



U.S. Department of Agriculture



Office of Inspector General
Financial & IT Operations

Audit Report

National Information Technology Center General Controls Review – Fiscal Year 2004

Report No. 88501-1-FM
September 2004



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250



DATE: SEP 22 2004

REPLY TO

ATTN OF: 88501-1-FM

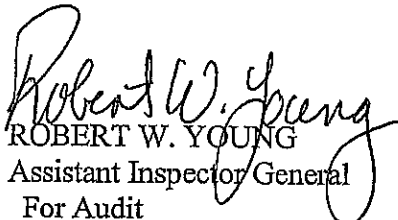
SUBJECT: National Information Technology Center General Controls
Review-Fiscal Year 2004

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 as of August 31, 2004. 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 30 days describing the corrective action 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 our staff during the audit.


ROBERT W. YOUNG
Assistant Inspector General
For Audit

Executive Summary

National Information Technology Center General Controls Review - Fiscal Year 2004

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 August 31, 2004. 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.

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 the period October 1, 2003 through August 31, 2004, (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. In 2004, the U.S. Government Accountability Office (GAO) issued its report on internal controls testing within the Department.¹ We conducted limited testing to determine the status of corrective action on issues identified in that report.

Our audit disclosed that, except for the matters referred to below; the control objectives and techniques identified in exhibit A present fairly, in all material respects, the relevant aspects of 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.

While significant improvements have been made, OCIO/NITC was still not compliant with the requirements of Office of Management and Budget (OMB) Circular A-130 and other Federal security guidance. Specifically, OCIO/NITC had not (1) finalized contingency planning, (2) conducted risk assessments consistent with Federal requirements, (3) prepared security plans for each of its general support systems, (4) completed system certifications

¹ GAO-04-154, "Further Efforts Needed to Address Serious Weaknesses at USDA," dated January 2004.

and accreditations for each of its general support systems, and (5) maintained a complete inventory of systems in its midrange environment. OCIO/NITC plans to have many of these areas corrected by fiscal year end as part of its certification and accreditation process, while others have been identified 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 involves major efforts and requires time and resources to comply thoroughly. However, until these controls and documents are in place, OCIO/NITC cannot be assured of the confidentiality, integrity, and availability of its computer resources.

OCIO/NITC had not ensured that all midrange server security settings were configured in accordance with departmental and NIST guidelines. Further, OCIO/NITC needed to improve management over the routers and firewalls in its general support system. This occurred because OCIO/NITC had not established a policy or implemented controls to require midrange systems and general support systems to follow OCIO or NIST configuration guidance; and OCIO/NITC security staff have not played a significant role in establishing or monitoring security over midrange and general support systems. As a result, data residing on these servers in the midrange environment could be compromised.

OCIO/NITC has made significant improvements over logical access controls. 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) waivers were obtained for user accounts with non-expiring passwords, (2) policies and procedures outlining monitoring of security logs were implemented, (3) global system settings were fully documented, and (4) controls from the internet were properly secured. While OCIO/NITC has made significant progress to address these issues, 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.

OCIO/NITC has improved its system change management process. However, we continued to find that approval, testing, and implementation documentation was not always maintained. While this condition was more prevalent in OCIO/NITC's midrange system environment, improvements over changes to its mainframe environment are still needed. Despite its own policies to document approval, testing, and implementation, OCIO/NITC had not established controls to ensure that the procedures were being properly carried out. 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.

We believe that the findings in this report, taken as a whole, constitute a material weakness in the general control structure and should be reported in OCIO/NITC's Federal Manager's Financial Information 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 recommendations for OCIO/NITC to:

- Establish a plan of action with specific milestone dates toward updating its contingency plans to meet OMB requirements, and completing business resumption plans and business impact analyses for all components of OCIO/NITC's network and midrange environments;
- develop a strategic plan with specific milestone dates for establishing policies and procedures to address the midrange security weaknesses we identified, and increased security involvement in the midrange environment;
- develop a control to ensure that router and firewall configurations are properly maintained, documented, and that backup configurations are stored off-site;
- establish a plan with milestone dates on when it plans to finalize its documentation of global system settings and have those settings documented in its security plan; and
- establish controls to ensure that its change management process includes adequate documentation of approval, testing and implementation.

Agency Response

OCIO generally agreed with the findings and recommendations in this report and is in the process of developing corrective action plans and/or finalizing corrective actions.

Abbreviations Used in This Report

BCP	Business Continuity Plan
BIA	Business Impact Analysis
BR	Business Resumption
COOP	Continuity of Operations Plan
CS	Cyber Security (A division of the OCIO)
DM	Departmental Manual
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
GAO	Government Accountability Office
GSS	General Support System
ICS	Incident Command Structure
ID	Identification (i.e., user accounts or user identification)
ISS	Infrastructure Support Services
IT	Information Technology
MOU	Memorandum 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	U.S. Department of Agriculture

Table of Contents

Executive Summary	i
Abbreviations Used in This Report	iv
Report of the Office of Inspector General	1
Findings and Recommendations	3
Section 1. Security Program Management and Compliance	3
Finding 1 Further Actions are Needed toward Achieving Compliance with Federal Regulations.....	3
Recommendation No. 1.....	6
Recommendation No. 2.....	6
Finding 2 Stronger Controls Over Management and Configuration of Midrange and General Support Systems are Needed	7
Recommendation No. 3.....	10
Recommendation No. 4.....	10
Recommendation No. 5.....	10
Recommendation No. 6.....	10
Section 2. Mainframe Access Controls	11
Finding 3 Mainframe Access Controls Have Significantly Improved but Additional Actions are Needed	11
Recommendation No. 7.....	13
Recommendation No. 8.....	13
Section 3. System Change Controls	14
Finding 4 Change Control Improvements Need to be Finalized and Implemented	14
Recommendation No. 9.....	15
Exhibit A – Office of Inspector General, Review of Selected Controls	16



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 the period October 1, 2003 through August 31, 2004, (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; ensure adequate security controls are in place over its midrange environment; and ensure that it is in compliance with existing Federal security guidelines.

