U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

National Information Technology Center
General Controls Review – Fiscal Year 2005

Report No. 88501-2-FM
September 2005

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 21, 2005

REPLY TO
ATTN OF: 88501-2-FM

TO: David Combs
Acting Chief Information Officer
Office of the Chief Information Officer

THRU: Sherry Linkins
Office of the Chief Information Officer
Information Resources Management

FROM: Robert W. Young /s/
Assistant Inspector General
for Audit

SUBJECT: National Information Technology Center General Controls Review-Fiscal Year 2005

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, 2005. The audit 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. The report contains an unqualified opinion on the internal control structure and contains no recommendations. Therefore, no response from your office is necessary.

We appreciate the courtesies and cooperation extended during our audit.

Executive Summary

National Information Technology Center General Controls Review - Fiscal Year 2005

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, 2005. 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. The center has taken significant actions to mitigate the weaknesses we identified in prior audit reports. And while minor control issues are still being mitigated in the midrange environment, our report contains an unqualified opinion on the center's internal control structure as a whole.

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 OCIO/NITC's policies and procedures in place and operating effectiveness during the period October 1, 2004 through August 31, 2005; (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 testing to determine the status of corrective action on the issues identified in that report.

Our audit disclosed that the control objectives and techniques identified in exhibit A present fairly, in all material respects, the relevant aspects of OCIO/NITC's control environment taken as a whole. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the control objectives would be achieved and operating effectively.

Recommendation In Brief

Because of the actions OCIO/NITC has initiated and planned, we do not make any new recommendations in this report.

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

Table of Contents

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

Report of the Office of Inspector General

To: David Combs
Acting 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 OCIO/NITC's policies and procedures in place and operating effectiveness during the period October 1, 2004 through August 31, 2005; (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.

In our opinion, 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, 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, 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, 2004 through August 31, 2005. 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, 2005, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 2004, through August 31, 2005. 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.

/s/

ROBERT W. YOUNG
Assistant Inspector General
for Audit

August 31, 2005

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 OCIO/NITC's policies and procedures in place for the period October 1, 2004 through August 31, 2005; (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 Office of Inspector General (OIG) audits. We performed such tests as we considered necessary to evaluate whether the operating and control procedures described by OCIO/NITC and the extent of compliance with them are sufficient to provide reasonable, but not absolute, assurance that control objectives are achieved.

