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

NATIONAL INFORMATION TECHNOLOGY CENTER – GENERAL CONTROLS REVIEW FISCAL YEAR 2002

Report No.
88099-4-FM
December 2002

USDA UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20250

DATE: DEC 12 2002

REPLY TO
ATTN OF: 88099-4-FM

SUBJECT: National Information Technology Center – General Controls Review Fiscal Year 2002

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 September 30, 2002. The audit was conducted in accordance with "Government Auditing Standards" and Statement on Auditing Standards No. 70. The report contains a qualified opinion on the internal control structure because certain control policies and procedures, as described in the report, were not suitably designed or placed in operation.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 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.

Richard D. Long

RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

NATIONAL INFORMATION TECHNOLOGY CENTER
GENERAL CONTROLS REVIEW
FISCAL YEAR 2002

AUDIT REPORT NO. 88099-4-FM

PURPOSE

The objectives of our audit were to obtain reasonable assurance about whether (1) the accompanying description of the internal control structure of the U.S. Department of Agriculture's, Office of the Chief Information Officer/National Information Technology Center (OCIO/NITC) presents fairly, in all material respects, the aspects of the OCIO/NITC's policies and procedures that may be relevant to a user organization's internal control structure; (2) the control structure of policies and procedures was suitably designed to achieve control objectives; (3) the policies and procedures were complied with; (4) the policies and procedures had been placed in operation; and (5) the policies and procedures were operating effectively.

RESULTS IN BRIEF

Our audit disclosed that, except for the matters referred to below, the accompanying description of the internal control structure 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.

NITC continues to take actions toward complying with Federally mandated security requirements, but additional actions are needed. NITC has made a concerted effort toward completion of risk assessments, which is an important step toward improving security. With the completion of risk assessments imminent, NITC should be able to focus resources toward completion of other Federally mandated security requirements. Specifically, NITC had not:

- Addressed all security program planning requirements prescribed by Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated

November 30, 2000, and National Institute of Standards and Technology (NIST) Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," dated December 1998;

- updated contingency plans to reflect deficiencies identified during its testing process;

- documented system security check procedures to ensure all tests are performed consistently; and

- provided the training needed by its security staff to properly maintain and monitor its systems.

NITC had improved its controls over logical access to its systems, but additional actions are needed to ensure resource security. We noted instances where NITC had not:

- Removed separated employees' remote access accounts;

- followed departmental procedures for password settings;

- documented users with special access privileges;

- documented security software parameters;

- developed and implemented security log monitoring policies and procedures; and

- completed the implementation of secure Internet access.

We also noted where NITC was not always following its current written policies in place for identifying, selecting, installing, and modifying system software, for both routine and emergency changes. For example, we noted the lack of an audit trail to support the approval and testing of system modifications. Generally, these conditions exist because NITC has allowed agencies to establish their own account restrictions, and because NITC has not placed a priority on documenting its system software changes.

We believe that all of the weaknesses identified in this report are material internal control weaknesses and need to be addressed in OCIO's Federal Managers' Financial Integrity report until adequately corrected.

KEY RECOMMENDATIONS

To improve controls over security requirements, we recommended that NITC:

- Establish a time-phased plan for ensuring that contingency plans are periodically updated to reflect changes and results of testing. Ensure that the plans contain the names of disaster recovery team members and alternates. Ensure disaster recovery team members are trained in their responsibilities.

- Develop and implement standard security assessments for testing system security before system changes are placed into the production environment. Implement policies requiring that testing be documented.

- Ensure adequate training of all employees and contract personnel is completed and necessary documentation is maintained.

To improve controls over logical access, we recommended that NITC:

- Establish a written policy requiring minimum account settings that conform to OMB, NIST, and departmental requirements. When customer agencies request a deviation from these standards, periodically require the administrator of the agency and the Department's Chief Information Officer to sign a waiver acknowledging the inherent risks.

- Establish controls to ensure users requesting special access privileges are properly documented and formally approved.

- Establish procedures to ensure that the agency security officer listing remains current and that no accounts with the security privilege exist for non-agency security officers.

- Establish a plan of action addressing timeframes for completing its process for documenting and testing the global system settings for all its systems.

- Establish procedures for logging and monitoring access through the security software, and required follow-up on problems noted.

To improve change control procedures, we recommended that NITC:

- Establish controls to ensure that change control procedures include documenting written authorizations and testing before changes are implemented.

- Establish controls to notify managers of changes that affect their areas of responsibility prior to making changes and include necessary staff in the testing and approval process.