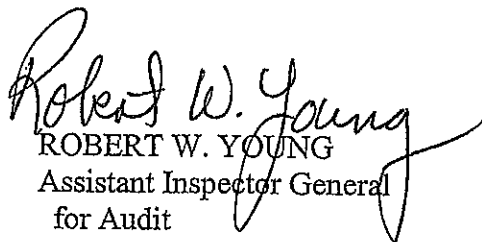
In our opinion, except for the matters referenced to in the previous paragraph, the control objectives and techniques identified in exhibit A of this report present fairly, in all material respects, the relevant aspects of OCIO/NITC. Also, in our opinion, except for the deficiencies referred to in the 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, 2003 through August 31, 2004. 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 performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The control objectives and techniques at OCIO/NITC are as of August 31, 2004, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 2003, through August 31, 2004. 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.


ROBERT W. YOUNG
Assistant Inspector General
for Audit

August 31, 2004

Findings and Recommendations

Section 1. Security Program Management and Compliance

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.

Finding 1

Further Actions are Needed toward Achieving Compliance with Federal Regulations

While significant improvements have been made, OCIO/NITC was still not compliant with the requirements of Office of Management and Budget (OMB) Circular A-130 and other Federal security guidance. Specifically, OCIO/NITC had not (1) finalized contingency planning, (2) conducted risk assessments consistent with Federal requirements, (3) prepared security plans for each of its general support systems, (4) completed system certifications and accreditations for each of its general support systems, and (5) maintained a complete inventory of systems in its midrange environment. OCIO/NITC plans to have many of these areas corrected by fiscal year end as part of its certification and accreditation process, while others have been identified 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 comply thoroughly. 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 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 also requires agencies to maintain an inventory of the agency's major information systems.

Contingency/Disaster Recovery Plans (DRP)

Based in part on the OIG's prior recommendations, OCIO/NITC completed disaster recovery plans for its general support systems. Our review of those plans disclosed that additional documentation is needed to meet Federal and departmental guidelines.

OMB Circular A-130, Appendix III, requires the development and maintenance of two types of contingency plans: (1) a continuity of support or contingency plan that addresses the recovery of major applications and support systems in the event of minor disruption, and (2) a disaster recovery plan, (DRP) which as its name implies, applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Further, NIST² emphasizes the Business Impact Analysis (BIA) as a key step in the contingency planning process. The BIA enables the organization to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities for both short-term and long-term contingencies. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan, and Business Resumption Plan.

OCIO/NITC has a COOP plan in place to address business continuity at the highest level of the organization in a widespread emergency affecting the metropolitan area. OCIO/NITC does not have continuity of support plans in place to 1) address short-term versus long-term contingencies of a localized nature and 2) address all of the various components of OCIO/NITC's operations and how those components will be recovered in the event of a limited contingency, such as a service interruption, as required by OMB Circular A-130. Further, we found that OCIO/NITC had not performed a BIA before preparing its disaster recovery plan for its general support system. Finally, our review disclosed that the DRP for the Infrastructure Support System, Sun General Support System (GSS), and Windows GSS did not outline procedures for restoring operability of the target systems at an alternate site after an emergency. Instead, the plans focus on reloading the operating system in the event of system failure. Those plans do not address steps to take if the OCIO/NITC facility is no longer accessible because of an emergency.

Without effective, operable plans for those systems, OCIO/NITC cannot be assured that it will be able to provide efficient automated processing services to support its customers.

² SP 800-34, "Contingency Planning Guide for IT Systems," dated June 2002.

Risk Assessments

As part of the certification and accreditation efforts of OCIO/NITC, a contractor was hired to perform risk assessments of OCIO/NITC's GSS and major applications. Risk assessments had been performed on four midrange servers, the telecom components, the mainframe, and the Infrastructure Support Services (ISS). Despite these efforts, we found that risk assessments were performed without a BIA being performed first. According to CS-031, Risk Assessment Methodology, the first step in characterizing an IT system is to define the business case for the system. The business case defines the system's function and importance to the program and to USDA's overall mission. CS-031 also states that NIST SP 800-34 requires a BIA, which is also roughly equivalent to a business case. This BIA will also aid in the identification of the system's data needed for the next step of the process. According to NIST SP 800-34, the BIA helps to identify and prioritize critical IT systems and components. The NIST guidance states the BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, characterize the consequences of a disruption to the system components. Without the BIA being performed first, NITC cannot be assured that all system components and critical services provided by them were adequately identified, prioritized, and included in the risk assessment.

