.

**Responsible Organization:**
ASD Division Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 14</u>**

Require all "emergency" application maintenance projects and "special production processing" requests to be documented by SPRs.

**Management Response:**

OCFO concurs with this recommendation.

NFC will develop procedures that will cover documentation of all "emergency" and "special production processing" projects. A determination will be made as to whether the Software Problem Report (SPR) process is the best method of documenting the projects or if a different process should be used. These procedures will be developed by June 30, 2002.

**Estimated Completion Date:**

The estimated completion date is June 30, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**OIG Recommendation No. 15**

Expand SPRs to document the outcome and, where applicable, the resulting "special production processing" request or program change. Establish controls to ensure that SPR information is completely entered into the SPR database.

**Management Response:**

OCFO concurs with this recommendation.

NFC will develop procedures that will cover documentation of all "emergency" and "special production processing" projects. A determination will be made as to whether the SPR process is the best method of documenting the projects or if a different process should be used. These procedures will be developed by June 30, 2002. NFC will also establish controls to ensure that the present requirements for entering data into the SPR database are followed to ensure that all information is completely entered.

**Estimated Completion Date:**

The estimated completion date is June 30, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

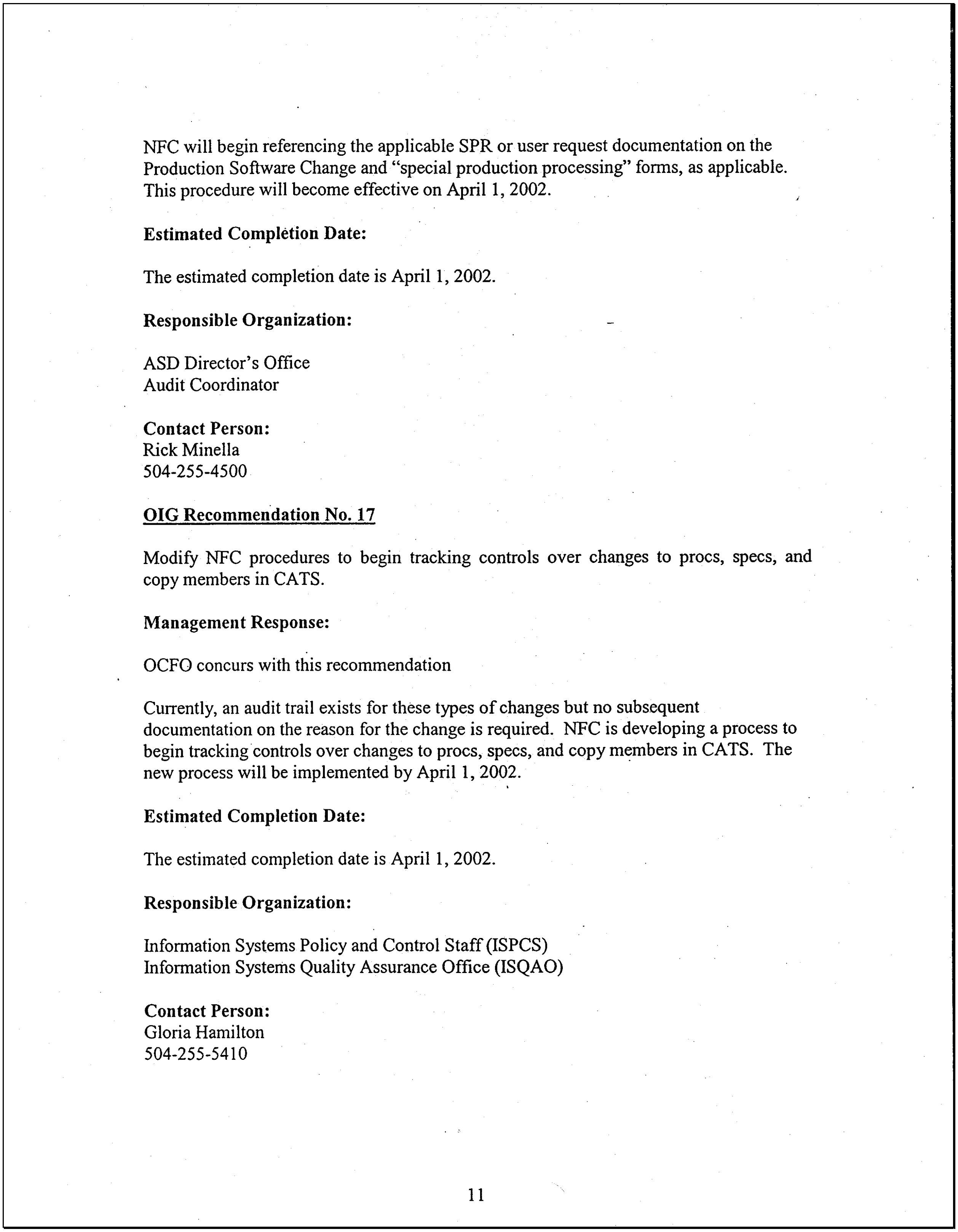
**Contact Person:**
Rick Minella
504-255-4500

