U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

National Information Technology Center
General Controls Review – Fiscal Year 2006

Report No. 88501-9-FM
September 2006

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 19, 2006

REPLY TO
ATTN OF: 88501-9-FM

TO: David M. Combs
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 2006

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 June 30, 2006. 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 2006 (Audit Report No. 88501-9-FM)

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 June 30, 2006. 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. Our report contains an unqualified opinion on the center's internal control structure.

Our objectives were to perform testing necessary to express an opinion about (1) whether the control objectives and techniques in exhibit A for the 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, 2005 through June 30, 2006; (2) whether this control structure of policies and procedures was suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily; and (3) the operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

Our audit disclosed that 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

We do not make any recommendations in this report.

Table of Contents

Report of the Office of Inspector General

To: David M. Combs
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, 2005 through June 30, 2006; (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, 2005 through June 30, 2006. 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 June 30, 2006, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 2005 through June 30, 2006. 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, 2006

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, 2005 through June 30, 2006; (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 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. g. Personnel policies encourage training and development to qualify personnel for their functional responsibilities.	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. We reviewed OCIO/NITC security related personnel policies and procedures to ensure employees have adequate training.	The control structure policies and procedures were suitably designed to achieve the control objective. We found the overall organizational structure was suitably designed to achieve the control objective and was operating effectively. We found 87 percent of the staff received training and documentation was maintained.

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, 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. f. Operations personnel are assigned fixed shifts.	We reviewed OCIO/NITC level of service for various mainframe and midrange servers/customers. We tested duties performed by OCIO/NITC system administrators on both NITC owned and customer mainframe and 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. We reviewed selected system settings and user rights on the mainframe and selected midrange environment servers. We reviewed responsibility for midrange platform logs to determine if our issue from our "NITC General Controls Review – Fiscal Year 2005" (Audit Report No. 88501-2-FM) was resolved. NITC has implemented a new system to consolidate midrange platform logs into one file viewable only by the OCIO/NITC security staff. NITC is implementing the software to mitigate 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
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. The installation/modification of midrange server operating systems hardware and software. Monitor security via commercial off-the-shelf software. Research security patches, fixes and virus alerts. d. Applications are well documented as they are being designed. e. Formal, standard control practices are followed in application design and development, and are reviewed for proper implementation. f. 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 selected change requests (including mainframe, midrange and firewall changes) to determine if (a) changes received documented authorization, review, and approval before implementation and (b) testing is performed before changes are made.	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
4. Provide reasonable assurance that new or modified applications systems and data files are properly converted and implemented.	a. Testing plans and approvals are tailored to meet the needs of the agency for whom the application is being built and are documented in the Agency Application Service Division Project Life Cycle Documentation Guide. b. Conversion procedures ensure proper cutoffs and conversion of data files. c. Testing is performed using only test data. d. Test results are documented and approved by the contracting customer before acceptance of a new system. e. Customers are involved in preparing the test data. f. 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.