Security Plans

During our prior audit,³ we reported that OCIO/NITC had not completed security plans for its GSS, but had plans to complete them by September 30, 2003. Progress had been made during the year to finalize many of its security plans; however, we found that security plans for its telecommunications network including routers, firewalls, intrusion detection system, and mainframe access software had not been completed. Until a security plan is completed for this GSS, OCIO/NITC cannot be assured that it has adequately addressed its security needs and that its security policies and practices have become an integral part of its operations. OCIO/NITC officials informed us that security plans have been prepared as part of its certification and accreditation process, which will be completed by September 30, 2004. Because OCIO/NITC has a corrective action plan in place to complete security plans, we will make no recommendation concerning this issue.

System Certification and Accreditation

OCIO/NITC has not completed system certifications and accreditations for its GSS. During fieldwork OCIO/NITC was in the process of completing these certifications in accordance with the Department's directives. NITC officials

³ Audit Report No. 88099-05-FM, "National Information Technology Center General Controls Review - Fiscal Year 2003," dated October 2003.

informed us that they intend to have their GSS certified and accredited by September 2004; therefore, we will make no recommendation concerning this issue.

Inventory

Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, dated December 17, 2003 requires all federal departments and agencies to identify, prioritize, and protect their internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies are to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

During our review, we found that OCIO/NITC did not have an accurate inventory of its midrange environment that included such vital information as system name, owner/manager of the system, operating platform and IP address.

According to NIST,⁴ when assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization boundaries, and provides information such as hardware, software, system connectivity, and responsible division or support personnel that is essential to defining the risk.

Without an accurate inventory, OCIO/NITC cannot be assured that all systems have been identified, risks on those systems have been assessed, and security controls have been established over those systems.

Recommendation No. 1

OCIO/NITC should establish a plan of action with specific milestone dates toward updating its contingency plans to meet OMB requirements, and completing business resumption plans and business impact analyses for all components of OCIO/NITC's network and midrange environments.

Recommendation No. 2

OCIO/NITC should implement controls to ensure that an inventory of OCIO/NITC's midrange environment is maintained, including essential information such as system name, owner/manager of the system, operating platform and IP address.

⁴ SP800-30, Risk Management Guide for Information Technology Systems

Finding 2

Stronger Controls Over Management and Configuration of Midrange and General Support Systems are Needed

OCIO/NITC had not ensured that all midrange server security settings were configured in accordance with departmental and NIST guidelines. Further, OCIO/NITC needed to improve management over the routers and firewalls in its GSS. This occurred because OCIO/NITC had not (1) established a policy or implemented controls to require midrange systems and GSS to follow OCIO or NIST configuration guidance, (2) finalized policies or standard operating procedures for the midrange environment, and (3) ensured that security staff played a significant role in establishing or monitoring security over midrange and GSS. Further, OCIO/NITC assigned control over administration and security to the systems administrators of the midrange environment. As a result, data residing on these servers, as well as other servers in the midrange environment were at risk of compromise.

Configuration management is essential in ensuring that system settings are documented and configured in the best interest of performance and security while ensuring that changes to systems are approved and do not inadvertently affect the system security. Departmental⁵ and NIST⁶ guidance require that agencies have formal configuration management processes in place. Further, the Department and NIST have issued configuration checklists that should be used by agencies to ensure proper security configurations are used. Finally, OCIO/NITC has issued its own policies⁷ for identifying unused user accounts on all its systems, and for limiting access to only those systems and data necessary to perform their job duties.

Midrange Configuration Management

Our evaluation of OCIO/NITC's midrange⁸ environment included detailed security reviews of 2 servers owned and managed by OCIO/NITC. Our review disclosed that system administrators had not configured midrange server security in accordance with departmental and NIST guidance. Specifically, we found:

⁵ Cyber Security guidance CS-009, "Interim Guidance on USDA Configuration Management," dated October 15, 2001.

⁶ NIST SP 800-12, "An Introduction to Computer Security," dated October 1995; and SP 800-43, "Guidance for Security Windows 2000," dated November 2002.

⁷ OCIO/NITC Security Directive SD 1-5, "Least Privilege Policy," dated March 26, 2003; Security Directive SD 5-1, "Inactive Accounts," dated March 12, 2003.

⁸ Midrange is defined as a server system running a multi-user operating system with less computing power than a mainframe system, but more computing power than an end-user system. Typically, these include Windows server-class operating systems, Unix servers from various vendors, and IBM AS400 servers.

- Password security settings, such as password expiration and length, and access permissions did not always meet departmental and NIST guidelines;
- system users included generic accounts, guest accounts, and other accounts unidentifiable to employee lists;
- administrator and user rights did not always meet departmental and NIST guidelines;
- access Authorization did not exist for OCIO/NITC staff on midrange systems, and no periodic reconciliation was performed of user IDs on the midrange systems;
- excessive access rights were granted to directories and files;
- windows registry keys were not always configured in accordance to departmental and NIST guidelines;
- network services running were not configured to departmental and NIST guidelines; and
- current vendor-supplied patches had not been installed on the systems.

OCIO/NITC officials acknowledged the weaknesses on its servers under their management control and began implementing corrective actions.

Since security vulnerabilities on one midrange server have the potential to affect other midrange servers in its environment, we selected four additional servers to review. Our review included 2 servers owned by agencies, but partially managed by OCIO/NITC, and 2 servers owned and managed by the agencies. We found similar issues on these 4 servers and communicated those weaknesses to the appropriate agency managers, who began to take corrective actions.

