U.S. Department of Agriculture

Office of Inspector General
Financial and IT Operations

Audit Report

National Information Technology Center
General Controls Review – Fiscal Year 2003

Report No. 88099-5-FM
October 2003

USDA

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: OCT 20 2003

REPLY TO
ATTN OF: 88099-5-FM

SUBJECT: National Information Technology Center – General Controls Review
Fiscal Year 2003

TO: Scott Charbo
Chief Information Officer
Office of the Chief Information Officer

This report presents the results of our audit of the internal control structure at the Office of the Chief Information Officer/National Information Technology Center (OCIO/NITC) as of September 30, 2003. The audit was conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States including the American Institute of Certified Public Accountants Professional Standards AU Sections 316, 319, and 324 as amended by applicable statements on auditing standards. While the center has taken significant corrective actions during the fiscal year, the report contains a qualified opinion on the internal control structure because certain control policies and procedures were not suitably designed or had not yet been placed in operation at the time of our review.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned, and the timeframes for implementation. Please note that the regulation requires a management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

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

for Marlane T. Evans

RICHARD D. LONG
Assistant Inspector General
for Audit

Executive Summary

National Information Technology Center – General Controls Review Fiscal Year 2003

Results in Brief

This report presents the results of our audit of the Office of the Chief Information Officer/National Information Technology Center's (OCIO/NITC) internal control structure as of September 30, 2003. Our review was conducted in accordance with "Government Auditing Standards" issued by the Comptroller General of the United States including American Institute of Certified Public Accountants Professional Standards AU Sections 316, 319, and 324 as amended by applicable statements on auditing standards. While the center has taken significant actions to mitigate the weaknesses we identified, the report contains a qualified opinion on the internal control structure because certain control policies and procedures were not suitably designed or had not yet been placed in operation at the time of our review. The U.S. General Accounting Office (GAO) recently completed internal controls testing at OCIO/NITC and a separate report will be issued by that office. We worked closely with GAO to ensure that we did not duplicate its efforts. Therefore, we limited our review to the control objectives and techniques identified in exhibit A of this report.

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

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

OCIO/NITC continues to take actions toward complying with federally mandated security requirements. However, the necessary corrective actions are long-term in nature and continued actions are needed. OCIO/NITC has made a concerted effort toward completion of risk assessments, which is an important step toward improving security. We found that OCIO/NITC needs to prepare security plans and contingency plans for its general support systems and complete the system certification and accreditation process for

its critical systems. Corrective action is scheduled to be completed in early calendar year 2004.

OCIO/NITC has improved its controls over logical access to its systems, but additional actions are needed to ensure the confidentiality and integrity of its resources. Specifically, we noted instances where OCIO/NITC had not removed separated employees' remote access accounts, completed documentation of users with special access privileges, completed its review and documentation of security software parameters, implemented polices and procedures outlining monitoring of security logs, and completed its implementation of secure Internet access. OCIO/NITC is implementing corrective actions.

Finally, OCIO/NITC has strengthened and continues to improve its system change management process. However, since not all of its improved controls were in place throughout the fiscal year, we continued to find that approval, testing, and implementation documentation was not always maintained. Without proper change management controls, OCIO/NITC's systems are at risk of processing irregularities that could occur or security features that could be inadvertently or deliberately omitted or rendered inoperable. OCIO/NITC plans to correct the change management process by July 2004.

Our qualified opinion on OCIO/NITC's general control structure is based on its operations from October 1, 2002, through September 30, 2003. While we believe that the findings in this report are material, OCIO/NITC has taken significant actions throughout the year to mitigate the weaknesses we identified. Therefore, we do not recommend that they be included as material weaknesses in its Federal Managers' Financial Integrity Act Report.

Recommendation In Brief

OCIO/NITC is in the process of implementing significant actions to correct the weaknesses we identify in this report, based on prior Office of Inspector General (OIG) recommendations. Therefore, we make no additional recommendations on outstanding issues. However, we have made a recommendation to periodically reconcile OCIO/NITC user identifications to current employees and contractors to ensure timely removal of unneeded accounts.