- Establish controls to ensure changes are properly recorded, including all relevant information about the change.

AGENCY POSITION

OCIO/NITC generally agreed with our findings and recommendations.

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 accompanying description (see Exhibit A) of controls of the U.S. Department of Agriculture's (USDA), Office of the Chief Information Officer's (OCIO), National Information Technology Center (NITC). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the OCIO/NITC's policies and procedures that may be relevant to a user organization's internal control structure; (2) the control structure of policies and procedures were suitably designed to achieve control objectives; (3) the policies and procedures were complied with; (4) the policies and procedures had been placed in operation; and (5) the policies and procedures were operating effectively as of September 30, 2002. The control objectives were specified by OCIO/NITC.

Except as discussed in Finding No. 3, the audit was conducted in accordance with "Government Auditing Standards" issued by the Comptroller General of the United States. We also followed 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 three 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 its security policies and procedures comply with existing Federal security guidelines.

In our opinion, except for the matters referenced to in the previous paragraph, the accompanying description of the internal control structure presents 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.

In addition to the procedures we considered necessary to render our opinion, as expressed in the previous paragraph, we applied tests to specific controls included in

Exhibit B of this report, to obtain evidence about their effectiveness in meeting the specified control objectives during the period October 1, 2001, to September 30, 2002. The specified controls and the nature, timing, extent and results of the tests are listed in Exhibit B. In our opinion, except for the matters discussed above, the policies and procedures that were tested, as described in Exhibit B, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Exhibit B were achieved during the period from October 1, 2001, to September 30, 2002. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Exhibit B were achieved; accordingly, we express no opinion on achievement of control objectives not included in Exhibit B.

The relative effectiveness and significance of specific controls at 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 description of policies and procedures at OCIO/NITC is as of September 30, 2002, and information about tests of the operating effectiveness of specific controls cover the period from October 1, 2001, to September 30, 2002. 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 customer agencies, and their auditors.

/s/

RICHARD D. LONG
Assistant Inspector General
for Audit

September 30, 2002

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	FURTHER ACTIONS ARE NEEDED TO COMPLY WITH FEDERALLY MANDATED SECURITY REQUIREMENTS

FINDING NO. 1

NITC continues to take necessary actions toward compliance with Federally mandated security requirements; however, additional actions are needed. Specifically, NITC had not:

- Completed a Security Plan that addresses all the requirements prescribed by the Office of Management and Budget (OMB)[1] and National Institute of Standards and Technology (NIST);[2] [3]
- updated contingency plans to reflect deficiencies identified during its testing process;
- documented standard test procedures to ensure all system security checks are performed consistently; and
- provided the training needed by its security staff to properly maintain and monitor its systems.

NITC officials have recognized the need to complete these actions and indicated that other priorities, such as completing Federally required risk assessments, have prevented them from focusing on these efforts. With the completion of its risk assessments imminent, NITC should be able to focus resources toward completion of these other Federally mandated requirements. Because NITC provides information management and other automated processing services to support program and administrative missions of the Department and other users, it needs to promptly complete planned actions to comply with Federally mandated requirements. Without these controls, NITC cannot be assured that computer resources are properly protected/monitored and controls are consistently applied.

OMB Circular A-130 established a minimum set of controls for agencies' automated information security programs, including certifying to the security of any systems that maintain sensitive data, establishing contingency plans and recovery procedures in the event of a disaster, and establishing a comprehensive security plan. OMB Circular A-130 further requires

[1] OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.
[2] NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," dated December 1998.
[3] Subsequent to our review, NITC finalized its 2002 Security Plan.

agencies to ensure that all individuals are appropriately trained in how to fulfill their security requirements before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and Office of Personnel Management, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system. NIST Special Publication 800-18 states that one of the keys to a successful computer security program is security awareness and training. If employees are not informed of applicable organizational policies and procedures, they cannot be expected to act effectively to secure computer resources.

Security Plan

At the time of our review, NITC had not yet updated its internally-prepared risk assessment and its fiscal year 2001 NITC Security Plan to incorporate deficiencies identified during our fiscal year 2000 audit.[4] NITC was revising the plan to incorporate identified problem areas and mitigations as well as missing elements. Problem areas included developing agreements with customers regarding security requirements, identifying and monitoring information systems security program performance measures, and documenting system software security settings.