OIG recognizes that OCIO/NITC exercises different levels of management responsibility over its midrange environment. For some systems, OCIO/NITC simply maintains physical security at its facilities, while others are managed entirely by OCIO/NITC staff. OIG also recognizes that it is ultimately the responsibility of the owner agency to ensure its systems are properly secure and in compliance with departmental and Federal security guidelines. However, OCIO/NITC needs to work with its customer agencies to ensure a balance between its role as a service provider and its responsibility to all of its customers to provide a secure operating environment and network. OCIO/NITC had issued security directive SD 1-3, "Requirements for Approval of System Operation," dated March 2003, which requires the owner agencies to provide written approval to operate (also called accreditation), for every system in OCIO/NITC's environment. The Department initiated its certification and accreditation effort during this fiscal year to address a long-standing material weakness in that the Department and its agencies had not been accrediting its systems in accordance with OMB

Circular A-130. Most agencies will not have authorizations to operate until the end of the fiscal year; therefore, OCIO/NITC has been unable to enforce its policy. OCIO/NITC needs to ensure that it obtains these authorizations to operate as they become available for current systems, and that these authorizations are obtained for future systems that enter its environment.

General Support System Configuration

Routers and firewalls are significant components of OCIO/NITC's GSS. These components ensure that only authorized access is obtained from the departmental intranet and global Internet. OCIO/NITC has maintained its routers and firewalls adequately; however, improvements could be made to strengthen the configuration of these devices. Specifically, we found that:

- Changes to routers did not follow OCIO/NITC's change control process (see Finding No. 4);
- routers were not configured to completely log all successful and unsuccessful access attempts;
- one router had an excessive number of virtual terminals configured;
- firewall rules implemented before OCIO/NITC established its configuration management policy were not thoroughly documented;
- access authorization to firewalls was not documented;
- OCIO/NITC had not obtained waivers, in accordance with Department policy,⁹ for the use of certain non-secure protocols through its firewalls; and
- backup of firewall configurations were not being maintained off-site.

OCIO/NITC personnel responsible for configuration of the routers and firewalls concurred with our observations and have begun to take corrective actions.

Midrange Monitoring and Security Oversight

OCIO/NITC does not have policies and procedures in place to ensure that the security staff monitors midrange systems. As noted above, we observed midrange systems that had not been configured to log security events. In cases where logging was activated, system administrators, not security staff, monitored the logs. For proper segregation of duties and effective security management, OCIO/NITC needs to establish policies and controls to ensure that midrange security logging is enabled and that security staff monitor those logs.

⁹ OCIO Cyber Security CS-012, "Cyber Security Guidance Regarding Gateway and Firewall Technical Security Standards," dated January 22, 2002.

Vulnerability Scanning

OCIO/NITC had not been conducting thorough vulnerability scanning on all its routers. Further, while OCIO/NITC had conducted vulnerability scans on its midrange system networks, OCIO/NITC officials only recently implemented a control to notify agency Chief Information Officers when vulnerabilities were not timely corrected. In fiscal year 2001, the Department purchased a license to a commercial off-the-shelf software package that identified vulnerabilities in operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP). The Department implemented a policy that required the use of this software to scan all systems at least monthly.¹⁰ This policy also requires all agencies to maintain a complete inventory of all its networks and systems. Based in part on our audits, OCIO/NITC began scanning all midrange systems for its customers; however our current review disclosed that OCIO/NITC had not been scanning its routers, which can also be subject to TCP/IP vulnerabilities.

Recommendation No. 3

OCIO/NITC should develop a strategic plan with specific milestone dates for establishing policies and procedures to address the midrange security weaknesses we identified, and increased security involvement in the midrange environment.

Recommendation No. 4

OCIO/NITC should develop a control to ensure that it obtains authorization to operate from system owner agencies for all systems in its operating environment.

Recommendation No. 5

OCIO/NITC should develop a control to ensure that router and firewall configurations are properly maintained, documented, and that backup configurations are stored off-site.

Recommendation No. 6

OCIO/NITC should develop a control to ensure it conducts thorough vulnerability scanning of its routers.

¹⁰ OCIO Cyber Security, CS-007, "Security Vulnerability Scan Procedures," issued September 2001.

Section 2. Mainframe Access Controls

Finding 3 Mainframe Access Controls Have Significantly Improved but Additional Actions are Needed

OCIO/NITC has made significant improvements over logical access controls in its mainframe environment; however, further actions are needed to ensure the confidentiality and integrity of its IT resources. Specifically, OCIO/NITC had not completed implementation of procedures to ensure (1) waivers were obtained for user accounts with non-expiring passwords, (2) policies and procedures outlining monitoring of security logs were implemented, (3) global system settings were fully documented, and (4) access from the Internet were properly secured. While OCIO/NITC has made significant progress 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.

OMB¹¹ 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 NIST¹² stress the need for agencies to implement the “least privilege” concept, granting users only those accesses required to perform their duties. Departmental Manual (DM)¹³ requires security staff to remove employee user identifications (ID) and passwords when the employee is no longer with the agency.

User Accounts

We continue to find an excessive number of user IDs that have non-expiring passwords. As reported last year, one agency is responsible for a majority of these user IDs. As of the end of our fieldwork, OCIO/NITC had not obtained the waiver from agency management documenting why these IDs needed passwords that did not expire. OCIO/NITC has begun to obtain waivers for newly created IDs with non-expiring passwords; however our test sample of 14 newly created IDs found that OCIO/NITC did not have waivers for 3 of

¹¹ OMB Circular A-130, Appendix III, Section A, November 30, 2000.

