U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

National Information Technology Center
General Controls Review – Fiscal Year 2007

Report No. 88501-10-FM
September 2007

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 27, 2007

REPLY TO
ATTN OF: 88501-10-FM

TO: Charles R. Christopherson, Jr.
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 2007

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, 2007. 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 commonly referred to as a Statements on Auditing Standards 70 audit. The report contains an unqualified opinion on the internal control structure and contains no recommendations.

If you have any questions, please call me at (202) 720-6945, or have a member of your staff contact Steve Rickrode, Director, Administration and Finance Division, at (202) 720-1918.

Executive Summary

National Information Technology Center General Controls Review - Fiscal Year 2007 (Audit Report No. 88501-10-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, 2007. 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 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 procedures necessary to express opinions about whether (1) OCIO/NITC's description of controls in exhibit A presents fairly, in all material respects, the aspects of OCIO/NITC's controls that may be relevant to a customer agency's internal control as it relates to an audit of financial statements; (2) the controls included and/or referenced were placed in operation and suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and customer agencies applied the controls contemplated in the design of OCIO/NITC's controls; and (3) the controls we tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified were achieved during the period from July 1, 2006, through June 30, 2007.

Our audit disclosed that the control objectives and techniques identified in exhibit A presented 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, were suitably designed to provide reasonable assurance that the control objectives would be achieved and were operating effectively.

Recommendation In Brief

We do not make any recommendations in this report.

Abbreviations Used in This Report

ASSERT	Automated Security Self-Evaluation and Remediation Tracking
C&A	certification and accreditation
ID	Identification
IT	information technology
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OCIO	Office of the Chief Information Officer
PIA	Privacy Impact Assessments
POA&M	Plan of Action & Milestones
RFP	Request for Procurement
SAC	Special Agreement Check
SFUG	Security Features User Guide
ST&E	Security Test and Evaluation
USDA	U.S. Department of Agriculture

Table of Contents

Executive Summary ..... **i**

Abbreviations Used in This Report ..... **ii**

Report of the Office of Inspector General **1**

Exhibit A – Office of Inspector General, Review of Selected Controls **3**

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

Report of the Office of Inspector General

To: Charles R. Christopherson, Jr.
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 whether (1) the accompanying description of control objectives and techniques of the USDA's OCIO/NITC presents fairly, in all material respects, the aspects of OCIO/NITC's controls that may be relevant to a customer agency's internal controls as it relates to an audit of financial statements; (2) the controls included had been placed in operation as of June 30, 2007; and (3) such controls were suitably designed to achieve the control objectives, if those controls were complied with satisfactorily, and customer agencies applied the controls contemplated in the design of OCIO/NITC's controls. 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 that had been placed in operation as of June 30, 2007. Also, in our opinion, the controls included or referenced in exhibit A were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and customer agencies applied the controls contemplated in the design of OCIO/NITC's controls.

In addition, we performed tests to obtain evidence regarding the effectiveness of specific controls in meeting the control objectives included in exhibit A during the period from July 1, 2006, to June 30, 2007. The specific controls and the nature, timing, extent, and results of our tests are identified in exhibit A. This information has been provided to customer agencies and their auditors to be taken into consideration, along with information about the internal control at customer agencies, when making assessments of control risk for customer agencies. In our opinion, the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in exhibit A were achieved during the period from July 1, 2006, through June 30, 2007.

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 customer agencies.

The control objectives and techniques at OCIO/NITC are as of June 30, 2007, and information about tests of the operating effectiveness of specific controls covers the period from July 1, 2006, through June 30, 2007. 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 fraud 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 customer 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 27, 2007

The objectives of our examination were to perform testing necessary to express an opinion about whether (1) the Office of the Chief Information Officer/National Information Technology Center's (OCIO/NITC) description of controls in exhibit A presents fairly, in all material respects, the aspects of OCIO/NITC's controls that may be relevant to a customer agency's internal control as it relates to an audit of financial statements; (2) the controls included and/or referenced were placed in operation and suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and customer agencies applied the controls contemplated in the design of OCIO/NITC's controls; and (3) the controls we tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified were achieved during the period from July 1, 2006, through June 30, 2007.

