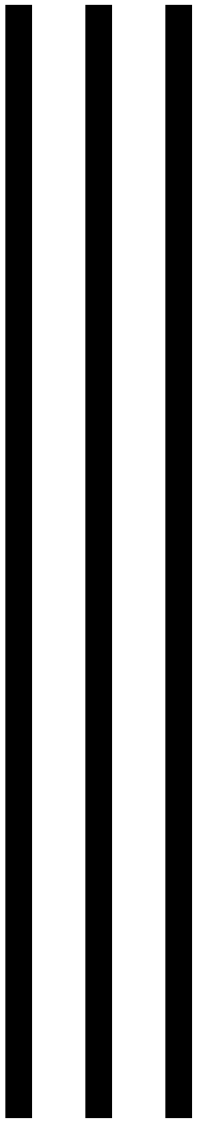

U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

NATIONAL INFORMATION TECHNOLOGY CENTER - GENERAL CONTROLS REVIEW FISCAL YEAR 2000

Report No.
88099-3-FM
September 2001

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: SEP 21 2001

REPLY TO
ATTN OF: 88099-3-FM

SUBJECT: National Information Technology Center General Controls Review for Fiscal Year 2000

TO: Ira L. Hobbs
Acting 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, 2000. This audit was conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States. The report contains a qualified opinion on the internal controls 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 time frames for implementation. Please note that the regulation requires a management decision be reached on all findings and recommendations within 6 months of report issuance.

Richard D. Long

RICHARD D. LONG
Assistant Inspector General
for Audit

TABLE OF CONTENTS

EXECUTIVE SUMMARY

NATIONAL INFORMATION TECHNOLOGY CENTER
GENERAL CONTROLS REVIEW
FISCAL YEAR 2000

AUDIT REPORT NO. 88099-3-FM

PURPOSE

The objectives of our audit were to obtain reasonable assurance about whether: The accompanying description of the internal control structure of the U.S. Department of Agriculture's (USDA), 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; the control structure policies and procedures included were suitably designed to achieve control objectives, if those policies and procedures were complied with satisfactorily; the policies and procedures had been placed in operation; and whether 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 needs to take additional steps to ensure that only authorized users access its systems, needs to better control special privileges on user IDs, and needs to track all access to sensitive and critical datasets. NITC needs to develop formal procedures to require periodic assessment of its mainframe user identifications (ID), including those users with the non-cancelable[1] privilege, and assure that access activity relating to sensitive and critical dataset is logged.

[1] Non-cancelable access allows the user of the account to access any dataset on the mainframe regardless of their user privileges.

- NITC needs to better conduct its vulnerability scanning and better assure the vulnerabilities it does identify are corrected. Based on our prior audit recommendation, NITC began to conduct vulnerability scans of its own, and its customers' systems. However, NITC was not scanning all of its systems, nor had it corrected all the vulnerabilities identified.

- NITC needs to establish controls over access to its resources from the Internet. NITC does not require users that log into its mainframe through the Internet to do so through its virtual private network (VPN) services. Without the use of its VPN services NITC cannot be assured that data being transmitted over the Internet is protected from disclosure. Further, NITC does not have a warning banner on all its mainframe access points that informs its users that they have accessed a U.S. Government system, that access could be monitored, and that unauthorized access is punishable under Federal law. Without this banner, NITC could find it difficult to prosecute unauthorized access to its mainframe.

KEY RECOMMENDATIONS

We recommend that NITC improve its controls over logical access to its resources, review its security software logging rules to ensure that all access to sensitive and critical operating system datasets are logged, and establish controls to ensure that special access privileges are properly authorized and formally approved. We also recommended that NITC investigate and take appropriate action on the vulnerabilities identified in our scans, ensure that it includes all appropriate systems in its vulnerability scan methodology, and that it establish policies to take prompt action to investigate and mitigate the vulnerabilities it identifies. We recommended that NITC ensure that its security plan meets all requirements of Office of Management and Budget "Circular" A-130. Finally, to improve security of Internet access, we recommended that NITC establish controls to require Internet access of its mainframe to go through a controlled, secure manner; and implement a warning banner to ensure that users acknowledge their access to a U.S. Government System.

AGENCY POSITION

OCIO/ NITC generally agreed with our Findings and Recommendations.

REPORT OF THE OFFICE OF INSPECTOR GENERAL

TO: Ira L. Hobbs
Acting 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 policies and procedures were suitably designed to achieve objectives outlined in the description, if those controls were complied with satisfactorily, and (3) such controls had been placed in operation as of September 30, 2000. 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. 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 material internal control weaknesses. We found that the OCIO/NITC needs to improve its logical access controls, identify vulnerabilities on systems within its network, establish controls over access to its network from the Internet, and ensure that its security policies and procedures are brought into compliance with existing Federal security guidelines.