**OIG Recommendation No. 16**

Begin referencing the SPR that initiated the change on Production Software Change and "special production processing" forms to ensure that changes can be traced back to the initial user authorization.

**Management Response:**

OCFO concurs with this recommendation.



NFC will begin referencing the applicable SPR or user request documentation on the Production Software Change and "special production processing" forms, as applicable. This procedure will become effective on April 1, 2002.

**Estimated Completion Date:**

The estimated completion date is April 1, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 17</u>**

Modify NFC procedures to begin tracking controls over changes to procs, specs, and copy members in CATS.

**Management Response:**

OCFO concurs with this recommendation

Currently, an audit trail exists for these types of changes but no subsequent documentation on the reason for the change is required. NFC is developing a process to begin tracking controls over changes to procs, specs, and copy members in CATS. The new process will be implemented by April 1, 2002.

**Estimated Completion Date:**

The estimated completion date is April 1, 2002.

**Responsible Organization:**

Information Systems Policy and Control Staff (ISPCS)
Information Systems Quality Assurance Office (ISQAO)

**Contact Person:**
Gloria Hamilton
504-255-5410

OIG Recommendation No. 18

Update the General Purpose Library Maintenance Form to include the ASD maintenance project number or other reason for the change to a procedure, specification, or copy member.

**Management Response:**

OCFO concurs with this recommendation

NFC is updating the General Purpose Library Maintenance Form to include the ASD maintenance project number or other reason for the change to a procedure, specification, or copy member.

**Estimated Completion Date:**

The estimated completion date is April 1, 2002.

**Responsible Organization:**

Information Systems Policy and Control Staff (ISPCS)
Information Systems Quality Assurance Office (ISQAO)