Abbreviations Used in This Report

DM	Department Manual
FIPS	Federal Information Processing Standards
GAO	General Accounting Office
ICS	Incident Command Structure
ID	Identification (i.e., user accounts or user identification)
IT	Information Technology
MOU	Memorandums of Understanding
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication
USDA	United States Department of Agriculture

Table of Contents

Report of the Office of Inspector General

To: Scott Charbo
Chief Information Officer
Office of the Chief Information Officer

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

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

Our review disclosed material internal control weaknesses. We found that the OCIO/NITC needs to strengthen its logical access controls; establish controls to ensure system software changes are approved, documented, and tested; and ensure that it is in compliance with existing Federal security guidelines.

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

Also, in our opinion, except for matters discussed above, the policies and procedures that were tested, as described in the exhibit, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified were achieved during the period from October 1, 2002, to September 30, 2003. The scope of our engagement did not include tests to determine whether control objectives not listed in the exhibit were achieved; accordingly, we express no opinion on achievement of control objectives not included in the exhibit.

The relative effectiveness and significance of specific controls at OCIO/NITC and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have preformed no procedures to evaluate the effectiveness of controls at individual user organizations.

The control objectives and techniques at OCIO/NITC are as of September 30, 2003, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 2002, to September 30, 2003. Any projections of such information to the future are subject to the risk that, because of change, they may no longer portray the controls in existence. The potential effectiveness of specific controls at OCIO/NITC is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. The projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions. Furthermore, the accuracy and reliability of data processed by OCIO/NITC and the resultant report ultimately rests with the user agency and any compensating controls implemented by such agency.

This report is intended solely for the management of OCIO/NITC, its users, and their auditors.

Marlene T. Evans

for RICHARD D. LONG
Assistant Inspector General
for Audit

September 30, 2003

An entity-wide program for security planning is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied.

The Computer Security Act of 1987 provides a means for establishing minimally acceptable security practices related to Federal computer systems. The Act requires agencies to identify and protect systems containing "sensitive" information and requires a computer standards program and security training. Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," established a minimum set of controls for agencies' automated information security programs, including (1) preparing security plans for each general support or major application, (2) preparing and testing contingency plans and recovery procedures in the event of a disaster, (3) conducting system certifications to ensure systems are properly secured, and (4) ensuring that all individuals are appropriately trained in how to fulfill their security requirements before allowing them access to the system.

Finding 1

Further Actions are Needed to Ensure Compliance with Federal Regulations and Guidance

While significant improvements have been made, such as its efforts toward completion of risk assessments, OCIO/NITC is still not totally compliant with the requirements of OMB Circular A-130 and other Federal security guidance. Specifically, OCIO/NITC had not (1) completed security plans for each of its general support systems, (2) prepared contingency plans for each of its general support systems, (3) completed system certifications and accreditations for each of its general support systems, or (4) provided security awareness training to all staff to ensure staff are aware of system rules of behavior and know what actions to take in the event of a disaster. OCIO/NITC recognizes that these actions need to be completed and has identified them in its Plans of Action and Milestones. OCIO/NITC officials informed us that meeting the requirements of OMB Circular A-130 and National Institute of Standards and Technology (NIST) security guidelines involve major efforts

and require time and resources to thoroughly comply. However, until these controls and documents are in place, OCIO/NITC cannot be assured of the confidentiality, integrity, and availability of its computer resources.

OMB Circular A-130[1] established a minimum set of controls for agencies' automated information security programs, including preparing security plans for major applications and general support systems, certifying to the security of any systems that maintain sensitive data, and establishing contingency plans and recovery procedures in the event of a disaster. OMB further requires agencies to ensure that all individuals are appropriately trained in how to fulfill their security requirements before allowing them access to the systems.

Security Plans

While OCIO/NITC has completed a security plan for its mainframe operations, it has not completed security plans for its general support systems. OCIO/NITC's mid-range system environment is an increasingly expanding segment of its operations. As such, OCIO/NITC has recognized the need for these security plans and was in the process of completing these during our fieldwork. OCIO/NITC officials estimated completion of these plans by September 30, 2003.

Contingency Plans

Based in part on the Office of Inspector General's (OIG) prior recommendations,[2] OCIO/NITC has strengthened its business continuity and contingency planning process. However, OCIO/NITC has not completed contingency plans for its general support systems. OCIO/NITC has also recognized the need to create contingency plans for each of its general support systems and has established a mid-range recovery team to address this issue. OCIO/NITC is currently in the process of preparing contingency plans for its general support systems, and telecommunications and estimates completing this effort in early calendar year 2004. Without an effective, operable recovery plan for those systems, OCIO/NITC cannot be assured that it will be able to provide efficient continued automated processing services to support its customers.