In our opinion, except for the matters referred 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 paragraphs, 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, 1999, to September 30, 2000. 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, 1999, to September 30, 2000. 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, 2000, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 1999, to September 30, 2000. 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 reports 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.

/s/

RICHARD D. LONG
Assistant Inspector General

September 10, 2001

FINDINGS AND RECOMMENDATIONS

FINDING NO. 1

NITC NEEDS TO IMPROVE ITS LOGICAL ACCESS CONTROLS

The NITC needs to better ensure that only authorized users access its mainframe resources, better control special access privileges on user IDs, and track all access to sensitive and critical datasets. We attributed this problem to the absence of procedures that require periodic assessment of its mainframe user IDs, including those users with the non-cancelable privileges. As a result, NITC cannot be fully assured that mainframe resources are properly safeguarded or that access to sensitive information is properly controlled.

The Office of Management and Budget (OMB), Circular A-130, Appendix III, Security of Federal Automated Information Resources, established a minimum set of controls for agencies' automated information security programs, including certifying to the security of any systems that maintain sensitive data. Further, Departmental Manual 3140-1.6 (DM3140-1.6), ADP Management Security Manual (Part 6 of 8), section 6c, requires security staff to remove employee user IDs and passwords when the employee is no longer with the agency.

Unused Accounts

In our prior audit of NITC's General Controls[2], we identified a large number of accounts on the NITC mainframe system for users who no longer required access. NITC completed the removal of these accounts in August 2000, except for one large agency and its own users. Our current review of user accounts showed that NITC personnel have not established controls to identify and remove unused IDs for approximately 26 percent of its users, including its own staff. NITC officials advised us that they now plan to review the access of all user accounts which should resolve this problem.

We identified over 160 NITC user accounts that had not been accessed within 120 days, but were still active.

[2] Audit Report No. 88099-1-FM, "NITC General Controls Review," dated December 10, 1999.

Tracking Access to Sensitive Datasets

NITC is tracking some, but not all write access to sensitive datasets through its implementation of CA-ACF2 security software. Normally, access to sensitive datasets by users that have the non-cancelable[3] privilege will be logged; however, those users that have been given explicit access to these datasets are not always being logged. IBM's Mainframe operating system manual recommends that access to sensitive operating system libraries be logged. Further, the General Accounting Office recommends that write access to sensitive datasets that are a part of the Mainframe operating system be tracked and monitored to ensure the appropriateness of such access. NITC has advised us that it is unreasonable to log access to datasets when a user's job function requires such access. However, since these datasets are responsible for the operation of the system, as a whole, write access should be logged and monitored regardless of the user's responsibilities. Without this logging capability NITC security staff cannot review all write access to its Mainframes' sensitive datasets.

Special Privilege User IDs

NITC had not followed procedures requiring formal, documented approval to grant special access privileges such as non-cancelable access to its users. NITC attributed this to the lack of oversight of the 119 NITC accounts that have the non-cancelable privilege, we found that only 47, or 39 percent, had the required formal, documented approval for such access. While NITC advised us that they do periodically review special user privileges, NITC needs to establish controls to ensure that the proper approvals are received.

RECOMMENDATION NO. 1	Establish controls to review on a monthly basis all unused IDs and assure these user accounts are deleted timely.

[3] Non-cancelable access allows the user of the accounts to access any data set on the mainframe regardless of their user privileges.

RECOMMENDATION NO. 2	Ensure security software logging rules require all access to critical and sensitive operating system datasets, including all access by users with non-cancelable privilege, are logged.
RECOMMENDATION NO. 3	Establish controls to ensure IDs requesting non-cancelable privileges are properly documented and formally approved.

FINDING NO. 2

NITC'S SYSTEM OF VULNERABILITY SCANNING LEAVES ITS SYSTEMS SUSCEPTIBLE TO ATTACK

NITC does not perform vulnerability scanning on all of its systems; nor had it taken sufficient, and timely actions to correct the vulnerabilities they identified. NITC advised us that they did not scan all its systems every time they performed vulnerability scans and that correcting vulnerabilities requires review and approval which delays the process. Our own scans of selected systems noted numerous high and medium level vulnerabilities that make the NITC susceptible to attack or other security vulnerabilities. As a result, sensitive and critical data is at risk of theft, modification, or unauthorized disclosure.

In our prior audit,[4] we performed vulnerability scans that disclosed significant vulnerabilities in NITC's systems. We recommended that NITC correct the deficiencies and establish procedures to ensure that the operating system vulnerabilities we detected do not recur. NITC agreed to scan its systems on a monthly basis. However, our review of NITC's scanning procedures showed that NITC does not scan all of the systems under its control and does not ensure the timely correction of identified vulnerabilities.