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. There is thorough supervision and review of all changes. c. Problems and change requests to the operating system and software controlled by OCIO/NITC are tracked using manual and automated systems that provides an audit trail of system changes. d. Operating systems and systems software changes are tested to ensure that they operate properly and provide necessary functionality. e. Modified or new software is not installed until the appropriate approving authorities have reviewed change requests. f. Operational personnel are not involved in changes to the operating system (mainframe or midrange server) or user applications.	We reviewed software change policies to determine if adequate controls existed over modifications to the network, midrange servers, and mainframe operating systems. We reviewed selected change requests (including mainframe, midrange, and firewall changes) to determine if (a) changes received documented authorization, review, and approval before implementation and (b) testing is performed before changes are made.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. Further, OCIO/NITC continues to make improvements in its change management process.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
6. Conduct the planning activities needed to provide reasonable assurance that 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. To ensure smooth and efficient operations, OCIO/NITC generally does not install new versions of operating systems and key utilities until they have been generally available and tested in our test logical partitioning for a sufficient period of time for vendors to correct problems. d. 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. We reviewed both mainframe and Financial Data Warehouse (FDW) midrange disaster recovery tests which were conducted during our review. 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.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
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. In that environment, system administrators are responsible for initializing 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 selected 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 reviewed 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. Access to midrange servers were logged. We reviewed OCIO/NITC's approach to reviewing logs and determined that better segregation of duties was occurring. OCIO/NITC was not able to readily identify privileged access users for servers within the midrange environment. OCIO/NITC developed a mechanism to better track this security. We identified several mainframe access privileges for which OCIO/NITC was not regularly reviewing access. OCIO/NITC immediately updated its special access privilege policies and user IDs and multiple accesses were removed.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
8. Provide reasonable assurance that operations staff operates automated equipment in accordance with the management criteria.	a. An OCIO/NITC manual details processes and procedures performed to maintain operational stability and accessibility, to all mainframe systems and their associated resources, along with actions and monitoring required for normal automated operations. The manual is available online or in printed formats. In the midrange server environment, backup schedules and administration tasks are documented within spreadsheets, news groups and also available on-line. b. The procedures to be followed by technicians and librarians are thoroughly documented. c. Access to resources and data files is limited by security software to those required to do their work. d. On most systems, critical and repetitive operations to maintain systems are automated using scheduling services and the mainframe operating system. The exception is prior to and during the weekend maintenance period when technicians are required to perform system backups in preparation of scheduled maintenance. e. Technician and librarian job responsibilities are defined in their position descriptions. f. 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 mainframe and midrange environment to determine if logs are maintained and reviewed.	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
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 OCIO/NITC operations and office area 24 hours per day, 7 days a week. d. Continuously monitors OCIO/NITC access control points and operational floor space through the use of differing video surveillance monitoring angles and alarm systems.	We reviewed and observed access to critical resources and the use of guards, key badges, and biometric devices utilized to control access to restricted areas. We reviewed documentation that NITC recertified individuals who require access to sensitive areas based on job function. We 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. We reviewed security tapes from the OCIO/NITC facility and identified several issues regarding building access. OCIO/NITC reviewed our findings, provided explanations, and where appropriate, identified changes to be made in its policies and procedures.

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. OCIO/NITC creates only those logon IDs 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. The appropriate Agency Data Base Manager or staff generally controls database access. h. Special privileges must be requested and approved by the appropriate Information System Security Program Managers or management officials. i. The passwords for hot-site and emergency logon IDs are changed regularly, and kept in secure locations. j. Security software is used to control user output and session activity. k. Firewalls and intrusion detection control and detect activity.	We reviewed related policies and procedures and security software access controls, including those for inactive user IDs and special privilege user IDs. 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 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.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively.

FDW: Provide reasonable assurance that only approved users have access to FDW 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. OCIO/NITC creates logon IDs requested by an agency security officer. c. Security software is used to control user logon ID and passwords for the mainframe FDW. d. All new logon IDs are created by OCIO/NITC with random passwords. Agency security officers assign the user ID, an initial password and notifies user. The initial password is set to expire, which forces the user to change the password. e. The appropriate Foundation Financial Information System personnel generally control data base access. f. The passwords for emergency logon IDs are changed regularly, and kept in secure locations. g. Security software is used to control user logon IDs and passwords for the FDW.	We reviewed related policies and procedures and security software access controls, including those for inactive user IDs and special privilege user IDs. We reviewed password settings to ensure adequate controls have been implemented over user IDs and passwords.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. OCIO/NITC was not able to readily identify privileged access users (including system administrators) for servers within the midrange environment. OCIO/NITC developed a mechanism to better track this security.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
11. Data files are adequately protected from unauthorized modification or destruction.	a. OCIO/NITC is responsible for backup and recovery of operating system software, which is completed on a fixed schedule. Customer agencies are responsible for backup and recovery of their applications and data. The backup 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 backup tapes off site at customer request and use the mainframe as a supplemental backup media through IBM's Tivoli Storage Manager. c. Procedures are documented in the NITC disaster recovery plans.	We reviewed NITC's backup procedures for the mainframe, midrange and firewalls. We reviewed the most current contingency/disaster recovery plans for OCIO/NITC Mainframe and FDW midrange.	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
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 physical disasters with minimal damage. d. The USDA Internet Access network provides the physical medium for the OCIO/NITC wide area network. This network uses Universal Telecommunications Network.	We reviewed OCIO/NITC disaster recovery plans. We reviewed both a mainframe and FDW midrange disaster recovery tests which were conducted during our review.	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. 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 mainframe and midrange environment. 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.