Additionally, documents used by NITC security staff in their day-to-day operations are referred to in NITC's Security Plan, but these documents were outdated. During our fiscal year 2000 audit, NITC officials indicated that the Security Administrator's Guide, containing the agency security staff listing, was being updated. However, the same version of the document was provided to us during this review, making this document over 4 years old. NITC staff indicated that the document has not been updated because security staff have been conducting risk assessments and revising the Security Plan to meet OMB requirements.

Another document referred to in NITC's Security Plan identifies NITC's internal controls, techniques, procedures, responsible staff, and testing and evaluation techniques. NITC's Strategic Plan states that this internal controls document is NITC's blueprint for all of its operations, which includes controls on (1) accessing the operating system and associated software; (2) restricting documentation to authorized personnel; and (3) applying appropriate controls to the systems development lifecycle. Several of the documents such as NITC Administrative Directives, Security Administrators Guide, and a telecommunications guide referenced in the internal controls document did not exist or were outdated. The directives define and communicate NITC's organizational structure, policies, and procedures.

[4] Audit Report No. 88099-03-FM, "NITC General Controls Review Fiscal Year 2000," dated September 21, 2001. Subsequent to our review, NITC had finalized its 2002 Security Plan.

The Security Administrators Guide is used by security staff in NITC's day-to-day system security operations. At the close of our audit, NITC officials provided some of the revised directives for our review; provided a revised internal controls document, and stated that they plan to update the remaining directives, and revise the security guide. While these documents still contain valid control techniques and should remain as important internal control documents, we believe NITC needs to ensure that they are properly maintained and that other documents they refer to are kept up-to-date.

OMB's requirement for establishing security plans has existed since December 1985; however, NITC has made a concerted effort in the past several months and continues to work toward OMB Circular A-130 compliance. Therefore, we are making no further recommendations on this issue in this report.[5] Subsequent to our fieldwork, NITC finalized its 2002 Security Plan. However, until such time that NITC complies with these requirements, NITC needs to include this material weakness, and those addressed elsewhere in this report, in its Federal Managers' Financial Integrity Act report. Further, NITC should consider establishing measurable performance goals relating to the security of its information technology (IT) resources in its Government Performance and Results Act report.

Contingency Plans

NITC has policies in place to perform contingency plan tests every 3 to 6 months. However, NITC's Contingency Plan, dated December 1998, is almost 4 years old and has not been updated to reflect the significant deficiencies identified during its own testing. NITC security staff are in the process of assessing its contingency plan to ensure it reflects any changes in hardware, software, and personnel. Our review of the May 2000 disaster recovery test assessment noted problems in variances between the production Initial Program Load (IPL) procedures and the hot site IPL procedures. However, these differences were not incorporated into the contingency plan.

Additionally, we noted that the contingency plan did not include detailed procedures to follow when the data service center is unable to receive or transmit data and did not identify the alternate processing facility or backup storage facility. Furthermore, we found that the contingency plan for one system did not identify the disaster recovery team members and their alternates. Therefore, we cannot be assured that disaster recovery team members had been trained on their responsibilities should a disaster occur.

NITC provides information management and other automated processing services to support program and administrative missions of the Department, its agencies, and other users. NITC's internal controls document states that

[5] We recommended that NITC ensure that its security plan is prepared in accordance with OMB Circular A-130 in Audit No. 88099-3-FM, "National Information Technology Center – General Controls Review Fiscal Year 2000," dated September 21, 2001.

it will develop and periodically test a plan that will allow NITC to recover operating systems and software within 3 days of disruption or failure. Without an effective operable recovery plan NITC cannot be assured that it will be able to provide efficient continued automated processing services to support its customers.

System Certification

NITC's Security Plan states that security staff participates in the certification of security software and security features during a formal system certification process. However, NITC staff did not document or have a standard testing process to ensure all system security checks are performed consistently during system testing. Departmental Manual (DM) 3200-002[6] requires that system test plan documentation be maintained throughout system operation. It further requires a clear, verifiable audit trail documenting approval, acceptance, and testing of the changes in a system test environment. Further, NIST guidance for conducting system certifications calls for a plan to ensure that the proper blend of completeness and focused emphasis is achieved in testing system controls. Because there is no documented standard testing process, NITC cannot be assured that computer resources are properly and thoroughly tested to ensure those resources are protected and monitored, and that controls are consistently applied.

Security Training

Our review of NITC training records showed that not all of the security staff attended formal training. NITC officials informed us that training may have been missed due to critical assignments or personal reasons. Without proper training, NITC cannot be assured that its staff has adequate skills to properly protect and monitor its systems.