[1] OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.
[2] Audit Report No. 88099-04-FM, "National Information Technology Center - General Controls Review Fiscal Year 2002," dated December 12, 2002.

System Certification and Accreditation

OCIO/NITC has not completed system certifications and accreditations for its general support systems. OCIO/NITC recognizes system certifications are needed and has established a plan to have the systems accredited within Department OCIO-established timeframes. As part of this effort, OCIO/NITC is developing system security check procedures to ensure all tests are performed consistently. OCIO/NITC is reviewing system security settings to ensure settings meet best practice standards and comply with laws and regulations. OCIO/NITC plans to implement a new policy and standardized procedures for security test and evaluation with an estimated completion date of September 30, 2003.

Security Training

OCIO/NITC was not able to provide evidence that all staff received security awareness training. OCIO/NITC did provide documentation that its staff received Bomb Threat Awareness training, Incident Command System (ICS), and ICS Live Test training. OCIO/NITC also provides staff with quarterly newsletters that provide security-related information. OCIO/NITC has since adopted the Department's recommended online security awareness training package and plans to have all staff complete the security-awareness training module by September 30, 2003.

We also noted that despite our prior report's recommendation to ensure that all disaster recovery members are trained in their responsibilities, OCIO/NITC had not provided disaster recovery training to all staff responsible for disaster recovery. This was due to the development of a new Incident Command Structure (ICS) as part of the restructuring of the Business Continuity Plan. This new structure included several more OCIO/NITC employees than prior structures. Not all of the newly added employees had received training in their responsibilities. OCIO/NITC anticipates all ICS members to have formal training by December 2003. Until such time, OCIO/NITC cannot be assured that this staff knows what actions to take in the event of a disaster. OCIO/NITC relies on its disaster recovery exercises as training for those with recovery responsibilities.

As we have noted above, OCIO/NITC has made a concerted effort over the last year and continues to work toward compliance with the federally mandated requirements. Many of the efforts are based on actions agreed to from our prior audit report; hence, we are making no further recommendations on these issues in this report.

Finding 2 — Access Controls Need Strengthening

OCIO/NITC continues to improve its controls over logical access to its systems based in part on prior OIG recommendations; however, further actions are needed to ensure the confidentiality and integrity of its information technology (IT) resources. Specifically, OCIO/NITC had not completed implementation of procedures to ensure (1) separated employee remote access accounts are timely removed, (2) users with special access privileges are documented, (3) global security software system parameters are documented, (4) policies and procedures outlining monitoring of security logs are implemented, and (5) access controls from the Internet are properly secured. While OCIO/NITC has begun to address these issues as discussed below, not all of the necessary controls were in place throughout the year to ensure the confidentiality and integrity of its IT resources. Until stronger controls over access are in place, OCIO/NITC resources are vulnerable to potential fraud and misuse, inappropriate disclosure, and potential disruption.

OMB[3] stresses the need for management controls affecting users of IT to protect the integrity, availability, and confidentiality of information by restricting access to only authorized users. OMB also stresses that individual accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. Both OMB and NIST[4] stress the need for agencies to implement the "least privilege" concept, granting users only those accesses required to perform their duties. Department Manual (DM)[5] requires security staff to remove employee user identifications (ID) and passwords when the employee is no longer with the agency.

User Accounts

Our review of OCIO/NITC employee and contractor user IDs disclosed the following:

- Two user accounts[6] for separated employees on its remote access system were no longer needed, and

[3] OMB Circular A-130, Appendix III, Section A, November 30, 2000.
[4] NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," dated December 1998.
[5] DM 3140-1.6, part 6 of 8, Section 6c, "Management ADP Security Manual," July 19, 1984.
[6] OCIO/NITC officials informed us that these two accounts have been deleted.

- 17 mainframe user IDs still existed for separated employees and contractors.

Since our prior report, OCIO/NITC established a "least privilege" policy[7] and an inactive account policy,[8] which outline their method to monitor account activity and remove user accounts that are no longer needed. However, we found that the security personnel who are responsible for removing user IDs do not consistently receive the forms used to process these requests. Further, OCIO/NITC does not have procedures in place to periodically reconcile user accounts to a list of current employees and contract personnel. OCIO/NITC immediately deleted the problem accounts after we brought them to its attention.