CONTROL OBJECTIVE	CONTROL TECHNIQUES	TESTS PERFORMED	CONCLUSION
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. c. Ensure that employees and contractors receive security awareness and training.	We reviewed procedures for removing physical access from separated employees.	The control structure policies and procedures were suitably designed to achieve the control objective and were operating effectively. OCIO/NITC had adequate controls over timely removal of unneeded user accounts.

NATIONAL INFORMATION TECHNOLOGY CENTER

Service Center Description

June 30, 2006

USDA NATIONAL INFORMATION TECHNOLOGY CENTER

Service Center Description

8930 Ward Parkway
Kansas City, MO 64114
Phone 888.USE.NITC • Fax 816.926.2804

Introduction

The National information Technology Center (NITC) is part of the Office of the Chief Information Officer (OCIO) for the United States Department of Agriculture (USDA). The mission of NITC is to *provide reliable and cost-effective Information Technology Solutions to achieve effective mission performance delivery for the USDA, its agencies, and others.*

The NITC headquarters is located in Kansas City, Missouri, with other service centers located in Fort Collins, Colorado, Washington, D.C., and Beltsville, Maryland. The NITC supports the missions of the USDA offices and agencies, which includes the Farm Service Agency (FSA), Rural Development (RD), Natural Resource Conservation Service (NRCS), Forest Service (FS), and non-USDA agencies including the Federal Aviation Administration (FAA), General Services Administration (GSA), Treasury Department, United States Coast Guard, and Department of Interior (DoI). The NITC specializes in Enterprise Information Technology Solutions that includes products, services, and resources.

Our Enterprise Solutions are developed utilizing government and industry standards. Our computing facilities use "leading edge technology" products, develop solutions using "best of breed" industry services, and provide proficient physical and professional resources for business continuity capability, consistency, and reliability. The NITC secure IT infrastructure consists of platforms for mainframe Complementary Metal Oxide Semiconductor (CMOS) based (Operating Systems – IBM z/OS, IBM z/VM, IBM UNIX System Services SUSE zLinux), midrange RISC based (Operating Systems – IBM AIX, HP-UX, Sun Solaris), and micro Intel/AMD based (Operating Systems – Windows Server, Windows Datacenter, RedHat Linux) computer environments. Our customers access NITC facilities from their remote locations throughout the continental United States via secure private and public networks to support their business requirements and services. The programs and applications deployed in the NITC environment are national in scope, mission critical, and important for the operations of the United States Government.

The NITC cooperatively partners with customers to understand their business and requirements. This results in NITC providing the technical resources, the professional expertise, and the IT processing environments critical to the success of their applications.

Our vision, *"The NITC team is committed to excellence in providing world-class leadership through innovative, reliable Information Technology services and enterprise solutions in support of our valued customers"* with emphasis on delivering timely and within budget support for our clients while remaining responsive to the issues and challenges facing our customers today, tomorrow, and in the future. Our employees maintain a high level of professionalism in partnering with our valued clients. We are proud of our reputation for excellent customer service, a high level of customer satisfaction, and continually striving to improve and enhance our offerings.

Centralized Services

The NITC operations are seven days a week, twenty-four hours a day, all year long. Our services are 100 percent reimbursable by our customers through competitive billing rates.