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

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
1. Define and communicate OCIO/NITC organizational structure, policies, and procedures.	a. OCIO/NITC relies on Department policy, in most matters, and provides hard copy and electronic access. b. When Department policy does not provide adequate guidance on administrative issues, OCIO/NITC issues internal Administrative Directives, which define administrative policies and procedures. c. Policy manuals, procedure manuals, and Administrative Directives are made available in electronic and hard copy form, and are used by personnel. d. The OCIO/NITC organizational structure and the responsibilities of OCIO/NITC divisions are well documented and understood. e. Division responsibilities, services, and procedures are documented. f. Adequate supervisory and approval levels exist in each OCIO/NITC functional area.	We reviewed OCIO/NITC policies and procedures to ensure: 1) Departmental policies had been taken into account. 2) They are revised, updated, and changed when necessary. 3) They were documented and appropriate. We reviewed the organization structure of OCIO/NITC divisions to ensure they were documented.	The control structure policies and procedures were suitably designed to achieve the control objective. Further, OCIO/NITC is in the process of updating all their security policies based on a detailed prioritization schedule. We found the overall organizational structure was suitably designed to achieve the control objective, and was operating effectively.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
2. Segregate duties between the specialized staff as much as practical.	a. OCIO/NITC is not responsible for Agency user operations or user, application, or data controls. b. The responsibilities of the OCIO/NITC staff and of the users of OCIO/NITC services are clearly differentiated. c. Separate duties are defined for the various technical specialties. d. OCIO/NITC personnel are prohibited from originating, changing, or correcting user input or data, unless so requested in writing. e. Separation of duty is enforced through access rules within the security software whenever practical and consistent with user requirements.	We reviewed OCIO/NITC level of service for various midrange servers/customers. We tested duties performed by OCIO/NITC system administrators on both NITC owned and customer midrange systems. We reviewed standard operating practices and directives for policies and procedures related to assignment of duties to NITC personnel. We reviewed access to critical operating system software data sets and compared settings to best practice standards. We reviewed user identifications (ID) with special access privileges. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness. We reviewed system settings and user rights on selected midrange environment servers.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. We identified one exception to adequate segregation of duties. Specifically, responsibility for review of the midrange platform logs rested with the midrange system administrators and was not segregated to an independent branch, such as OCIO/NITC security staff, for review. However, OCIO/NITC has contracted for implementation of a host-based intrusion detection system that will consolidate midrange platform logs into one file viewable only by the OCIO/NITC security staff. This system, once fully implemented, will mitigate this vulnerability.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
3. Apply appropriate controls to the system development life cycle.	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. b. The modification or installation of systems software requires the approval of OCIO/NITC management. c. Applications are well documented as they are being designed. d. Formal, standard control practices are followed in application design and development, and are reviewed for proper implementation. e. Customer approval of all report layouts, input formats, control reports, etc., is required.	We reviewed policies and procedures to ensure that departmental policies were considered. We reviewed internal policies and procedures to ensure that they are revised, updated, and changed when necessary and were properly implemented. We reviewed midrange software and firewall changes to determine if changes received documented authorization, review, and approval before implementation. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has initiated and planned actions to mitigate this weakness. We reviewed software changes to determine if testing is performed before changes are made to the midrange systems and firewalls. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has initiated and planned actions to mitigate this weakness.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. Further, OCIO/NITC is in the process of updating all their security policies based on a detailed prioritization schedule.
4. Provide reasonable assurance that new or modified applications systems and data files are properly converted and implemented.	a. Conversion procedures ensure proper cutoffs and conversion of data files. b. Testing is performed using only test data. c. Test results are documented and approved by the contracting customer before acceptance of a new system. d. Customers are involved in preparing the test data. e. As applicable, testing is performed on all interrelated systems to evaluate the integrity of those systems.	We reviewed policies and procedures to ensure that departmental policies were considered. We reviewed internal policies and procedures to ensure that they are revised, updated, and changed when necessary and were properly implemented.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. Further, OCIO/NITC is in the process of updating all their security policies based on a detailed prioritization schedule.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
5. Provide reasonable assurance that all software changes are appropriately reviewed and authorized.	a. Authorization and approval is required before modifications are made to the network, midrange server, office administration/local area network 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 reviewed by appropriate approving officials.	We reviewed software change policies to determine if adequate controls existed over modifications to the network, midrange servers, and mainframe operating systems. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness. We reviewed OCIO/NITC's information management system records to determine if midrange software and firewall changes were documented, approved before modification, and tracked to provide an audit trail. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness. We reviewed change records to determine if midrange and firewall changes were tested before being added to the production environment. This is a follow up issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
6. Conduct the planning activities needed to provide reasonable assurance that the OCIO/NITC will meet functional and control requirements.	a. Document current OCIO/NITC controls, and identify required new controls. b. To the degree possible, plan how OCIO/NITC will meet future Information System requirements. c. Ensure that sufficient capacity exists to meet peak demand.	We reviewed OCIO/NITC's internal controls framework and evaluated OCIO/NITC's Disaster Recovery Plan. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness. We interviewed OCIO/NITC personnel to determine future plans for securing various OCIO/NITC platforms.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively.