¹² NIST Special Publication 800-18, “Guide for Developing Security Plans for Information Technology Systems,” dated December 1998.

¹³ DM 3140-1.6, part 6 of 8, Section 6c, “Management ADP Security Manual,” July 19, 1984.

them. OCIO/NITC needs to implement an effective process for obtaining and maintaining these waivers.

Security Software Global System Settings

Based on our prior audit recommendations, OCIO/NITC has begun, but has not completed, its review and documentation of its security software's global system 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.

Monitoring Access

OCIO/NITC is still in the process of establishing 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. In part due to a recommendation made in last year's report, 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. Because OCIO/NITC is in the process of completing corrective action, we will not make additional recommendations on this issue.

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. OMB¹⁴ 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 3140-1.3¹⁵ requires maintaining access logs sufficient to permit reconstruction of events in case of unauthorized data or program access or use. Security/access control software should be used to

¹⁴ OMB Circular A-130, Appendix III, Section B (a)(2)(c), November 30, 2000.

¹⁵ DM 3140-1.3, "Management ADP Security Manual," Part 3 of 8, Section 16, July 19, 1984.

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 the audit trail information 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 alerted 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. Because OCIO/NITC is in the process of addressing our prior recommendation, we make no further recommendation in this report.

Mainframe Access From the Internet

OCIO/NITC is still in the process of working with its customers to encrypt all access to its mainframe, a process that began in September 2003 and was originally scheduled to be completed by January 2004. According to OCIO/NITC officials, this was the final step toward securing access to OCIO/NITC network resources from the Internet. OCIO/NITC customers need to implement changes on their networks before this process can be finalized. Until this process is complete, we consider this to be a material internal control weakness that OCIO/NITC needs to address. Because OCIO/NITC is in the process of addressing our prior recommendation, we are making no further recommendations on this issue in this report.

Recommendation No. 7

OCIO/NITC should develop controls to ensure that waivers are obtained and maintained for all accounts that have non-expiring passwords.

Recommendation No. 8

OCIO/NITC should establish a plan with milestone dates on when it plans to finalize its documentation of global system settings and have those settings documented in its security plan.

Finding 4 Change Control Improvements Need to be Finalized and Implemented

OCIO/NITC continues to improve its system change management process. However, we continued to find that approval, testing, and implementation documentation was not always maintained. While this condition was more prevalent in OCIO/NITC's midrange system environment, improvements over changes to its mainframe environment are still needed. Despite its own policies to document approval, testing, and implementation, OCIO/NITC had not documented what changes had been approved, or established controls to ensure that change control procedures were being properly carried out. 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 has formalized change control policies¹⁶ in place that govern the request, approval, testing, and implementation phases of the change control process. According to NIST,¹⁷ 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 two prior years' audits, we found that new system software versions or modifications to existing software were not properly authorized, tested, or logged. While most of the discrepancies in this year's audit were found in the OCIO/NITC's midrange system environment, we noted instances where changes were made in the mainframe environment that had not been properly approved. Below are a few of the discrepancies we identified in the mainframe and midrange platforms:

¹⁶ OCIO/NITC "Change Management Handbook," dated August 19, 2003.

¹⁷ NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004.

Mainframe

- Changes recorded in OCIO/NITC's management information system had been implemented without evidence that the change was approved.
- While OCIO/NITC officials informed us that testing of approved changes had been done before implementing them into production, OCIO/NITC had not maintained documentation showing the testing had been completed.

Midrange

- OCIO/NITC personnel were not following formalized change control procedures for OCIO/NITC managed midrange servers.
- OCIO/NITC had not always documented contact with agency-owners when making changes to systems managed by OCIO/NITC.
- Emergency changes were not always authorized or approved as required by OCIO/NITC policy.
- Documentation that testing of changes occurred was not always maintained.

During last year's audit, 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. OCIO/NITC recently conducted its own internal review of the accuracy of its change control database to ensure that it accurately reflected approved and implemented changes. Further, OCIO/NITC modified its database by adding an automated control that would not allow a change record to be closed without first being coded as approved. Despite these actions, however, OCIO/NITC needs to make a concerted effort to continue making improvements to implement sound change control practices.

Recommendation No. 9

OCIO/NITC needs to establish controls to ensure its change management process includes adequate documentation of approval, testing and implementation.

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

Exhibit A – Page 1 of 10

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 for the period October 1, 2003 through August 31, 2004, (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.