In 1972, the NITC introduced centralized computing services to USDA agencies. The centralized computing economies of scale propelled the NITC into a leading edge operation, which serves 70,000+ nationwide users. The NITC 64-bit architecture mainframes deliver 1,983 million instructions per second (MIPS). The systems provide reliable interactive processing using over 500 commercial off-the-shelf (COTS) programs and applications. The NITC assures the confidentiality, integrity, and availability of 65-Terabyte of mainframe data stored on direct access storage device (DASD) disk storage. The NITC enterprise scaleable Storage Area Network (SAN) has 105-Terabyte of secured disk data storage. NITC administrative services include data storage management, security administration, backup tape inventory management, technical support, and contingency disaster recovery planning.

The NITC supports an Open System hosting infrastructure. The platforms include IBM, HP, SUN, DELL and several others. With customer partnership, the NITC leverages the centralized data warehouse and database economy of scale. The NITC Open System services include application and database administration; help desk; system integration; and technical documentation. The NITC infrastructure compliments the mid-range open system diversity.

NITC offers multi-platform application, database development and maintenance. In addition to database administration and help desk, other capabilities include testing, system integration across multiple operating systems, and technical documentation. NITC continues to evolve an IT infrastructure design to compliment the market diversity and scope of system environments.

The NITC's configuration, incident, change, and problem management are maturing. Already established configuration baselines, streamlined configuration processes, and configuration management process documentation have been refined. The NITC is evaluating best practice automation solutions for more efficient operations.

The NITC incident and problem management processes are maturing. Incident visibility improved resource response and root cause analysis, which reduced service interruptions. All organizations experience incidents that either impact or threaten to impact normal business operations. As NITC's business has become more dependent on IT services, the need to react quickly and effectively to any incidents that adversely affect our IT services or infrastructure has become paramount. Utilizing the incident management process that is being built to ITIL standards, NITC ensures that all support resources are focusing on the issues that have the greatest urgency and impact on the business operations.

Telecommunications

NITC Communications Network consists of the following multiple networks with the capability to support a wide range of user requirements. NITC supports all Secure TCP/IP based protocols.

Services:

Internet, Public Access Network (DMZ)

The NITC maintains a TCP/IP routed network to service Public accessible midrange and mainframe servers. Features include the following:

Firewall Protection

Load Balancing (Local and Global Server)

High Availability (Local and Global Server)

Intranet, USDA Only Network

The NITC maintains a TCP/IP routed network to service USDA only accessible midrange and mainframe servers. Features include the following:

Firewall Protection

USDA Backbone Accessible

Extranet, Trusted Business Partner Network

The NITC maintains a TCP/IP routed network to service customers private network connections (customer owned circuits) terminating at NITC. Features include the following:

Firewall Protection

WAN and LAN Accessible

The NITC has mainframe based communications subsystems supported by our Telecommunications Software Specialists.

Storage Management

The National Information Technology Center (NITC) Technology Operation and Services Division (TOSD) Storage Management Branch (SMB) is responsible for data life cycle management. The NITC operates an enterprise mainframe storage environment and two open systems enterprise storage area networks (SAN). Disk and tape data storage consumption is 650-Terabyte. Asynchronous remote mirroring to the NITC's Beltsville, Maryland facility is a NITC SAN feature. The remote mirroring data replication SAN feature is a popular open system disaster recovery solution. A dual high-speed fibre network links customer servers to SAN disk and tape subsystems. The tape subsystem is a dedicated automated tape library (ATL/SILO). The silo has 575 high-speed tape cartridge slots and 16 high-speed tape drives.

The mainframe enterprise storage strategy exploits the System Managed Storage (SMS) features. Other mainframe storage features include system master data set and user catalogs, Data Facility Hierarchical Storage Manager (DFHSM), Data Facility Storage Management Subsystems (DFSMS), Aggregate Backup and Recovery Support (ABARS), and Data Facility Dataset Services (DFDSS). The mainframe disk and tape data storage consumption is 400-Terabyte.