Furthermore, we found only a slight decrease in user IDs with passwords set to never expire and requested to see the waivers for these user IDs. It was determined that one agency was responsible for a majority of these user IDs. Of the 22,180 user IDs on its main system, 928 had passwords set to never expire as compared to 941 out of 22,124 user IDs in 2002. OCIO/NITC informed the agency security officers of its new security policy that passwords should be set to expire within 60 days and that exceptions to this policy must have a waiver; however, the agency has yet to provide a waiver.

Special Access Privileges

Based on a prior OIG recommendation,[9] OCIO/NITC updated guidance for requesting and monitoring user accounts with special access privileges. This policy requires OCIO/NITC management staff and system or application owners to ensure the appropriate documentation is completed to justify the need for user accounts and conduct periodic reviews to eliminate special access privileges or removal of accounts no longer needed. OCIO/NITC is in the process of documenting and certifying all user accounts that OCIO/NITC is responsible for monitoring such as user accounts for agency security officers, started task, batch, and other system related user accounts. Thereby, OCIO/NITC will ensure that only staff that have a valid job-related need have system privileges.

[7] OCIO/NITC Security Directive-1-5, "NITC Least Privilege Policy," dated March 26, 2003.
[8] OCIO/NITC Security Directive-5-1, "NITC Inactive Accounts Policy," dated March 12, 2003.
[9] Audit Report No. 88099-3-FM, "National Information Technology Center - General Controls Review Fiscal Year 2000," dated September 21, 2001.

Security Software Global System Settings

During our review, OCIO/NITC had not completed its review and documentation of its systems' global security settings. Global system settings define how the network-wide security software operates within the mainframe environment, such as resource access control settings, user activity logs for IDs with special privileges, and logs of profile changes. While there are no 'required' global system settings, manufacturer and industry standard settings should be used to facilitate the most effective and secure computing environment. At a minimum, OCIO/NITC should document its global system settings and justify those settings when they do not conform to manufacturer or industry standard suggestions. Deviation from these standards may be appropriate since each operating environment is unique; however, without adequate documentation it is impossible to validate whether global system parameters are adequately configured and tested to maintain the integrity of the security software. OCIO/NITC officials have informed us that they have since completed their review and documentation of system global security settings and, when appropriate, have made the necessary changes to those settings.

Monitoring Access

OCIO/NITC does not have written policies and procedures outlining what (1) logs/reports will be reviewed, (2) actions will be taken for different security violations, (3) security violations will be investigated, or (4) supporting documentation will be created and maintained supporting any investigations. Additionally, OCIO/NITC has not documented which security violation it noted, the level of investigation it initiated, the results of its investigation, the remedial action taken by the security staff to prevent a recurrence, and whether it identified patterns of violations. OCIO/NITC is in the process of developing system security log review standards. Until these standards have been finalized and implemented, OCIO/NITC management cannot be assured that security violations are properly and consistently identified, and that followup is adequately carried out.

System audit logs would provide management with valuable information about activity on its computer systems, including a review and analysis of management, operational, and technical controls. OMB[10] states that identifying and authenticating system users, and subsequently tracing actions on the system to the users who initiated them normally accomplishes accountability. In addition, DM 3140-1.3[11] requires maintaining access logs sufficient to permit reconstruction of events in case of unauthorized data or

[10] OMB Circular A-130, Appendix III, Section B (a)(2)(c), November 30, 2000.
[11] DM 3140-1.3, "Management ADP Security Manual," Part 3 of 8, Section 16, July 19, 1984.

program access or use. Security/access control software should be used to maintain an audit trail of security accesses to determine how, when, and by whom specific actions were taken. Such information is critical in monitoring compliance with security policies and when investigating security incidents.

Because all of the audit trail information maintained is likely to be too voluminous to review on a routine basis, procedures should be implemented to selectively identify unauthorized, unusual, and sensitive access activity. It is important that an entity have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, others can be altered to potential threats, and appropriate investigations can be performed. Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an entity's resources indefinitely. Further, violators will not be discouraged from continuing inappropriate access activity, which could result in financial losses and disclosure of confidential information.

Mainframe Access From the Internet

Based in part on a prior OIG recommendation,[12] OCIO/NITC moved the mainframe environment behind its firewalls on September 7, 2003. According to OCIO/NITC officials, this was the final step toward securing access to OCIO/NITC network resources from the Internet. However, before OCIO/NITC can encrypt all access to its recourses, its customers need to implement changes on their networks. Therefore, OCIO/NITC officials will allow unencrypted access from the Internet until January 1, 2004, to provide its customers the time to take appropriate actions.