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>1. Define and communicate OCIO/NITC organizational structure, policies, and procedures.</p>	<p>a. The OCIO/NITC relies on Department policy, in most matters, and provides hard copy and electronic access.</p> <p>b. When Department policy does not provide adequate guidance on administrative issues, OCIO/NITC issues internal Administrative Directives, which define administrative policies and procedures.</p> <p>c. Policy manuals, procedure manuals, and Administrative Directives are made available in electronic and hard copy form, and are used by personnel.</p> <p>d. The OCIO/NITC organizational structure and the responsibilities of the OCIO/NITC divisions are well documented and understood.</p> <p>e. Division responsibilities, services, and procedures are documented.</p> <p>f. Adequate supervisory and approval levels exist in each OCIO/NITC functional area.</p>	<p>We reviewed OCIO/NITC policies and procedures, internal Administrative Directives, Security Directives, and policies and procedures to ensure:</p> <ol style="list-style-type: none"> 1) Departmental policies had been taken into account 2) They are revised, updated, and changed when necessary. 3) They were documented and appropriate. <p>We reviewed the organization structure, and responsibilities of the OCIO/NITC divisions to ensure they were documented and appropriate.</p>	<p>The control structure policies and procedures on the whole were suitably designed to achieve the control objective specified, but were not operating effectively.</p> <p>We noted problem/change management directives were not being followed (See Finding 4.)</p> <p>Vulnerability scan procedures were not being followed (Finding 2.)</p> <p>We identified 6 security directives that had not been finalized, as well as numerous Standard Operating Procedures (SOPs) for the midrange environment that had not been finalized. (See Finding 2.)</p> <p>We found the organizational structure policies and procedures were not suitably designed to achieve the control objective specified because responsibilities for the midrange environment were not clearly defined, nor adequately documented, and OCIO/NITC security staff did not provide oversight of the midrange environment. (Finding 2.)</p>

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>2. Segregate duties between the specialized staff as much as practical.</p>	<p>a. The OCIO/NITC is not responsible for Agency user operations or user, application, or data controls.</p> <p>b. The responsibilities of the OCIO/NITC staff and of the users of OCIO/NITC services are clearly differentiated.</p> <p>c. Separate duties are defined for the various technical specialties.</p> <p>d. OCIO/NITC personnel are prohibited from originating, changing, or correcting user input or data, unless so requested.</p> <p>e. Separation of duty is enforced through access rules within the security software whenever practical and consistent with user requirements.</p>	<p>We reviewed NITC level of service for various servers/customers.</p> <p>We tested duties performed by NITC system administrators on both NITC owned and customer systems.</p> <p>We reviewed SOPs and directives for policy and procedures related to assignment of duties to NITC personnel.</p> <p>We reviewed changes to agency systems performed by NITC personnel.</p> <p>We reviewed access to critical operating system software data sets and compared settings to best practice standards.</p> <p>We reviewed user IDs with special access privileges.</p> <p>We reviewed system settings and user rights on selected midrange environment servers.</p>	<p>The control structure policies and procedures were not suitably designed to achieve the control objective specified and controls were not operating effectively.</p> <p>We found: OCIO/NITC did not have an inventory of servers in their midrange environment nor clear identification for ownership and management of those servers. (See Finding 1.)</p> <p>NITC security staff did not provide oversight of the midrange environment. Instead, personnel administering the systems were also responsible for oversight. (See Finding 2.)</p> <p>Changes were made to customers' system software without evidence of customer approval. (See Finding 4.)</p> <p>OCIO/NITC should develop and implement controls associated with the configuration of access rules and the lack of efficient user grouping to prevent the assignment of unintended user access privileges. (See Finding 2.)</p> <p>Appropriate access permissions were not assigned on NITC-managed servers to protect critical system files and directories, including the root directory. (See Finding 2.)</p>

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>3. Apply appropriate controls to the system development lifecycle.</p>	<p>a. OCIO/NITC management and contracting agency development involvement is required prior to the design, development, testing, and conversion of new or modified application systems.</p> <p>b. The modification or installation of systems software requires the approval of OCIO/NITC management.</p> <p>c. The installation/modification of midrange server operating systems hardware and software. Monitor security via COTS SW. Research security patches, fixes and virus alerts.</p>	<p>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.</p> <p>We reviewed software change control procedures to determine if software changes received documented authorization, review, and approval before implementation.</p> <p>We reviewed system configurations in the midrange environment</p> <p>We reviewed software changes to determine if testing is performed before changes are made to the systems.</p>	<p>The control structure policies and procedures were not suitably designed to achieve the control objective specified.</p> <p>No controls exist to require security staff oversight of the midrange environment. (See Finding 2.)</p> <p>Security patches/fixes were not being applied to the Midrange servers as needed. (See Finding 2.)</p> <p>Change management controls were not operating effectively. (See Finding 4.)</p>
<p>4. Provide reasonable assurance that new or modified applications systems and data files are properly converted and implemented.</p>	<p>a. Test results are documented and approved by the contracting customer before acceptance of a new system.</p> <p>b. Customers are involved in preparing the test data.</p> <p>c. As applicable, testing is performed on all interrelated systems to evaluate the integrity of those systems.</p>	<p>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.</p> <p>We reviewed software changes to determine if testing is performed before changes are made to the systems.</p>	<p>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 4.)</p>

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>5. Provide reasonable assurance that all software changes are appropriately reviewed and authorized.</p>	<ul style="list-style-type: none"> a. Authorization and approval is required before modifications are made to the network, midrange server, OA/LAN and mainframe operating systems or software applications. b. Operational personnel are not involved in changes to the operating system (mainframe or midrange server) or user applications. c. There is thorough supervision and review of all changes. d. Problems and change requests to the operating system and software controlled by the OCIO/NITC are tracked using manual and automated systems that provides an audit trail of system changes. e. Operating systems and systems software changes are tested to ensure that they operate properly and provide necessary functionality. f. Modified or new software is not installed until installation plans have been reviewed by the respective Branch Chiefs and approved by the Change Management Review Team. 	<p>We reviewed software change policies to determine if adequate controls existed over modifications to the network, midrange servers and mainframe operating systems.</p> <p>We reviewed INFOMAN (OCIO/NITC’s Management Information System) records to determine if software changes were documented and approved before modification.</p> <p>We reviewed change/problem records in MIRT (OCIO/NITC’s Midrange Installation Review Team System) and INFOMAN to ensure all changes are tracked and provide an audit trail of changes.</p> <p>We reviewed change records to determine if changes were tested before being added to the production environment.</p>	<p>The control structure policies and procedures were not suitably designed to achieve the control objective specified because controls did not exist to ensure written documentation existed to support changes approved by the Change Configuration Board.</p> <p>Approval was not always obtained before software modifications were performed. (See Finding 4.)</p> <p>Emergency changes were not always authorized or approved as required by OCIO/NITC policies. (See Finding 4.)</p> <p>Testing of changes was not always performed before being put into the production environment. (See Finding 4.)</p> <p>Not all changes were recorded into INFOMAN. (See Finding 4.)</p>