Backup strategies include incremental, weekly, and monthly backup rotations. The customer has access to backup utilities, controls their dedicated backup process, and may designate one or more backup sets as disaster recovery critical data. File restoration utilities are available for the customer to initiate file recovery without involving other sources. A dedicated automated tape library (ATL SILO), which utilizes high-capacity high-speed tape drives, services the level 2 DASD data migration practice and the virtual tape cache migration policy.

The NITC utilizes a virtual tape control system (VTCS) and host software component (HSC) software, which virtualizes tape volumes and tape transports. The hardware for virtual storage manager (VSM) is the Virtual Tape Storage Subsystem (VTSS) RAID 6+ device with micro code that emulates 128 tape transports. The implementation benefits the NITC and its customers with reduced risk of data loss or data corruption. Operational benefits include faster tape processing, better tape and tape drive reliability, and environmental savings.

The NITC offers offsite data tape storage service. The mainframe tape management program and the bar code reconciliation process are the inventory control processes. The off site storage facility offers numerous levels of data security, excellent disaster response strategy, and interfaces with the NITC's inventory management process.

Security practices limit and strictly control access to data and storage media. The NITC internal controls practices mitigate or eliminate the risk to data confidentiality, integrity, and availability.

Contingency Planning/Disaster Recovery

NITC has a contingency management program that provides an alternate computing environment that would be available for customers to operate mission critical processes in the event of a disaster. Disaster recovery service and support varies by customer. The NITC has 14 years of contingency planning experience; follows industry best practices in managing its disaster recovery requirements; and can assist in designing a disaster recovery service that will meet the specific needs of the customer.

Disaster recovery exercises for mainframe systems are conducted twice a year at the emergency relocation facility (ERF). Customers are encouraged to participate in the semi-annual events and are notified well in advance of the exercise dates so that they may identify test objectives, review recovery plans, and plan their resources for the exercises.

Disaster recovery exercises for midrange systems are scheduled and coordinated on an individual basis. Disaster recovery hardware must be in place at the emergency relocation facility before testing may take place. System and database administration may also be provided during recovery exercises. The NITC also offers rapid recovery to customers subscribing to the storage area network (SAN) through a data mirror. Data residing on SAN storage is mirrored to the emergency relocation facility. A secured telecommunication link connects the primary facility to the emergency relocation facility during normal operations. In the event of a disaster, the network traffic is redirected to the emergency relocation facility and operations continue at the ERF. These redirection procedures are tested during a customer's exercise.

Vital data needed for disaster recovery is duplicated at the customer's request, and is stored at a secure off-site location. In the event of a disaster, the NITC will ensure that customer vital data is transported to the emergency relocation facility and is staged for the customer to begin recovery of their critical systems.

A well-designed test, training and exercise program is essential in building a disaster recovery program that will serve customers in a COOP event. The NITC is committed to partnering with our customers to facilitate an effective contingency planning and disaster recovery program.

Applications and Development Services for Enterprise Solutions

The National Information Technology Center's (NITC) Agency Applications Services Division (AASD) provides comprehensive application life-cycle support services to USDA agencies and other federal clients. NITC offers a full-range of information technology applications and development services that enable customers to accomplish their missions. These offerings are carefully tailored to our customers' requirements, and ranges from analysis, research and conceptual development – through design, build, and implementation – on to operations, maintenance, and user help desk support.

NITC professional services staff works personally and cooperatively with our customers in order to give individualized attention to their needs. Project teams are typically comprised of dedicated personnel and customer staff. A team of project management expertise as well as IT consultant skills consistently provides high-quality deliverables that meet customer goals.

NITC has remarkable success with this philosophy and has steadily grown with improved efficiency over the years. Projects that have been developed and maintained with this team philosophy have received numerous awards. In addition, this philosophy has allowed NITC to develop and nurture long-standing customer relationships. This has resulted in our staff being able to provide our customers with durable, intimate knowledge, and understanding of their missions and subject matter.