We identified that 39 of 315 (12 percent) NITC personnel and contractors' personnel (most of which were contract personnel) had not received security related training. Our audit included social engineering tests[7] to see if NITC personnel would reveal their passwords. Two individuals who divulged their passwords during our testing had not received the required security awareness training. NITC officials informed us that in September 2002, they provided security awareness training to their personnel and contractors. Further, NITC has assigned a staff person to monitor security awareness training and ensure that all NITC personnel and contractors are provided such training.

[6] DM 3200-002, "A Project Manager's Guide to Application Systems Life Cycle Management," Section 1.3.B (6); (7)(a), (b), (d); and (8)(b), dated March 3, 1988.

[7] Our social engineering tests included calling or sending an e-mail to randomly selected NITC personnel and asking them to divulge their password.

RECOMMENDATION NO. 1

Establish a time-phased plan for ensuring that contingency plans are periodically updated to reflect changes and results of testing. Ensure that the plans contain the names of disaster recovery team members and alternates. Ensure disaster recovery team members are trained in their responsibilities.

RECOMMENDATION NO. 2

Develop and implement standard security assessments for testing system security before system changes are placed into the production environment. Implement policies requiring that testing be documented.

RECOMMENDATION NO. 3

Ensure adequate training of all employees and contract personnel is completed and necessary documentation is maintained.

CHAPTER 2	WEAK ACCESS CONTROLS COULD IMPACT THE INTEGRITY AND CONFIDENTIALITY OF CRITICAL DATA

FINDING NO. 2

NITC has improved its controls over logical access to its systems; however, additional actions are needed to ensure the proper security of its resources. NITC had not:

- Removed remote access accounts held by separated employees;
- followed departmental procedures for password settings;
- documented users with special access privileges;
- documented security software parameters;
- developed and implemented policies and procedures outlining monitoring of security logs; and
- completed the implementation of secure Internet access.

While NITC has begun to address some of these issues, as discussed below, NITC officials indicated that other priorities, such as completing Federally required risk assessments, have prevented them from focusing on these efforts. In today's increasingly interconnected computing environment, inadequate access controls can expose an agency's information and operations to attacks from remote locations by individuals with minimal computer or telecommunications resources and expertise. As a result, the integrity, availability, and confidentiality of NITC resources are vulnerable to potential fraud and misuse, inappropriate disclosure, and potential disruption.

OMB Circular A-130[8] stresses management controls affecting users of IT. These controls help to protect operating systems and other software from unauthorized modification and protect the integrity, availability, and confidentiality of information by restricting the number of users and providing protection from disclosure of information to unauthorized individuals. OMB lists individual accountability as a primary mechanism for personnel security. It recognizes that 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[9] stress the need for agencies to implement the "least privilege" concept, granting users only those accesses required to perform

[8] OMB Circular A-130, Appendix III, Section A, November 30, 2000.
[9] NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998.

their duties. DM 3140-1[10] requires security staff to remove employee user identifications (ID) and passwords when the employee is no longer with the agency; and the use of individual user IDs and passwords to control access to systems processing personnel, financial, market-related, or other sensitive data. It also established the maximum password life for network access to 90 days.[11]

User Accounts

Effective security controls and mechanisms are required to ensure that all information is properly protected and available to those who have a requirement to access the information. Logical access controls can prescribe not only who or what is to have access to a specific system resource, but also the type of access permitted. Logical access controls such as user names, passwords, and access permissions, ensure that only authorized users have access to network resources, and users are only granted the access needed to conduct their job responsibilities.

Our review of user IDs disclosed the following.

- Of the 22,124 user IDs on NITC's main system, 941 had passwords that were set to never expire. Of those, 915 user IDs had passwords older than 90 days, including 381 current user accounts with passwords that were more than 10 years old. NITC did not have written requests from agency management requesting these settings.

- On another system, we identified 29 of 142 user IDs that had not been accessed in the last 6 months, including 4 that had never been used. While reviewing user IDs that NITC security staff are responsible for monitoring, we identified one user ID over 2 years old that had never been used and had a password interval of 120 days. NITC has informed us that they have deleted this ID.

- On its remote access system, NITC did not periodically reconcile user accounts to a list of current employees and contract personnel. We identified 12 active remote access user accounts that were not traceable to NITC's current employee, separated employee, or contract personnel listings. NITC had not obtained waivers for 4 shared group accounts.[12] We also identified a separated employee who still had an account. Complicating the identification of valid user accounts was the fact that NITC did not maintain a complete listing of the contract personnel it employed.