OMB A-130, Appendix III, Security of Federal Automated Information Resources, requires agencies to implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The Presidential Decision

[4] Audit Report 88099-1-FM, "National Information Technology Center General Controls Review", dated December 10, 1999.

Directive (PDD) 63[5] requires agencies that are vulnerable to infrastructure attacks to propose a plan to eliminate significant vulnerabilities.

During our current review, we conducted vulnerability scans on 50 network components[6] within NITC. We used commercially available network vulnerability scanning software that, at the time of our review, identified 900 known vulnerabilities in operating systems that use the TCP/IP protocol. Our assessments revealed 492 vulnerabilities: 15 high-risk, 110 medium-risk, and 367 low-risk vulnerabilities.[7] In today's increasingly interconnected computing environment, inadequate access controls and the failure to correct known security vulnerabilities, places an enormous amount of highly sensitive data at risk of theft, modification, or inappropriate disclosure. Furthermore, vulnerabilities on one system can lead to exploits on other systems.

Detailed below are examples of the high-risk vulnerabilities disclosed during our scans:

- The Administrator account was set to allow access by using a password that was the same as the Administrator's login ID. This vulnerability makes it easy for attackers to guess the password of the Administrator's account, the most trusted user on the system.

- A software application used to manage computer networks was left configured with their original default settings, which are well known by attackers. This vulnerability could allow an attacker to easily obtain or change system settings.

RECOMMENDATION NO. 4

Ensure that NITC includes all appropriate IP addresses in its vulnerability scanning on a monthly basis for all systems, excluding printers.

[5] The Presidential Decision Directive (PDD) 63 requires every department and agency of the Federal Government to manage and protect its critical infrastructure.
[6] A network component is a server computer, router, or switch that uses TCP/IP.
[7] High-risk vulnerabilities are those that provide access to the computer, and possibly the network of computers. Medium-risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher-risk vulnerabilities. Low-risk vulnerabilities are those that provide access to sensitive, but less significant network data.

RECOMMENDATION NO. 5	Establish controls to ensure that NITC scans its systems on a routine basis, but not less than monthly, and takes prompt action to investigate risk indicators and mitigate identified vulnerabilities.
RECOMMENDATION NO. 6	Ensure that NITC investigate all high and medium risk vulnerabilities identified during our audit and take appropriate corrective action.

FINDING NO. 3

ACCESS TO NITC SYSTEMS FROM THE INTERNET IS NOT SECURE

NITC does not ensure that access to its mainframe from the Internet goes through its virtual private network (VPN)[8] connection. Further, NITC does not have the required warning banner on its mainframe connections. Although NITC officials advised us that they discourage mainframe access through any means other than its VPN, it allows users to gain unencrypted access to its resources from the Internet. As a result, NITC is exposing its mainframe systems to attack from Internet users, and cannot be assured that data being transmitted from its mainframe through the Internet is encrypted to minimize the risk of unauthorized disclosure of the data. Further, without a warning banner, NITC may hinder its ability to prosecute unauthorized users that access their systems.

In our Audit Report Number 23099-1-FM dated March 30, 1995, we reported that the Department was at risk because agencies were not complying with department regulations which required data transmitted over the internet to be encrypted. The OCIO replied on July 19, 2000, that it concurred with our recommendations. It advised us that it was assembling an interagency team to analyze alternatives, on how to protect mission-critical and sensitive data transmitted via internet. It estimated completion of actions by September 2001. We plan to review the final actions taken by the OCIO in this area in our agency audits.

OMB A-130 requires that Federal agencies implement and maintain a program to ensure that adequate security is provided for all agency

[8] A VPN is an encrypted connection between two computers over a public network like the Internet.

information collected, processed, transmitted, stored, or disseminated in general support systems and mainframe applications. Further, USDA Departmental Regulation (DR) 3140-2 requires that data exempted from disclosure through the Freedom of Information Act or whose disclosure is forbidden by the Privacy Act, will not be transmitted over the Internet network unless encrypted. DR 3140-1 requires that a logon-warning message be displayed notifying users that they have accessed a U.S. Government computer system and that unauthorized use may be punishable by fines or imprisonment.

Mainframe Access From the Internet

Allowing access to mainframe resources from the Internet without requiring users to go through the VPN exposes its mainframe to possible attack from Internet users. Further, NITC allows agency data, some of which may be protected by the Freedom of Information Act or Privacy Act, to be transmitted through the Internet without encryption. NITC currently has VPN support to access its resources over the Internet; however, there are no controls in place to require users to go through the VPN, which provides encryption of the data being transmitted. NITC is in the process of acquiring additional VPN capabilities, however due to the cost and time required to move all of its users to VPN access, it has not taken steps to require its use.