**Contact Person:**
Gloria Hamilton
504-255-5410

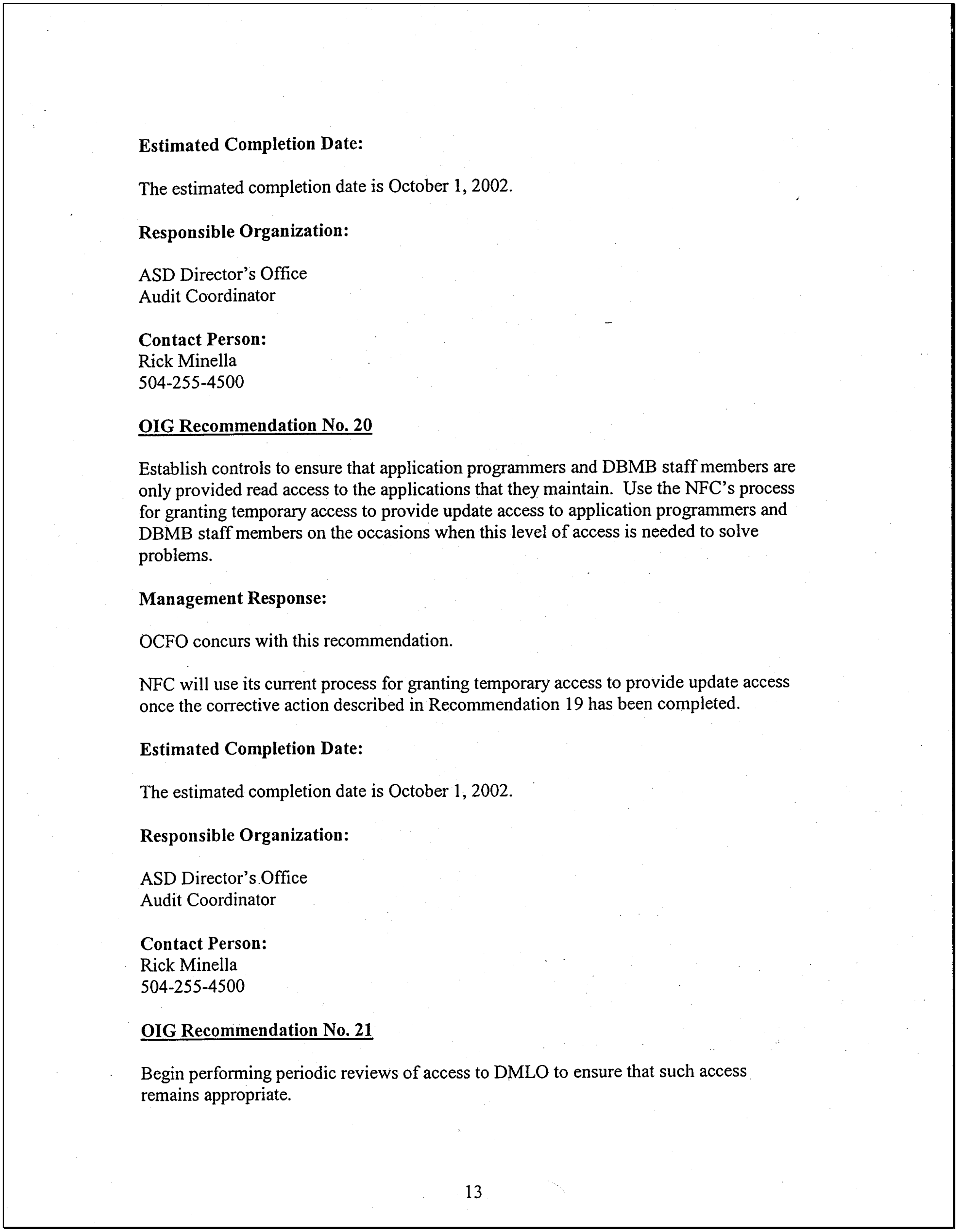
OIG Recommendation No. 19

Establish a method to allow "read only" access to all SPPS functions and re-evaluate access to SPPS to ensure that staff members are assigned the minimum level of access required to perform their job functions.

**Management Response:**

OCFO concurs with this recommendation.

The Special Payroll Processing System was developed with a "read only" capability. However, it was never implemented. NFC is in the process of testing the changes needed to implement the "read only" access and once implemented will ensure that access is granted to staff based on the minimum level of access needed for their job. We expect to implement the "read only" capability by October 1, 2002.



**Estimated Completion Date:**

The estimated completion date is October 1, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 20</u>**

Establish controls to ensure that application programmers and DBMB staff members are only provided read access to the applications that they maintain. Use the NFC's process for granting temporary access to provide update access to application programmers and DBMB staff members on the occasions when this level of access is needed to solve problems.

**Management Response:**

OCFO concurs with this recommendation.

NFC will use its current process for granting temporary access to provide update access once the corrective action described in Recommendation 19 has been completed.

**Estimated Completion Date:**

The estimated completion date is October 1, 2002.