NITC personnel are its most valuable asset. Our work force's foundation is a team of experienced, professional Information Technology specialists. Our surge capacity and short-term specialized skill requirements are met by utilizing a number of in-place support services contracts. This enables NITC to remain extremely competitive with private sector consulting companies and provide customers with a stable federally based work force. We understand the environments in which our customers work, and strive to help them accommodate legal requirements, policies, directives, and scarce resources as best we can.

NITC's management is dedicated to maintaining and improving the technical expertise it offers to customers. Training and project experiences are continuously provided to our staff. This ensures that we will be ready and able to help our customers design and implement the most technically current and effective solutions. In addition to preparing for the future, we maintain a solid foundation in the knowledge required to keep legacy systems finely tuned and executing reliably.

NITC assures a comprehensive and integrated approach to systems development, maintenance, and support on a variety of NITC and customer-owned platforms. This is accomplished by incorporating all areas of systems, database, applications and documentation disciplines.

NITC's development strategies and project management provide the flexibility to respond to changing customer requirements and it provides access to other architectures and tools for delivering a variety of quality products and services to customers, including:

Applications Design, Development and Support

Database Management and Support

Web Site Development and Management

Systems Re-engineering and Integration

Integrated Testing on Multiple Hardware Platforms

Enterprise Wide Applications

Technical Information Services

Web-enabling Legacy Applications

eGovernment Applications Support

Internet Applications Development

NITC Technical Expertise

Architectures

- Mainframe
- Client/Server
- Internet Web Servers
- MS Windows
- z/OS
- VM
- Linux (SUSE, RedHat)
- Unix System Services
- IBM-AIX
- HP-UX
- Sun Solaris

Databases

- Oracle
- Sybase
- Informix
- MS Access
- System 2000
- MS SQL
- mySQL
- SQL Server
- DB2
- CA-IDMS
- Adabas

Languages	Tools and Middleware
COBOL	Oracle Designer 2000
Visual Basic	Oracle Developer 2000
JAVA, J#	Power Designer
JAVAScript	System Architect
HTML	ESRI Map Server
XML	Crystal Reports
C, C++, C#	Hot Metal
Cold Fusion	WebSphere Studio
SQL, PL/SQL	Visual Studio
Perl, OraPerl	JBuilder
PHP	MX Studio
Unix Shell Script	Apache
SAS	TOMCAT
SAS/C	WebLogic
	Dreamweaver
	Rational Application Developer
	Rational Web Developer
	Filenet
	Stellant

Migration and Consolidation Experience

The National Information Technology Center (NITC) has been at the center of every major workload consolidation and relocation within the Department of Agriculture since 1988. Collectively, our staff has an enormous amount of years of experience in computer systems migration work. Most of it obtained through implementing NITC enterprise data center consolidation projects.

In 1988, the NITC built a conversion system image of the workload of the Washington Computer Center and successfully cut over the operation on a weekend. This project saved USDA from $40 million over five years.

In 1991, consolidation of a Unisys workload from the Fort Collins Computer Center progressed over an 18-month period. Activity involved creation of a mirror image and migration, then conversion, of 2.5 million lines of Unisys application code to the NITC IBM environment. This effort saved customer agencies approximately $33.4 million over the following 4 years.

Again in the early 1990's, NITC used the mirror image approach to migrate electronic mail and switched voice services of its own and its customers from Sprint to AT&T. NITC designed and implemented a dual network architecture, which ran in parallel for 18 months until all customers were migrated successfully.

During 1991-92, NITC managed a conversion project, which moved a production processing workload for several customers from the Honeywell to the IBM environment. Savings realized from this move were estimated at $1 million annually.

In May of 1997, the Federal Aviation Administration (FAA) awarded an outsourcing multiyear contract for the Integrated Computing Environment - Mainframe and Network (ICE-MAN) workload to NITC. ICE-MAN encompasses essential administrative functions for the FAA, including personnel, financial, and aviation safety information systems. Using a very aggressive project management approach, FAA and NITC worked together from July through November and over a long weekend successfully relocated the ICE-MAN operation to NITC from the previous contractor site.