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 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 were achieved.

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

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	OCIO/NITC follows the U.S. Department of Agriculture (USDA) and the National Institute of Standards and Technology (NIST) guidelines for access control policies and procedures. OCIO/NITC's security directive establishes a "least privilege" mode of operation for its staff and contractors. OCIO/NITC provides management of accounts through authorizations, approvals, and reviews. OCIO/NITC provides further control through the documentation and implementation of separation of duties. OCIO/NITC also employs system settings to provide additional access controls. These include limiting unsuccessful login attempts, displaying warning banners, session locks, and session termination.	We reviewed various OCIO/NITC documents regarding the management of information system accounts. We examined recent change records supplied by OCIO/NITC in the form of e-mail confirmations from agencies served by OCIO/NITC to determine account review status and frequency. We examined documents supplied by OCIO/NITC indicating implementation of access enforcement, discretionary access control. We reviewed various types of documentation to ensure separation of duties and least privilege access. We interviewed and observed system administrators to ensure lockouts occurred after a defined number of unsuccessful login attempts. We reviewed samples of system use notification banners to ensure the information system displays an approved system use notification message before granting system access. We interviewed and observed system administrators to ensure system timeouts and/or session termination occurred after a defined period of inactivity.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
			We examined documentation for evidence of organizational reviews and documentation of incidents and general user activity. We examined sample output from mainframe systems to ensure automated marking of documents is in use. We interviewed OCIO/NITC staff to determine if remote access occurred through secure methods.	
Awareness and Training	Organizations must (1) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (2) ensure that organizational personnel are adequately trained to carry out their assigned information security related duties and responsibilities.	The OCIO/NITC Information Security Program includes security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In this regard, the OCIO/NITC security directive for security awareness training requires new employees and contractor personnel to complete security awareness orientation before they are given access to OCIO/NITC computer systems.	We compared a listing of employees/contractors who completed AgLearn security training to a listing of all employees/contractors employed by OCIO/NITC to verify staff had completed required security training.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
	.	The OCIO/NITC security directive for security awareness training also requires employees to complete annual security awareness training to renew their awareness of their security responsibilities. OCIO/NITC requires employees and contractors to complete annual security awareness training that addresses basic USDA computer security concepts.		
Audit and Accountability	Organizations must (1) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (2) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	OCIO/NITC follows NIST and USDA guidelines and has supplemented with an OCIO/NITC specific security directive for audit and accountability. The OCIO/NITC security directive for audit and accountability states that administrators/system owners will (1) ensure security related events are recorded in the system log, (2) ensure that the system logs are routinely reviewed, and (3) notify the Chief Security Staff of any actual or suspected security incident revealed during reviews. It also provides that the security staff will (1) randomly review system logs, (2) investigate reported	We reviewed various documents to determine if log files were created and reviewed. We reviewed audit logs to ensure appropriate information was captured.	OCIO/NITC controls were suitably designed to achieve the control objective but were not operating effectively. However, compensating access controls mitigate the risk to OCIO/NITC systems. Additionally, OCIO/NITC is in the process of procuring software, hardware, maintenance, and training required for implementing a centralized Security Information and Event Management solution.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		incidents, (3) maintain record of the reviews made by security staff, and (4) assist administrators/system owners with analyzing the system logs.		