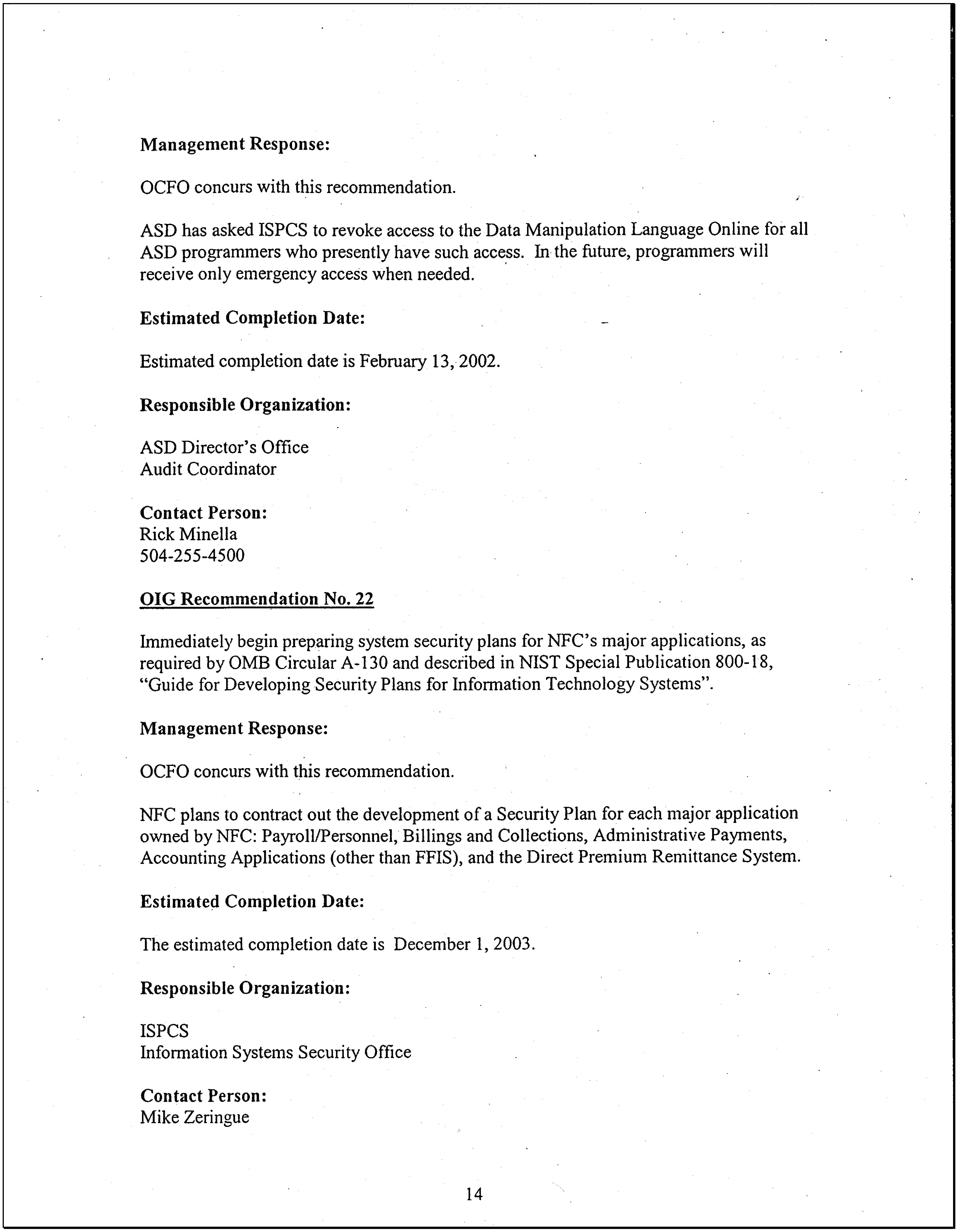
**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**<u>OIG Recommendation No. 21</u>**

Begin performing periodic reviews of access to DMLO to ensure that such access remains appropriate.



**Management Response:**

OCFO concurs with this recommendation.

ASD has asked ISPCS to revoke access to the Data Manipulation Language Online for all ASD programmers who presently have such access. In the future, programmers will receive only emergency access when needed.

**Estimated Completion Date:**

Estimated completion date is February 13, 2002.

**Responsible Organization:**

ASD Director's Office
Audit Coordinator

**Contact Person:**
Rick Minella
504-255-4500

**OIG Recommendation No. 22**

Immediately begin preparing system security plans for NFC's major applications, as required by OMB Circular A-130 and described in NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems".

**Management Response:**

OCFO concurs with this recommendation.

NFC plans to contract out the development of a Security Plan for each major application owned by NFC: Payroll/Personnel, Billings and Collections, Administrative Payments, Accounting Applications (other than FFIS), and the Direct Premium Remittance System.