During 2002-03, NITC successfully migrated from mainframe to midrange open system environment and migrated the financial database warehouses.

In June of 2003, the NITC successfully migrated the Farm Services Agency's (FSA) WebFarm to the Data Center in Kansas City, MO. The FSA's WebFarm consisted of 120 midrange servers using MS Windows operating system, tape library, tape backup equipment, routers, switches, and associated hardware. The migration was completed in two (2) weeks and fully operational.

Lessons learned in these efforts were considerable. Drawing upon this experience, the NITC can accomplish a partial or total relocation of workload with a proven record for managing all aspects of the project. Some areas where significant cost savings can be realized in your organization include the following:

- Physical infrastructure consists of maintenance of raised floor space, uninterruptible power source components. We have 7x24x365+ environments for customers' mid-range platforms, including Linux, HP, IBM, and Sun Solaris systems.

- Investment and maintenance costs for hardware, software, and telecommunications connections at the mainframe.

- Personnel costs.

Additional benefits include license leveraging, centralized technical support, feasibility to contract for offsite processing, potential for a greater selection of software, and an improved environment for data sharing.

Project Management Office

The National Information Technology Center (NITC) Project Management Office (PMO) is responsible for project management, new business management, customer account management, and marketing.

In the area of project management, primary goals of the PMO are to establish standard processes, tools, and templates to support project management throughout the organization and to train and mentor new and existing project managers. The PMO also provides project managers for both internal and customer projects. A number of the PMO staff are certified Project Management Professionals.

The New Business Relationship Management function in the PMO manages new business opportunities from both new and existing customers. For existing business, the PMO provides dedicated Account Managers that serve as the primary point-of-contact (POC) for the customer. The Marketing Program Manager is responsible for all aspects of the NITC marketing program.

Enterprise Shared Services

Enterprise Shared Services (ESS) is a suite of development aids, platforms, and applications that facilitate USDA's department-wide effort to deliver citizen-centric, online information and services. USDA developed ESS to leverage business, technology, and data principles to provide agencies the capability to maximize efficiencies and reduce costs while improving customer service. The business applications are hosted in a shared environment at the National Information Technology Center (NITC) using controlled IT hosting and operations procedures designed to support applications on the Enterprise Shared Services infrastructure.

ESS allows customers to develop and implement new or existing applications with development aids, different platforms and various application integration options. Procedures are in place to assist and improve USDA application stability, efficiency and quality of service-

Development Aids are also available for use, such as, templates, Web Standards and Guidelines, and a developer library. Using Web Standards and Guidelines improves site usability, increases consistency in look and feel, and creates a professional and engaging online presence. Developer Library allows access to reusable components and frameworks to reduce time, effort, and costs while developing an application using ESS.

Information Technology (IT) platforms are available for different development requirements. ESS uses Stellent's Web Content Management solution to streamline Web content delivery using reporting and workflow capabilities. IBM's WebSphere Hosting Platform is utilized to support non-portal specific application development. The IBM WebSphere portal configured J2EE Application Development platform is used to improve efficiency and reduce costs of application creation using portal technologies. FileNet's document management solution is used to create, edit, and publish documents and content to web sites and applications using document management and workflow capabilities.

Application Integration Options are available through the use of eAuthentication, Common Employee Database, Google Search Appliance, and AgLearn. eAuthentication is the single, centralized authentication service for web-based applications throughout USDA. The Common Employee Database (CED) is the centralized meta-directory of employee information for use by USDA agencies and systems. Google is available to integrate search engine capabilities with agency applications. USDA's learning management system, AgLearn, provides the capability to create and host a training course for an ESS application.

Security

The NITC security program is a major supporting function of the overall mission intended to ensure appropriate protections of the information resources. We strive to provide a secure and safe environment for clients to access, store and process their mission critical information. We also develop, implement, maintain and administer security measures to achieve a logical, structured, and comprehensive security posture and ensure privacy requirements are met in accordance with Federal and OCIO security policies and best practices.