Recommendation No. 1

Establish controls and procedures to periodically reconcile OCIO/NITC user IDs with current employees and contractors to ensure the timely removal of unneeded accounts.

[12] Audit Report No. 88099-3-FM, "National Information Technology Center - General Controls Review Fiscal Year 2000," dated September 21, 2001.

Finding 3

Change Control Improvements Need to be Finalized and Implemented

Based in part on a prior OIG recommendation,[13] OCIO/NITC has strengthened and continues to improve its system change management process. However, since not all of its improved controls were in place throughout the fiscal year, we continued to find that approval, testing, and implementation documentation was not always maintained. Without proper change management controls, OCIO/NITC's systems are at risk of processing irregularities that could occur or security features that could be inadvertently or deliberately omitted or rendered inoperable.

According to NIST SP 800-37,[14] "Guide for the Security Certification and Accreditation of Federal Information Systems," it is important to document the proposed or actual changes to the information system and to subsequently determine the impact of those proposed or actual changes on the security of the system. Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation. Ensuring adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment requires an effective agency configuration management and control policy and associated procedures.

In our prior year's audit, we found that new system software versions or modifications to existing software were not properly authorized, tested, or logged. OCIO/NITC began to address the system software change control issues at the close of our prior audit by revising its directives related to change management and reengineering the change control process. Implementing these directives should help ensure personnel follow established change control procedures for identifying, selecting, approving, installing, and modifying system software, and help ensure that

[13] Audit Report No. 88099-4-FM, "National Information Technology Center - General Controls Review Fiscal Year 2002," dated December 12, 2002.

[14] NIST SP 800-37, dated June 30, 2003, is still in draft and will replace Federal Information Processing Standards Publication (FIPS) 102, "Guidelines for Computer Security Certification and Accreditation," dated September 27, 1983, which is still current, FIPS 102 discusses these issues on page 19, Section 1.5.2; page 52, Section 2.7; and page 54, Section 2.7.3.

documentation exists for these change processes. Further, the updated policies require implementation of a Service Request System for the routine or very common changes. OCIO/NITC plans to have the change management process completed by July 2004.

General Comments

OCIO/NITC is in the process of preparing memorandums of understandings (MOUs) for their mainframe customers and expects to issue the revised MOUs to agencies after October 1, 2003. OCIO/NITC prepared MOUs for their mid-range or client/server customers. OCIO/NITC is converting the mainframe customer folders into the format that the client/server folders are in now.

The U.S. General Accounting Office (GAO) recently completed internal controls testing at OCIO/NITC and a separate report will be issued by that office. We worked closely with GAO to ensure that we did not duplicate its efforts. Therefore, we limited our review to the control objectives and techniques identified in exhibit A of this report.

Our qualified opinion on OCIO/NITC's general control structure is based on operations from October 1, 2002, through September 30, 2003. While we believe that Finding Nos. 1, 2 and 3 are material, OCIO/NITC has taken significant actions throughout the year to mitigate the weaknesses we identified. Therefore, we do not recommend that they be included as material weaknesses in its Federal Managers' Financial Integrity Act Report.

The objectives of our examination were to perform testing necessary to express an opinion about (1) whether the control objectives and techniques identified in this exhibit present fairly, in all material respects, the aspects of the OCIO/NITC's policies and procedures in place during fiscal year 2003; (2) whether the control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily; and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

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

Our testing of OCIO/NITC's control structure policies and procedures was restricted to the control objectives and the related policies and procedures listed in the matrices in this exhibit. Our testing was not intended to apply to any other procedures described in OCIO/NITC's Service Center Description and Internal Controls Framework, that were not included in the aforementioned matrices or to procedures that may be in effect at user organizations.