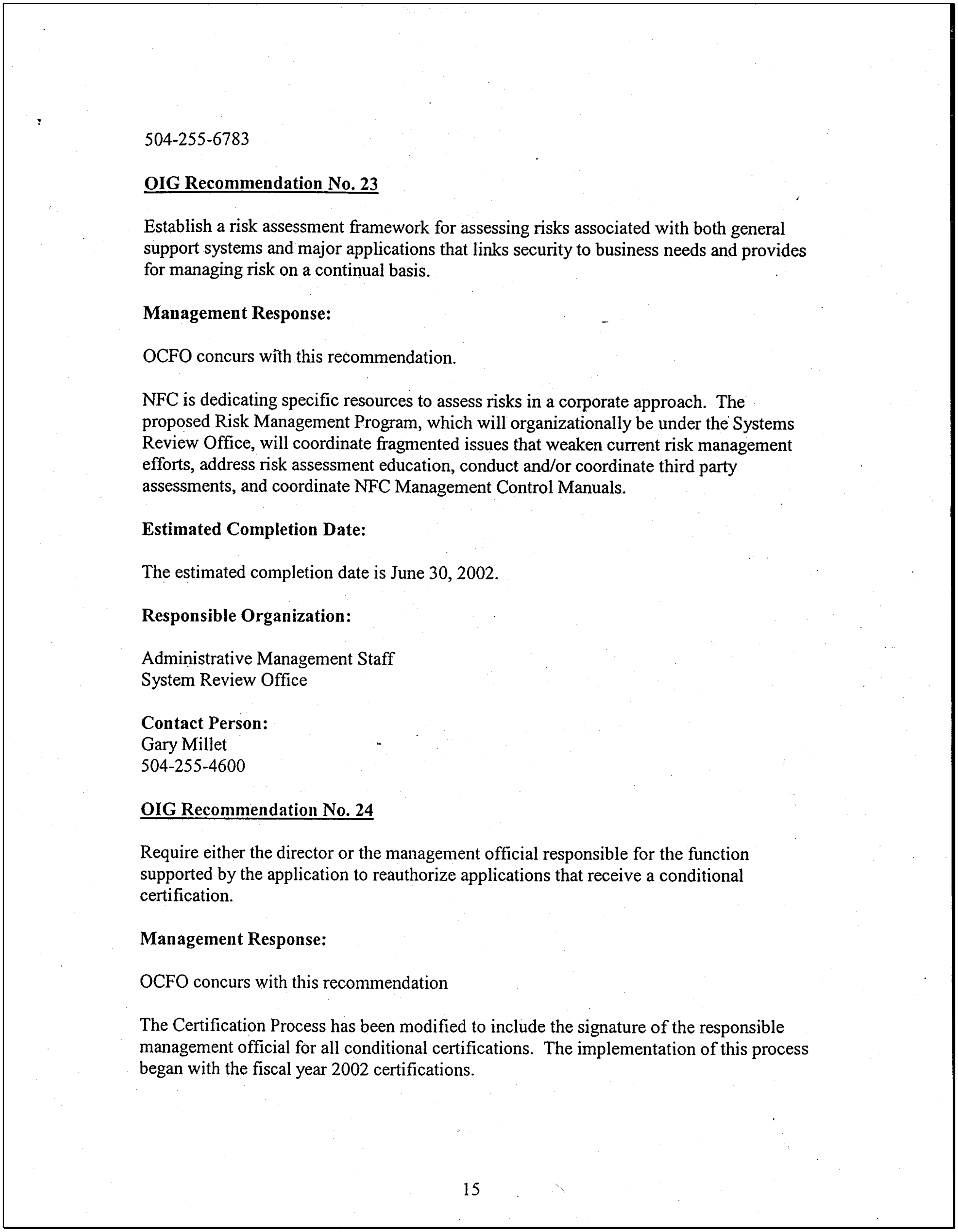
**Estimated Completion Date:**

The estimated completion date is December 1, 2003.

**Responsible Organization:**

ISPCS
Information Systems Security Office

**Contact Person:**
Mike Zeringue



504-255-6783

**OIG Recommendation No. 23**

Establish a risk assessment framework for assessing risks associated with both general support systems and major applications that links security to business needs and provides for managing risk on a continual basis.

**Management Response:**

OCFO concurs with this recommendation.

NFC is dedicating specific resources to assess risks in a corporate approach. The proposed Risk Management Program, which will organizationally be under the Systems Review Office, will coordinate fragmented issues that weaken current risk management efforts, address risk assessment education, conduct and/or coordinate third party assessments, and coordinate NFC Management Control Manuals.