7. Access to the operating system, associated software, and documentation is restricted to authorized personnel.	a. Software system specialists are prohibited from initializing the operating system (except in the midrange environment where system administrators will initialize the operating system). b. Operational personnel are prohibited from making modifications to the operating system and software. Office administration/local area network is administered per memorandum of understanding and security staff oversight. 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. 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.	We reviewed system logging policies and procedures. We reviewed change management policies and procedures, and recently completed their information management records. 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. We attempted to review written access authorizations for persons with system administrator duties in the midrange environment.	The control structure policies and procedures were suitably designed to achieve the control objective. and were operating effectively. No written policies and procedures exist outlining midrange system logs that are to be reviewed or what actions to take for various security violations. Access to midrange servers were logged. However, as discussed in Control Objective 2, responsibility for review of the midrange platform logs rested with the midrange system administrators. See conclusion section for Control Object 2 for further information. Written access authorizations did not exist for system administrators in the midrange environment. However, OCIO/NITC immediately drafted a policy to control access and has taken steps to identify and restrict access to the midrange systems thereby mitigating these vulnerabilities. Special access privilege policies had been updated and user IDs with special access privileges had been limited.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
8. Provide reasonable assurance that operations staff operates automated equipment in accordance with the management criteria.	a. The procedures to be followed by technicians and librarians are thoroughly documented. b. Access to resources and data files is limited by security software to those required to do their work. c. On most USDA systems, critical and repetitive operations to maintain systems are automated using scheduling services and the mainframe operating system. c. Technician and librarian job responsibilities are defined in their position descriptions. d. The Daily Log/Shift Review is used to document and track operational events.	We reviewed critical data sets to determine if user IDs accessing these data sets were being logged. We reviewed system configuration in the midrange environment to determine if logging is maintained on the servers. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has initiated and planned actions to mitigate this weakness.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. Access to midrange servers were logged. However, as discussed in Control Objective 2, responsibility for review of the midrange platform logs rested with the midrange system administrators.
9. Provide reasonable assurance that equipment is used by authorized persons following prescribed procedures.	a. Access to the operations area and office is physically restricted through the use of a key badge system. The door system uses a proximity reader biometric fingerprint to prevent unauthorized access. Access to the operations area is further restricted through the use of a double door access point. b. Policies and procedures ensure that access to the operations area is highly restricted. This includes midrange server activities. c. Guards protect the NITC operations and office area 24 hours per day, 7 days a week. d. Continuously monitors NITC access control points and operational floor space through the use of differing video surveillance monitoring angles and alarm systems.	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. Reviewed documentation that NITC recertified individuals who require access to sensitive areas based on job function. Reviewed physical access to consoles to ensure access limited to only those individuals that require it to perform their job.	The control structure policies and procedures were suitably designed to achieve the control objective.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
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.	a. Interactive and batch access to resources and data files is controlled through management controls and the use of the security package. b. Access to sensitive regions and transactions is restricted. c. OCIO/NITC, on a monthly basis, suspends or deletes logon IDs that have been inactive for a designated period of time d. Security software is used to control user logon-ID and passwords. e. The OCIO/NITC creates only those login identifications requested by an agency security officer. f. All new logon IDs are created in suspend status. Agency security officers must unsuspend the logon ID and change the unknown password before it is usable. g. Special privileges must be requested and approved by the appropriate Information System Security Program Managers or management officials. h. Firewalls and intrusion detection control and detect activity.	We reviewed related policies and procedures and security software access controls over inactive user IDs. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness. 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. We reviewed related policies and procedures and security software access controls over special privilege user ID. We reviewed policies and procedures, reviewed firewall rules, and tested access controls over firewalls. We reviewed system configurations to ensure settings did not allow excessive user privileges. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
11. Data files are adequately protected from unauthorized modification or destruction.	a. OCIO/NITC is responsible for back-up and recovery of operating system software, which is completed on a fixed schedule. Customer agencies are responsible for back-up and recovery of their applications and data. The back-up tapes are stored at a secure off-site facility and can be retrieved in less than 2 hours. b. 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 back-up tapes off site at customer request and use the mainframe as a supplemental back-up media through IBM's Tivoli Storage Manager. c. Procedures are documented in the NITC Disaster Recovery Plans.	We performed testing in NITC's back-up procedures for the mainframe and firewalls. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness. We reviewed the most current Contingency/ Disaster Recovery Plans for OCIO/NITC Infrastructure Support, Mainframe and General Support Systems. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively.
12. Assess the vulnerability of OCIO/NITC to physical and other disasters, and put in place procedures for maintaining essential operations after such an occurrence.	a. Risk assessments are performed on OCIO/NITC systems. b. A Contingency Plan for Alternate Site Operations is in place. c. The OCIO/NITC facility is designed to survive numerous physical disasters with minimal damage. d. The USDA Internet Access network provides the physical medium for the OCIO/NITC wide area network.	We reviewed OCIO/NITC Disaster Recovery Plans. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
13. Evaluate and substantiate information technology controls on a regular basis.	a. Vulnerabilities are assessed on a regular basis through risk assessments, vulnerability assessments, and security testing. 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.	We interviewed OCIO/NITC officials to determine if all network devices were periodically scanned. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has effectively mitigated this weakness. We obtained and reviewed scan reports of selected systems. We interviewed OCIO/NITC security staff to determine the oversight of the security staff on the midrange environment. This is a followup issue from our NITC General Controls Review – FISCAL YEAR 2004 (Audit Report No. 88501-1-FM). NITC has implemented and planned actions to mitigate this weakness. We reviewed OCIO/NITC Disaster Recovery Plans. We reviewed firewall rules to ensure National Institute of Standards and Technology and OCIO guidelines were being followed.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. OCIO/NITC had updated their procedures to document all changes to the firewall in INFOMAN records. However, firewall rules implemented before NITC established its configuration management policy were not thoroughly documented. OCIO/NITC were in the process of implementing a commercially available software product that would correct this vulnerability. Network devices were scanned routinely.
14. Provide an appropriate level of personnel security and security awareness.	a. Ensure that OCIO/NITC staff and contractors have the appropriate level background investigation. b. Ensure terminated employees are disallowed access to NITC and NITC resources.	We reviewed procedures for removing physical access from separated employees. We reviewed policies and procedures, reviewed firewall rules, and tested access controls over firewalls.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. OCIO/NITC has adequate controls over timely removal of unneeded user accounts. As discussed in Control Objective 10, OCIO/NITC had limited access to the firewalls. Only one inappropriate account was identified and OCIO immediately deleted the account.