Warning Banner Does Not Exist on Mainframe Access Points

NITC does not have a warning banner on its mainframe access points, either from the Internet or from the USDA network. A warning banner is intended to notify users that they are about to access a U.S. Government system, that their access could be monitored, and that unauthorized access is punishable under Federal law. The U.S. Justice Department has pointed out the legal ramifications of not having a banner on Federal systems. In a legal conclusion written to the National Institute of Standards and Technology, the Justice Department stated that, “At a minimum, however, those individuals who are using computers without or in excess of their authority, and those authorized users who are subject to monitoring, should be told expressly that by using the system they are consenting to such monitoring.” Without this type of warning banner, NITC may find it difficult to prosecute unauthorized access into its systems.

RECOMMENDATION NO. 7

NITC should establish controls to ensure that users that access NITC resources from the Internet are required to connect through a controlled, secure manner

RECOMMENDATION NO. 8

NITC should post a warning banner on all system presentation screens to ensure that users acknowledge their access to a U.S. Government system and that their use implies consent of monitored use.

FINDING NO. 4

NITC HAS NOT ENSURED ITS COMPLIANCE WITH FEDERALLY MANDATED SECURITY GUIDELINES

Our review disclosed that the NITC draft "Overall Program Security Plan"[9] did not meet all the requirements of a General Support System Security Plan as prescribed by OMB Circular A-130 and NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems. In preparing its security plan, NITC followed OCIO's security plan guidance in effect at the time, which omitted these elements. OMB requires agencies to prepare a security plan to provide an overview of the security requirements of its systems.[10] Security plans should define who has responsibility for system security; who has authority to access the system; appropriate limits on interconnectivity with other systems; and security training of individuals authorized to use the system. In addition, USDA Departmental Manual 3140[11] requires each agency to submit an automated data processing security plan or an annual update to an existing plan to the OCIO.

The Office of Management and Budget (OMB), Circular A-130, Appendix III, Security of Federal Automated Information Resources, 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.

[9] At the time of our review, NITC had not finalized its security plan, but has since finalized its security plan.
[10] The Computer Security Act of 1987 also requires that security plans be developed for all Federal computer systems that contain sensitive information.
[11] DM 3140-1.1, Part 9

NITC's plan did not meet OMB requirements in that it did not include (1) a general description and purpose of the support system, including a list of all applications supported by the general support system; (2) a list of interconnected systems, the type of interconnections, and any concerns with those interconnections; (3) a description of the sensitivity of the information being handled, including any laws and regulations that affect the system, (4) rules of the system clearly delineating responsibilities and expected behavior of all individuals with access to the system; (5) planning for the lifecycle of the system and how security will be incorporated into that lifecycle; and (6) system authorization.

RECOMMENDATION NO. 9

NITC needs to ensure that its Security Plan includes all required elements.

FINDING NO. 5

NITC'S PERSONNEL CONTROLS NEED IMPROVEMENT

NITC does not have controls in place to ensure that employee background investigations are conducted, or that all employees have completed the required security awareness training. NITC does not follow Departmental guidelines, or OMB A-130 requirements regarding these personnel issues. As a result, NITC cannot be assured of the integrity of its security personnel, and cannot ensure that all employees have had the proper security training.

NITC's draft Overall Program Security Plan requires that all NITC Division Chiefs, Branch Chiefs, Staff Chiefs, Security Team, and the Directors Office have background investigations equivalent to Critical Sensitive that are renewed every 5 years. All other NITC employees shall have limited background investigations. The NITC Security and Analysis Staff is responsible for ensuring that background checks are carried out for all prospective NITC employees. We found that 2 of 10 security personnel have not had background investigations within the last 13 years.

Our review also determined that NITC does not maintain sufficient records of personnel training. The NITC Security Plan states it coordinates and conducts security awareness training, security reviews, and briefing of Federal, contractor, and vendor employees on facility security. OMB Circular A-130 requires that all individuals be appropriately trained in how

to fulfill their security responsibilities. NITC informed us that security training had been provided. Our discussions with several NITC personnel found that those individuals did not complete their fiscal year 2000 security awareness training, and that NITC had not maintained documentation showing that any NITC employee had completed the required security awareness training.

RECOMMENDATION NO. 10

NITC needs to establish controls to ensure that paperwork requesting employee background investigations is completed every 5 years.

RECOMMENDATION NO. 11

NITC needs to establish controls to ensure that all employees receive the required security awareness training and that documentation of the training is maintained.

ABBREVIATIONS

CFO	Chief Financial Officer
CIO	Chief Information Officer
GAO	U.S. General Accounting Office
IP	Internet Protocol
IT	Information Technology
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
TCP/IP	Transmission Control Protocol / Internet Protocol
USDA	U.S. Department of Agriculture
Y2K	Year 2000