[10] DM 3140-1.6, "Management ADP Security Manual," part 6 of 8, Section 6c, July 19, 1984.
[11] DM 3140-1.6, "Management ADP Security Manual," Part 6 of 8, Appendix D, Amendment 6, sections 5 and 6b, July 19, 1984.
[12] NITC subsequently removed three of the four shared group accounts.

These conditions occurred because NITC allows certain account restrictions to be dictated by its customer agencies. Specifically, NITC did not establish written documentation outlining use of a default setting for all new accounts created; create consistent procedures for customer agencies to follow in requesting waivers from the customer agency administrator and Department Chief Information Officer (CIO) from standard NITC settings; maintain written documentation to support why an account was created and by whom; and keep a complete listing of contract personnel. As a result, NITC cannot be assured that internal controls over user account settings are implemented and adequately safeguard agencies' data. NITC should establish minimum account settings and require written justification from the agency administrator and Department CIO when agency-requested settings do not conform with the established minimums.

Special Access Privileges

While NITC has substantially reduced the number of user IDs that have the non-cancel[13] privilege, NITC still does not have justification and management approval for user accounts with the other five special access privileges that should be monitored. NITC security staff informed us that they are still in the process of reviewing these privileges and establishing requirements for approval, based on our fiscal year 2000 audit recommendation. As a result, NITC could not be assured that the persons responsible for the 193 accounts we identified that were assigned special access privileges had a valid job-related need to have those privileges.

We also identified that NITC had not ensured that only those individuals who actually perform security officer functions at its customer agencies have the security officer privileges. Agency security officers' control access to agency data and can request NITC security staff to create user accounts. NITC security staff personnel are not maintaining a current listing of agency security officers and could not ensure that restricted special access privileges are being removed when no longer required. We determined not all of the 125 users whose accounts have the agency security officer privilege can request that NITC create new user accounts. NITC had not maintained a list of only those agency security officers that had this authority.

Security Software Global System Settings

NITC did not have documentation supporting its global system security settings. Global system settings define how the network-wide security software environment operates, such as resource access control settings, user activity logs for IDs with special privileges, and logs of profile changes.

[13] The non-cancel access allows the user of the account to access any data set on the mainframe regardless of their other user privileges.

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, 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 were adequately configured and tested to maintain the integrity of the security software. NITC was aware of this issue and had contracted out a review of all the global system settings. When complete (estimated completion date of September 30, 2002), the contractor will be required to assist NITC in implementing corrected global system settings (if appropriate), and provide a detailed document supporting the purpose and justification for each setting.

Monitoring Access

NITC staff informed us that it reviews system security logs to identify and follow up on security violations. However, we cannot be assured that this practice is being applied thoroughly and/or timely because NITC did not have standard policies in place to ensure follow up was being performed. NITC does not have any written policies and procedures outlining what:

- Logs/reports will be reviewed;
- actions will be taken for different security violations;
- security violations will be investigated; and
- supporting documentation will be created and maintained supporting any investigations.

Additionally, NITC has not documented which security violations it noted, the level of investigation it initiated, the results of its investigation, the remedial actions taken by the security staff to prevent a reoccurrence, and whether it identified patterns of violations.

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. According to OMB, 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[14] requires the maintenance of access logs sufficient to permit the reconstruction of events in the case of unauthorized data or program access or use. Security/access

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

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 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. 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 on the recommendation made in our fiscal year 2000 audit, NITC is working toward, but has not completed, the implementation of its Enterprise Cyber Security Project. The project includes establishing controls to ensure users that access to NITC resources from the Internet are required to connect through a controlled, secure manner. NITC is currently working with agency staffs to (1) migrate agency resources to the Public Access Network; (2) ensure all sensitive data is encrypted; (3) allow only connections from USDA Intranet sources and secure Extranet business partners; and (4) identify resources required by their applications and defining actions needed to bring them into compliance.

RECOMMENDATION NO. 4

Establish a written policy requiring minimum account settings that conform to OMB, NIST, and departmental requirements. When customer agencies request a deviation from these standards, periodically require the administrator of the agency and the Department's CIO to sign a waiver acknowledging the inherent risks.

RECOMMENDATION NO. 5

Establish controls to ensure users requesting special access privileges are properly documented and formally approved.

RECOMMENDATION NO. 6

Establish procedures to ensure that the agency security officer listing remains current and that no accounts with the security privilege exist for non-agency security officers.