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>6. Conduct the planning activities needed to provide reasonable assurance that the OCIO/NITC will meet functional and control requirements.</p>	<p>a. Document current OCIO/NITC controls, and identify required new controls.</p> <p>b. To the degree possible, plan how the OCIO/NITC will meet future Information System requirements.</p>	<p>We reviewed OCIO/NITC’s internal controls framework and evaluated various plans such as OCIO/NITC’s Security Plans, contingency plans, and system accreditations.</p> <p>We interviewed OCIO/NITC personnel to determine future plans for securing OCIO/NITC various platforms.</p>	<p>The control structure policies and procedures were not suitably designed to achieve the control objective specified because planning activities were informal and undocumented, and OCIO/NITC has not complied with OMB Circular A-130 requirements. (See Finding 1.)</p>
<p>7. Access to the operating system, associated software and documentation is restricted to authorized personnel.</p>	<p>a. Software system specialists are prohibited from initializing the operating system.</p> <p>b. Operational personnel are prohibited from making modifications to the operating system and software. OA/LAN is administered per MOU and security staff oversight.</p> <p>c. 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.</p> <p>d. 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.</p>	<p>We reviewed system logging policies and procedures.</p> <p>We reviewed system logs, change management policies and procedures, and recently completed INFOMAN records.</p> <p>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.</p> <p>We attempted to review written access authorizations for persons with system administrator duties in the midrange environment.</p>	<p>The control structure policies and procedures were not suitably designed to achieve the control objective as shown below:</p> <p>No written policies and procedures exist to outline what system logs to review for the mainframe and what actions to take for various security violations. (See Finding 3.)</p> <p>Not all servers in the midrange were logging system access. For those servers with logging enabled, review of the logs was responsibility of system administrators. (See Finding 2.)</p> <p>Implementation of its reengineered change control process has not been completed. (See Finding 4)</p> <p>Written access authorizations did not exist for system administrators in the midrange environment. (See Finding 2.)</p> <p>Special access privilege policies had been updated but not yet implemented because not all user IDs with special access privileges had approval forms on file. (See Finding 3.)</p>

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>8. Provide reasonable assurance that operations staff operates automated equipment in accordance with the management criteria.</p>	<p>a. Access to resources and data files is limited by security software to those required to do their work.</p> <p>b. On most USDA systems, critical and repetitive operations to maintain systems are automated using CA-7 and OPS/MVS.</p>	<p>We reviewed critical data sets to determine if user IDs accessing these data sets were being logged.</p> <p>Reviewed documentation and INFOMAN records to determine if the MAINT (maintenance) privileges had been utilized in a manner to effectively limit its user to predefined, routine system management activities.</p> <p>We reviewed system configuration in the midrange environment to determine if logging is maintained on the servers.</p>	<p>The control structure policies and procedures were suitably designed to achieve the control objective specified; however, the controls had not been placed into operation.</p> <p>System activities on the midrange servers were not always being logged, and when logging did occur, system administrators reviewed the logs. (See Finding 2.)</p> <p>Although OCIO/NITC had reduced its usage of the MAINT privilege, its usage has not been reduced to restrict its use for only routine system management activities. (See Finding 3.)</p>
<p>9. Provide reasonable assurance that equipment is used by authorized persons following prescribed procedures.</p>	<p>a. Access to the operations area and office is physically restricted through the use of a key badge system.</p> <p>b. Policies and procedures ensure that access to the Operations area is highly restricted. This includes midrange server activities.</p>	<p>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.</p> <p>Reviewed documentation that NITC recertified individuals who require access to sensitive areas based on job function.</p> <p>Reviewed provisions in Directive A-8</p> <p>Reviewed physical access to consoles to ensure access limited to only those individuals that require it to perform their job.</p> <p>Reviewed configuration consoles to allow only the functions necessary to support NITC operations.</p>	<p>The control structure policies and procedures were suitably designed to achieve the control objective specified, had been placed into operation, and were operating effectively.</p>