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

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
1. Define and communicate OCIO/NITC organizational structure, policies, and procedures.	The OCIO/NITC relies on Department policy, in most matters, and provides hard copy and electronic access.	We reviewed policies and procedures to ensure that departmental policies had been taken into account.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.
	When Department policy does not provide adequate guidance on administrative issues, OCIO/NITC issues internal Administrative Directives, which define administrative policies and procedures.	We reviewed internal Administrative Directives and policies and procedures to ensure that they are revised, updated, and changed when necessary.	The control structure policies and procedures were suitably designed to achieve the control objective specified, but were not operating effectively. We noted instances where terminated employees' system accesses were not being timely removed. (See Finding No. 2.)
	Policy manuals, procedure manuals, and Administrative Directives are made available in electronic and hard copy form, and are used by personnel.	We reviewed policy manuals, procedure manuals, and administrative directives to ensure they were available in electronic form.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.
	The OCIO/NITC organizational structure and the responsibilities of the OCIO/NITC divisions are well documented and understood.	We reviewed the organizational structure to ensure that they were documented and appropriate. We reviewed OCIO/NITC's Security Program Plan to ensure the plan met OMB Circular A-130 requirements. We reviewed OCIO/NITC's listing of agency security officers.	The control structure policies and procedures were not suitably designed to achieve the control objective specified because OCIO/NITC staff responsible for removing user IDs did not consistently receive the forms used to process the removal of user IDs when staffs were terminated. See (Finding No. 2.)
	Division responsibilities, services, and procedures are documented.	We reviewed the organization structure, responsibilities of the OCIO/NITC divisions, Administrative Directives, and procedural documents used by division staff to ensure that they were documented and appropriate.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed into operation. However, the controls were not operating effectively. OCIO/NITC was developing Trusted Facility Manuals, revising its special access privilege policy, and not following the inactive account policy. (See Finding No. 2.)

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
	Personnel policies encourage training and development to qualify personnel for their functional responsibilities.	We reviewed personnel policies to ensure they encourage training and development. We reviewed training documentation.	The control structure policies and procedures were suitably designed to achieve the control objective and had been placed into operation, but were not operating effectively. We noted that OCIO/NITC had not ensured that all employees received training on the implementation of contingency plan responsibilities, and maintained evidence that all staff received security awareness training. (See Finding No. 1.)
2. Segregate duties between the specialized staff as much as practical.	The responsibilities of the OCIO/NITC staff and of the users of OCIO/NITC services are clearly differentiated.	We determined if all customers had MOUs or service level agreements in place.	The control structure policies and procedures were not suitably designed to achieve the control objective specified and controls were not operating effectively. OCIO/NITC needed to revise MOUs for their mainframe customers. OCIO/NITC expects to issue the revised MOUs to agencies after October 1, 2003. (See General Comments.)
	Separation of duty is enforced through access rules within the security software whenever practical and consistent with user requirements.	We reviewed access to critical operating system software data sets and compared settings to best practice standards. We reviewed user IDs with special access privileges.	The control structure policies and procedures were suitably designed to achieve the control objective specified. However, controls were not operating effectively. We noted instances where OCIO/NITC does not maintain standard documentation supporting system security settings. OCIO/NITC had not completed implementation of special access privilege guidance. (See Finding No. 2.)
3. Apply appropriate controls to the system development lifecycle.	The modification or installation of systems software requires the approval of OCIO/NITC management.	We reviewed policies and procedures to ensure that departmental policies were considered. We reviewed internal Administrative Directives and policies and procedures to ensure that they are revised, updated, and changed when necessary and were properly implemented.	The control structure policies and procedures were suitably designed to achieve the control objective specified. However, change management controls were not operating effectively. (See Finding No. 3.)