Physical Security:

The NITC has a multi-tiered physical security concept deployed to restrict access to sensitive equipment and information. The first level of security restricts site access to unauthorized vehicles by directing all vehicular traffic through three security gates. The gates are designed to prevent unauthorized passage of vehicles and have been rated to stop large vehicles, such as fully loaded tractor-trailers. The second level of security restricts building access. The building exterior is lighted and under constant closed-circuit television surveillance. Armed Security Officers regularly patrol and monitor the complex and parking areas. The third level restricts access to sensitive interior areas of the building with the use of fingerprint scanning technology with biometric devices.

Environmental Safeguards:

The NITC Operations area is protected by a dual source fire suppression and extinguishing system. The fire detection and alarm system continuously monitor the operations area via several hundred detection devices positioned throughout the space. NITC has built an electrical power supply system with multiple redundancies. Three commercial power feeders, from two separate substations, supply the NITC electrical distribution center. Uninterruptible Power Systems (UPS) condition the incoming power to ensure that sensitive computer related equipment is supplied with clean electrical power. Integral to the UPS are battery back-up systems. In the event of a loss of commercial power, three emergency power Diesel Driven Generators (DDG) automatically supply power to sensitive computer equipment and all required support systems (i.e. HVAC, lighting).

Personnel Clearances:

The NITC employees and contractors have security clearances, appropriate for the position, ranging from Limited Background Investigation (LBI) to Top Secret. Strict policies limit access to the building, the computer room, the telecommunications room, and other facilities.

NITC Capabilities

Products

Client/Server
COTS Software (500+)
Database Architectures
eGovernment
Enterprise Systems Environments
Enterprise Total Solutions
Firewall Technology
Internet
Intranet
Mainframe
Middleware
Midrange
Multiple Languages
Networks
On-Line Transaction Processing
Operating Systems
Security Technology
Storage Area Networks (SAN)
Telecommunications
Tools
Virtual Tape
Web Access

Services

Application Analysis
Application Development
Application Maintenance
Bronze Level Service
Configuration Management
Contingency Planning
Continuity/Uptime
Curriculum Development
Data Security
Database Administration
Database Design
Database Development
Database Management
Disaster Recovery
Facility Management
Gold Level Service
Hardware Support
Installations
Intrusion Detection
Intrusion Scanning
IT Management and Development
IT Strategic Planning (AS-IS/TO-BE)
Life Cycle Management
Managed IT Solutions Hosting
Network Management
Operations Management
Procurement Assistance
Re-engineering
Secured Operating Environment (24/7)
Security Administration
Silver Level Service
Software Conversion
Software Migration
Storage Management Services
System Certification
System Engineering
System Integration
Tape Backups
Training
Troubleshooting
Turn Key Solutions
Web Application Development
Web Site Development
Web Site Management

Resources

24/7 Operations
508 Compliant
Application Support
Capacity/Performance Tuning
Certification and Accreditation
Consulting
Diesel Generators
Dry Pipe Sprinkler System
Dual Power Feed
Environmental Safeguards
Hot Site Recovery
Industry "Best of Breed" Practices
Industry Standards Applied
Leading Edge Technology
Life Cycle Support
NITC Help Desk (24/7)
Off Site Storage
Program Management
Project Management
Secure Facilities
Security Program Management
Software Support
System Testing
Uninterruptible Power Supplies

Benefits

Account Managers
Cost Savings/Incentives
Customer Notification System
Customer Satisfaction
Customized Solutions
Managing Your FUTURE
Maximum Systems Uptime
Minimized Administrative Logistics
MOU/Task Order Process
On-Line Billing Information
Program Management Control
USDA Incident Reporting System

NATIONAL INFORMATION TECHNOLOGY CENTER

NITC Website: www.ocio.usda.gov/nitc

Business Contact: 888-USE-NITC