RECOMMENDATION NO. 7	Establish a plan of action addressing timeframes for completing its process for documenting and testing the global system settings for all its systems.
RECOMMENDATION NO. 8	Establish procedures for logging and monitoring access through the security software, and required follow-up on problems noted.

CHAPTER 3	WEAK CHANGE CONTROL PRACTICES COULD IMPACT THE INTEGRITY OF THE OPERATING ENVIRONMENT

FINDING NO. 3

We identified that weak change control practices could compromise the integrity of the operating system. Specifically, based on available documentation, we were unable to validate that new system software versions or modifications to existing software were properly authorized, supported, tested and logged. While NITC had current written policies in place for identifying, selecting, installing, and modifying system software, for both routine and emergency changes, NITC had not established controls to ensure that personnel were following these established procedures. Without proper software change controls, NITC's general support system is at risk of processing irregularities that could occur or security features that could be inadvertently or deliberately omitted or rendered inoperable.

DM 3200-002[15] requires a change control process for all major application systems, that properly documents the change process including approval, acceptance, and testing of the changes in a system test environment. It also requires a clear, verifiable audit trail documenting all production library changes. Further, NIST,[16] recognizes that computer systems and the environments in which they operate change continually. For both major and minor changes, the manual mandates system testing and appropriate documentation.

Our review of the Agency Applications Services Division (AASD) change control request forms for one accounting system determined that the forms were not signed to show that the change request was approved. Therefore, we could not be assured that acceptance of all changes was obtained before changes were implemented on production systems.

Furthermore, our review of the last nine completed system changes disclosed that seven had not been approved. According to NITC Administrative Directive No. 17, Problem/Change Management, the Problem/Change Management Team is to review and approve all changes prior to their implementation. In addition, NITC could provide no support that managers had been notified in advance of the changes and that the changes had been properly researched and tested by the managers of the affected areas.

NITC security staff was using a software-based reporting tool to monitor

[15] DM 3200-002, "A Project Manager's Guide to Application Systems Life Cycle Management," Section 1.3.B (7)(a), (b), (d), and (8)(b), dated March 3, 1988.
[16] NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," dated October 1995.

changes made to the authorized program facility (APF) libraries on a weekly basis providing after-the-fact proof that a change had actually been made. In the first 6 months of 2002, NITC security staff identified 276 changes to the APF libraries. However, NITC security staff were not made aware of the changes prior to their occurrence and informed us they were unable to locate appropriate support for the changes in NITC's management information system. We identified two APF libraries that were added to the system and then deleted the following week. Such immediate changes would indicate that the change was found to be either inappropriate or problematic. Proper notification to the NITC security staff prior to changes to the APF libraries would help prevent such problems. NITC officials acknowledged that some system software changes may be approved verbally which may not have been properly recorded in its management information system. NITC officials informed us that they have begun to address the system software change control issues we identified during our review.

Control of APF libraries and programs, which can run with special privileges and potentially sidestep the security mechanisms of the operating system, including access control software, is critical to the overall integrity and security of the operating environment. The APF libraries are the key security feature of the operating system under NITC's control. APF authorized programs can circumvent or disable all security mechanisms, including security software products, in addition to accessing all production data. Programs that meet APF authorization requirements can issue a command to switch themselves into supervisor state. Programs in this supervisor state are permitted to execute privileged machine instructions. In addition, programs authorized to bypass password protections are able to access password-protected data sets and thus, bypass all security software protection. Therefore, control over these libraries and programs, and changes to them, is critical to the overall security of the operating environment. Changes to these programs, without the prior knowledge, testing, and approval of NITC security staff could result in significant unknown security weaknesses in the operating environment. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted, "turned off," and/or irregularities or malicious code may be processed.

RECOMMENDATION NO. 9	Establish controls to ensure that change control procedures include documenting written authorizations and testing before changes are implemented.
RECOMMENDATION NO. 10	Establish controls to notify managers of changes that affect their areas of responsibility prior to making changes and include necessary

staff in the testing and approval process.

RECOMMENDATION NO. 11	Establish controls to ensure changes are properly recorded, including all relevant information about the change.

EXHIBIT A:

DESCRIPTION OF THE

INTERNAL CONTROL STRUCTURE

FOR THE

U.S. DEPARTMENT OF AGRICULTURE

OFFICE OF THE CHIEF INFORMATION OFFICER

NATIONAL INFORMATION TECHNOLOGY CENTER

AS OF SEPTEMBER 30, 2002

Prepared by:
NITC