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
5. Provide reasonable assurance that all software changes are appropriately reviewed and authorized.	There is thorough supervision and review of all changes.	We reviewed software change policies and INFOMAN records to determine if software changes were documented and approved. We interviewed officials to obtain software change control reengineering status.	The control structure policies and procedures were not suitably designed to achieve the control objective specified. We determined OCIO/NITC is reengineering its change control process. We determined that system change approvals were not always documented. (See Finding No. 3.)
6. Conduct the planning activities needed to provide reasonable assurance that the OCIO/NITC will meet functional and control requirements.	Document current OCIO/NITC controls, and identify required new controls.	We reviewed OCIO/NITC's internal controls framework and evaluated various plans such as OCIO/NITC's Security Plans, contingency plans, and system accreditations.	The control structure policies and procedures were suitably designed to achieve the control objective specified, but had not been effectively placed into operation. OCIO/NITC has not complied with OMB Circular A-130 requirements. (See Finding No. 1.)
7. Restrict access to the operating system, associated software and documentation to authorized personnel.	Automated and manual procedures are used to track all significant mainframe operating system and software modifications, as well as other significant changes to other OCIO/NITC infrastructure components.	We reviewed system logging policies and procedures. We reviewed system logs, change management policies and procedures, and recently completed INFOMAN records.	The control structure policies and procedures were suitably designed to achieve the control objective; however, OCIO/NITC does not have written policies and procedures outlining what system logs to review and what actions will be taken for different security violations. OCIO/NITC also has not completed implementation of its reengineered change control process. (See Finding Nos. 2 and 3.)
	System privileges that bypass normal system controls are allowed only when necessary and requested by the appropriate supervisor in writing, and are logged and/or closely monitored.	We reviewed policies and procedures for special system privileges. We reviewed user IDs with these accesses. We interviewed OCIO/NITC security staff to determine how these user IDs are monitored. We determined if forms were completed for user IDs with high-level system privileges.	The control structure policies and procedures were suitably designed to achieve the control objective specified; however, the controls had not been placed into operation. We found that Security Staff were not adequately documenting their review of system security logs and security violations. We found that special access privilege policies and procedures had recently been updated but not yet implemented. We determined that not all user IDs with special access privileges had approval forms on file. (See Finding No. 2.)
8. Provide reasonable assurance that operations staff operates automated equipment in accordance with the management criteria.	Access to resources and data files is limited by security software to those required to do their work.	We reviewed critical data sets to determine if user IDs accessing these data sets were being logged. We reviewed policies and procedures to document security violations.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
9. Provide reasonable assurance that equipment is used by authorized persons following prescribed procedures.	Access to the operations area and office is physically restricted through the use of a key badge system. The door system uses a proximity reader biometric fingerprint to prevent unauthorized access. Access to the operations area is further restricted through the use of a double door access point.	We reviewed and observed access to critical resources and the use of guards, key badges, and biometric devices utilized to control access to restricted areas.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.
	Policies and procedures ensure that access to the Operations area is highly restricted. This includes mid-range server activities.	We reviewed related policies and procedures for access to controlled areas.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.
	Guards protect OCIO/NITC operations and office area 24 hours per day, 7 days a week.	We reviewed policies and procedures for security and observed guard monitoring area at various times of day.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.
	Continuously monitors OCIO/NITC access control points and operational floor space through the use of differing video surveillance monitoring angles and alarm systems.	We reviewed policies and procedures for OCIO/NITC security staff monitoring of surveillance cameras. We observed operational area to determine if it was monitored continuously.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.
10. USDA: Provide reasonable assurance that only approved users have access to OCIO/NITC and that they are accessing and processing only within approved boundaries.	OCIO/NITC, on a monthly basis, suspends or deletes logon IDs that have been inactive for designated periods of time.	We reviewed related policies and procedures and security software access controls over inactive user IDs.	The control structure policies and procedures were suitably designed to achieve the control objective specified; however, the controls had not been effectively placed into operation. We identified two separated employees that still had user IDs and OCIO/NITC policies and procedures were not being followed. (See Finding No. 2.)
	CA-ACF2 is used to control user Logon-IDs and passwords.	We reviewed user IDs that have not been used for an extended period of time and password settings to ensure adequate controls have been implemented over user IDs and passwords.	The control structure policies and procedures were designed to achieve the control objective specified; however, agencies were not complying with OCIO/NITC's policies and procedures to obtain waivers for using passwords set to never expire. (See Finding No. 2.)