**Estimated Completion Date:**

The estimated completion date is June 30, 2002.

**Responsible Organization:**

Administrative Management Staff
System Review Office

**Contact Person:**
Gary Millet
504-255-4600

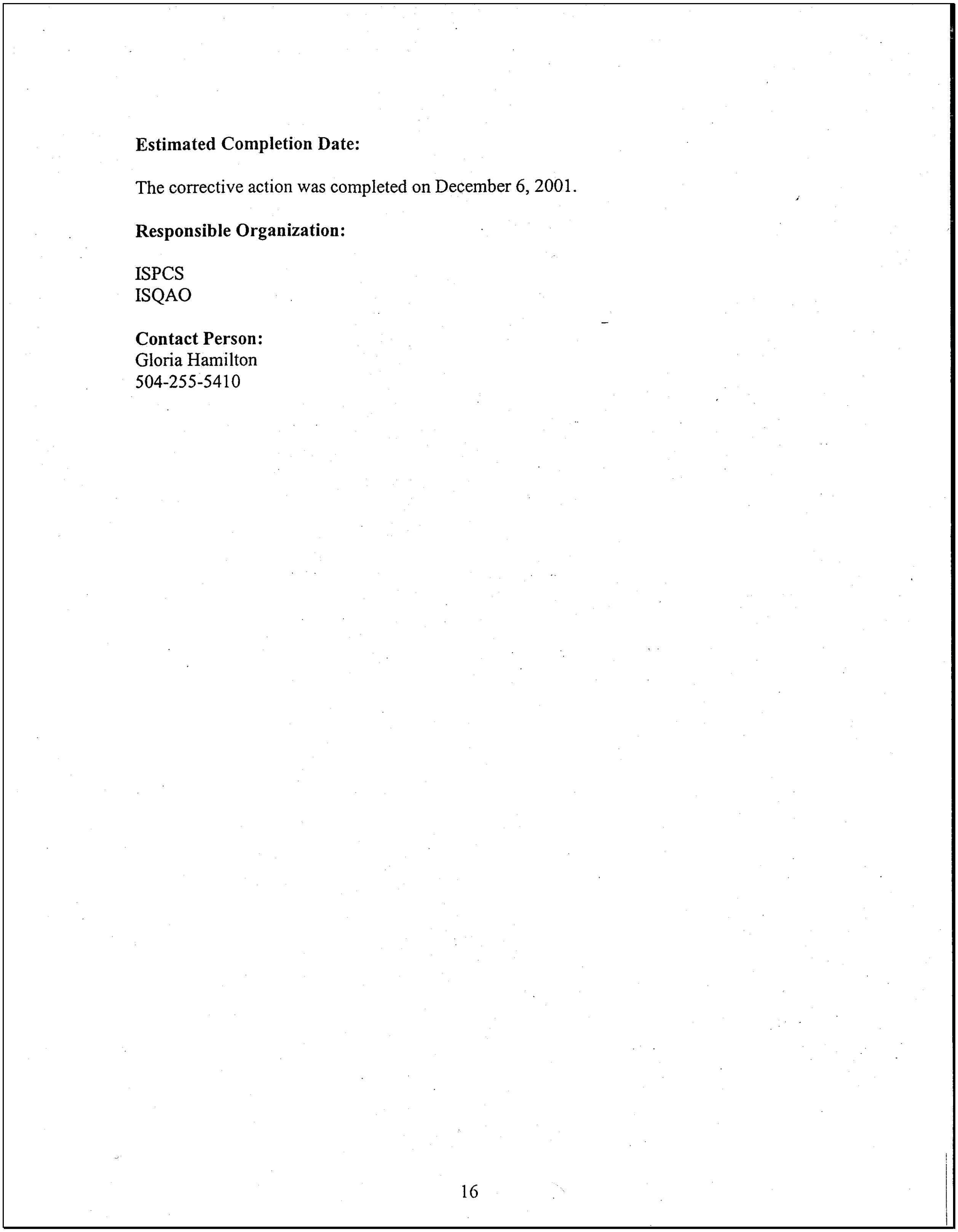
**OIG Recommendation No. 24**

Require either the director or the management official responsible for the function supported by the application to reauthorize applications that receive a conditional certification.