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>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.</p>	<p>a. TSO and batch access to resources and data files is controlled through management controls and the use of the security package CA-ACF2. This also covers midrange server and OA/LAN responsibilities.</p> <p>b. OCIO/NITC suspends or deletes logon IDs that have been inactive for designated periods of time monthly.</p> <p>c. CA-ACF2 is used to control user Logon-IDs and passwords.</p> <p>d. The OCIO/NITC creates only those LIDs requested by an Agency Security Officer.</p> <p>e. Special privileges must be requested and approved by the appropriate ISSPMs or management officials.</p> <p>f. Firewalls and intrusion detection control and detect activity.</p>	<p>We reviewed related policies and procedures and security software access controls over inactive user IDs.</p> <p>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.</p> <p>We reviewed related policies and procedures and security software access controls over special privilege user IDs.</p> <p>We reviewed policies and procedures, reviewed firewall rules and tested access controls over firewalls.</p> <p>We reviewed access controls over TSO accounts.</p> <p>We reviewed policies and procedures and tested access controls over routers.</p> <p>We tested user rights to ensure users were able to access only areas associated with their assigned responsibilities.</p> <p>We reviewed system configurations to ensure settings did not allow excessive user privileges.</p>	<p>The control structure policies and procedures were not designed to achieve the control objective specified.</p> <p>Unsecured access to the NITC mainframe is still being allowed via the Internet. (See Finding 3.)</p> <p>For midrange servers and firewalls, a policy had not been established to ensure only authorized users had access, nor established a policy for review of user access to the system. (See Finding 2.)</p> <p>Agencies were not complying with OCIO/NITC's policies and procedures to obtain waivers for using passwords set to never expire, nor did they follow the policy for changing passwords. (See Finding 3.)</p> <p>Weaknesses identified in the midrange environment (See Finding 2) include:</p> <ul style="list-style-type: none"> • Password security settings and access permissions did not always meet departmental and NIST guidelines; • User accounts comprised of generic accounts, guest accounts, and other accounts unidentifiable to employee lists; • Administrator accounts and user rights did not always meet departmental and NIST guidelines; and, • Excessive access rights were granted to directories and files.

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>11. Data files are adequately protected from unauthorized modification or destruction.</p>	<p>a. Agency Security Officers are responsible for identifying critical user files. Users back up their applications and data on the schedule they deem appropriate. On midrange server environments, NITC system administrators rotate customer backup tapes off site at customer request and use the mainframe as a supplemental backup media through IBM's Tivoli Storage Manager.</p> <p>b. Procedures are documented in the NITC Disaster Recovery Plans.</p>	<p>We performed testing in NITC's midrange environment over system ownership.</p> <p>We interviewed NITC system administrators regarding back-up procedures taken.</p> <p>We requested the most current Contingency/ Disaster Recover Plans for OCIO/NITC Infrastructure Support, Mainframe and General Support Systems.</p>	<p>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 1.)</p>
<p>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.</p>	<p>a. Risk assessments are performed on OCIO/NITC systems.</p> <p>b. A Contingency Plan for Alternate Site Operations is in place. A plan for midrange server environments has not been documented. It will be in the next issuance of the contingency plan.</p> <p>c. The USDA Internet Access network provides the physical medium for the OCIO/NITC wide area network.</p>	<p>We obtained and reviewed risk assessments performed on OCIO/NITC systems.</p> <p>We reviewed desk exercises conducted relating to disaster recovery.</p> <p>We requested OCIO/NITC Contingency Plans.</p> <p>We determined if communication software logical controls have been implemented.</p>	<p>The control structure policies and procedures were suitably designed to achieve the control objective specified, however, OCIO/NITC had not conducted a Business Impact Analysis (BIA) before completing their risk assessments. The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, characterize the consequences of a disruption to the system. Without the BIA first, OCIO/NITC cannot be assured that all system components and critical services were adequately identified, prioritized, and included in the risk assessment. (See Finding 1.)</p> <p>Unencrypted access from the Internet is still available, even though OCIO/NITC planned to have this corrected by 01/01/2004. (See Finding 3.)</p>

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
<p>13. Evaluate and substantiate IT controls on a regular basis.</p>	<p>a. Vulnerabilities are assessed on a regular basis through risk assessments, vulnerability assessments, and security testing.</p> <p>b. 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 midrange disaster recovery strategy. An AIX recovery strategy has been developed and tested.</p>	<p>We determined if OCIO/NITC periodically identifies significant threats to the well-being of sensitive and critical resources and identifies related risks.</p> <p>We interviewed OCIO/NITC officials to determine if all network devices were periodically scanned.</p> <p>We obtained and reviewed scan reports of selected systems.</p> <p>We interviewed OCIO/NITC security staff to determine the oversight of the security staff on the midrange environment.</p> <p>We requested OCIO/NITC Contingency Plans.</p> <p>We reviewed firewall rules to ensure NIST and OCIO guidelines were being followed.</p>	<p>The control structure policies and procedures were not suitably designed to achieve the control objective specified.</p> <p>No procedures exist to allow for security staff oversight of the midrange environment. (See Finding 2)</p> <p>OCIO/NITC had not documented justification of their firewall configuration. (See Finding 2.)</p> <p>Network devices were not scanned for the first 9 months of FY 2004. (See Finding 2.)</p> <p>OCIO/NITC recognized the need to create contingency plans for OCIO/NITC-owned general support systems, and telecommunications. (See Finding 1.)</p>
<p>14. Provide an appropriate level of personnel security and security awareness.</p>	<p>a. Ensure terminated employees are disallowed access to the NITC and NITC resources.</p>	<p>We tested access controls over selected midrange servers to determine if terminated employees were disallowed access to NITC resources.</p>	<p>The control structure policies and procedures were not suitably designed to achieve the control objective specified. OCIO/NITC did not have procedures in place to reconcile user IDs to employee lists.</p> <p>We identified that OCIO/NITC has weak controls over timely removal of unneeded user accounts.</p>