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
	The OCIO/NITC creates only those logon identifiers requested by an Agency Security Officer.	We reviewed a listing of user IDs beginning with "K" to ensure user IDs were current. We compared these user IDs with OCIO/NITC's listing of Agency Security Officers and other documentation to determine if only valid user IDs were available on the system.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, but were not operating effectively. We noted instances where user IDs were no longer needed. (See Finding No. 2.)
11. Data files are adequately protected from unauthorized modification or destruction.	Key documentation is also stored off-site at a secure location.	We reviewed policies and procedures for off-site storage and confirmed that copies were maintained at an off-site facility. We reviewed contingency plans.	The control structure policies and procedures were suitably designed to achieve the control objective specified, however, OCIO/NITC recognized the need to create contingency plans for OCIO/NITC-owned general support systems, and telecommunications. (See Finding No. 1.)
12. Assess the vulnerability of the OCIO/NITC to physical and other disasters, and put in place procedures for maintaining essential operations after such an occurrence.	Risk assessments are performed on OCIO/NITC systems.	We reviewed risk assessment policies and determined if the OCIO/NITC security and contingency plans are documented, approved and current, and if the plans cover the topics prescribed by OMB Circular A-130.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed into operations and were operating effectively.
	A Contingency Plan for Alternate Site Operations is in place. A plan for mid-range server environments has not been documented. It will be in the next issuance of the contingency plan.	We reviewed contingency plans and determined if the contingency plan is periodically reassessed and if appropriate, revised to reflect changes in hardware, software, and personnel.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed into operation, but were not operating effectively. We determined that not all disaster recovery team members and alternates have been trained on their responsibilities should a disaster occur. Furthermore, OCIO/NITC recognized the need to create contingency plans for OCIO/NITC-owned general support systems. (See Finding No. 1.)
	OCIO/NITC is designed to survive many physical disasters with minimal damage.	We determined if physical controls (e.g., smoke detectors, fire extinguishers, and sprinkler systems) have been implemented and are periodically checked. We determined if an uninterruptible power supply or backup generator has been provided so that power will be adequate for orderly shutdown.	The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
	The USDA Internet Access network provides the physical medium for the OCIO/NITC wide area network. This network, which uses FTS 2001 circuits, has diverse routes, and is self-healing. Local loop diversity is currently being implemented.	We determined if communication software logical controls have been implemented. We reviewed pertinent policies and procedures. We interviewed telecommunications management staff.	The control structure policies and procedures were suitably designed to achieve the control objective specified. However, unencrypted access from the Internet will still be available until January 1, 2004. (See Finding No. 2.)
13. Evaluate and substantiate ADP controls on a regular basis.	Vulnerabilities are assessed on a regular basis through risk assessments, vulnerability assessments, and security testing.	We determined if OCIO/NITC periodically identifies significant threats to the well-being of sensitive and critical resources and identifies related risks. We interviewed OCIO/NITC officials to determine if all network devices were periodically scanned.	The control structure policies and procedures were suitably designed to achieve the control objective specified, but had not been effectively placed into operation. OCIO/NITC has not completed action to secure Internet access. Unencrypted access from the Internet will still be available until January 1, 2004. (See Finding No. 2.)
	Develop and periodically test a plan that will allow OCIO/NITC to recover operating systems and software at the Alternate Operations Site within 72 hours after disaster declaration. A disaster recovery plan has been developed and tested to restore the Tivoli Storage Manager Server, which is a component of the mid-range disaster recovery strategy. An AIX recovery strategy has been developed and tested.	We reviewed policies on testing, test results, final test reports, and documentation supporting contingency plan adjustments to determine if the current plan has been tested under conditions that simulate a disaster, test results are analyzed and contingency plans are adjusted accordingly.	The control structure policies and procedures were suitably designed to achieve the control objective specified and had been placed into operation, but were not operating effectively. We determined that not all disaster recovery team members and alternates have been trained on their responsibilities should a disaster occur. We determined that not all general support systems had contingency plans. (See Finding No. 1.)
14. Provide an appropriate level of personnel security.	Ensure that staff and contractors have the appropriate level background investigation…Due to the nature of the duties performed by OCIO/NITC the ability to bypass controls is often necessary. Accordingly, OCIO/NITC management made the determination to upgrade the level of security clearances for OCIO/NITC and contractor personnel.	We reviewed the status of the background investigations and training records for OCIO/NITC personnel. We reviewed the status of nondisclosure statements.	The control structure policies and procedures were suitably designed to achieve the control objective specified, but not been effectively placed into operation. We identified staff that had not received security awareness training and determined that not all disaster recovery team members and alternates have been trained on their responsibilities should a disaster occur. (See Finding No. 1.)

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
	Ensure that terminated employees are disallowed access to OCIO/NITC and OCIO/NITC resources.	We compared a system-generated list of users to a list of active employees to determine if user IDs and passwords for terminated employees exist. We compared the user listings to contract personnel listings. We examined documents showing compliance with policies for a selection of terminated/transferred employees. We reviewed policies and procedures.	The control structure policies and procedures were not suitably designed to achieve the control objective specified. We identified that OCIO/NITC has weak controls over timely removal of unneeded user accounts. We identified terminated employees who still had user IDs and OCIO/NITC did not have procedures in place to reconcile user IDs to employee lists. (See Finding No. 2.)
	Ensure that employees and contractors receive security awareness training.	We reviewed policies and procedures for security awareness training and reviewed formal records and listing of personnel who attended training.	The control structure policies and procedures were suitably designed to achieve the control objective specified, but were not operating effectively. We identified that OCIO/NITC had not maintained documentation that all staff received security awareness training. (See Finding No. 1.)