**Management Response:**

OCFO concurs with this recommendation

The Certification Process has been modified to include the signature of the responsible management official for all conditional certifications. The implementation of this process began with the fiscal year 2002 certifications.



**Estimated Completion Date:**

The corrective action was completed on December 6, 2001.

**Responsible Organization:**

ISPCS
ISQAO

**Contact Person:**
Gloria Hamilton
504-255-5410

# ABBREVIATIONS

| | |
|---|---|
| ASD | Application Systems Division |
| CATS | Change Authorization Tracking System |
| CMM | Capability Maturity Model |
| DBMB | Database Management Branch |
| DMLO | Data Manipulation Language Online |
| GAO | General Accounting Office |
| ISQAO | Information Systems Quality Assurance Office |
| IT | Information Technology |
| MISCPAY | Miscellaneous Payment System |
| NFC | National Finance Center |
| NIST | National Institute of Standards and Technology |
| OB | Operations Branch |
| OCFO | Office of the Chief Financial Officer |
| OMB | Office of Management and Budget |
| PATS | Planning and Tracking System |
| SPPS | Special Payroll Processing System |
| SPR | Software Problem Report |
| SRD | Software Requirements Document |
| USDA | United States Department of Agriculture |

# GLOSSARY

Acceptance testing

At NFC, this type of software testing determines if the software satisfies the acceptance criteria of the owners, users, and operators.

Capability Maturity Model

The Capability Maturity Model (CMM) developed by the Software Engineering Institute is an internationally recognized model for rating software development capabilities. CMM defines five levels of organizational maturity, with Level 5 being the highest. A Level 2 office has consistent project planning and execution, and through uniformity, the means to repeat software successes and avoid repeating software errors.

Change Authorization Tracking System

The Change Authorization Tracking System (CATS) is used to obtain ASD approval and track the reason for changes to production software.

Copy members

Copy members contain common code that is shared by more than one program.

Data Manipulation Language Online

Data Manipulation Language Online (DMLO) is a powerful database utility that can be used to update the data stored in an Integrated Data Base Management System (IDMS) database directly (e.g. without using an application program).

Emergency change

NFC defines an “emergency” change as a production software change that require immediate implementation to correct an error in the existing version of application software and bypass testing controls prior to implementation.

Functional requirements

At NFC, functional requirements formally document all of the functions that the users require the application to perform. (Also see software requirements document.)

Integration testing

This type of software testing is used to demonstrate that different software components work together properly.

Mandated changes

NFC defines “mandated” changes as production software changes other than “emergency” changes and “routine” changes implemented as part of a scheduled release. Thus, “mandated” changes are not limited to changes mandated by legislative requirements.

Planning and Tracking System

The Planning and Tracking System (PATS) is an online database management system that provides NFC with information on the status and scheduling of projects and the staffing resources used in project development.

Procedures

Procedures (procs) are files that contain the execution Job Control Language (JCL) associated with a particular program.

Regression testing

This type of software testing is performed to detect faults introduced during modification of a system and ensure that software components that did not change are still working correctly.

Routine changes

NFC defines routine changes as production software changes that are approved modifications or enhancements of application software that can be planned for implementation in a scheduled release.

Scheduled release

A regularly planned update of an application in which routine changes are combined with the “emergency” and “mandated” changes implemented since the last scheduled release.

Software Problem Report

A software problem report (SPR) is used by ASD to document problems relating to the application systems it develops and maintains. SPRs also serve as documentation of maintenance requirements for ASD applications.

Software Requirements Document

ASD uses the software requirements document (SRD) to describe the functional requirements of a change request. Specifically, this document specifies purpose of the change and what needs to be accomplished with enough detail to enable programmers to satisfy the requirements and testers to ensure that the changes satisfy the requirements.

Special production processing

Special production processing, which was previously referred to as production deviations, is the term NFC uses to describe changes made to production data, programs, and procedures outside of standard methods.

Specifications

Specifications (specs) are files that contain data to be included in the execution JCL.

System testing

This type of software testing covers the entire application and may include tests of both automated and manual processes.

Unit testing

This type of software testing checks individual program modules for typographic, syntactic, and logic errors.

User management

The manager responsible for the operations that the application supports.