Certification, Accreditation, and Security Assessments.	Organizations must (1) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application, (2) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems, (3) authorize the operation of organizational information systems and any associated information system connections, and (4) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	OCIO/NITC follows USDA certification and accreditation (C&A) procedures which require an independent Security Test and Evaluation (ST&E) to determine the effectiveness of the security controls on the information technology (IT) system and the designated approving authority to decide whether or not to authorize the system for processing based on the ST&E results and residual risk. This accreditation decision, along with the supporting documentation and rationale, are documented in the final accreditation package. OCIO/NITC has a security directive that defines required documentation for the accreditation package. In addition, OCIO/NITC uses weaknesses identified from audits, reviews, self assessments, and the related corrective actions to document and track plan of action and milestones (POA&M). POA&Ms are tracked by	We obtained and reviewed ST&Es that were recently performed to ensure testing was based on NIST Special Publication 800-53. We obtained and reviewed Interconnection Security Agreements between OCIO/NITC and other organizations to determine if agreements were in place for external systems connecting to OCIO/NITC. We reviewed documentation to determine if POA&Ms were documented and monitored.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		the security staff and Project Management Office. OCIO/NITC reviews and updates System Security Plans and Privacy Impact Assessments (PIA) in addition to Annual Self Assessments.		
Configuration Management	Organizations must (1) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles and (2) establish and enforce security configuration settings for IT products employed in organizational information systems.	OCIO/NITC has an administrative directive that requires changes to the configuration of OCIO/NITC owned systems be approved by OCIO/NITC management prior to implementation, and that testing, customer coordination, and other key activities be documented. OCIO/NITC management approval is required for any changes. Baseline configuration of the information system is documented as part of the C&A process. Additionally, component information is maintained in an asset management database, and component and software information is maintained in Configuration Management Information Tracking System. OCIO/NITC uses a Cisco Security Agent client configured for monitoring system logs and program libraries for Windows systems and Computer Associates Examine for the mainframe to restrict access when changes are being implemented.	We interviewed OCIO/NITC Configuration Management personnel to determine if significant changes had been made to OCIO/NITC Configuration Management policies and procedures. We reviewed the system baseline documentation to ensure configurations were properly documented. We obtained and reviewed change requests for several systems to ensure changes were documented, reviewed, and approved. We reviewed samples of Configuration Control Board and Executive Review Board meeting minutes to determine if changes were reviewed and decisions to approve/disapprove were made. We reviewed firewall and router documentation to determine if port use was properly configured and documented. We obtained and reviewed inventory lists to determine if components of the information system and relevant ownership information were maintained.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		Additionally, the OCIO/NITC systems are configured according to OCIO/NITC configuration guides, which are built on NIST and USDA guidelines which document the functions, ports, and protocols that are allowed.		
Contingency Planning	Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.	OCIO/NITC follows planning policy and procedures provided by OCIO Cyber Security. Contingency plans for OCIO/NITC systems address roles, responsibilities, contact information, and activities associated with restoring the system after a disruption or failure are in place. The plans are updated and tested at least annually. The USDA Mainframe General Support System plans are tested twice each year. OCIO/NITC backs up user-level and system-level information (including system state information) contained in the information system nightly and stores backup information in a secured alternate site. Two alternate processing sites have been identified (1) a contracted hot site in Boulder, Colorado, and (2) a second OCIO/NITC site in Beltsville, Maryland. Both are used for the resumption of mission critical functions.	We reviewed various plans related to contingency planning for the enterprise, network, infrastructure support system, midrange UNIX, Customer Information Management System, and mainframe. We reviewed disaster recovery test results to verify tests performed and training participants. We reviewed documentation related to off-site storage and alternate processing sites.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
Identification and Authentication	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.	OCIO/ NITC follows identification and authentication policy and procedures provided by OCIO Cyber Security and NIST guidelines. OCIO/NITC also has implemented a Personnel Security Plan and an additional security directive which provides guidance on passwords. These guidelines and directives assist OCIO/NITC in managing access to its systems. OCIO/NITC also has an administrative directive that defines the revocation process of identifiers. OCIO/NITC requires unique user identity and authentication for access to its systems. Identification and authentication of devices is also required for access to resources.	We obtained and reviewed policies and procedures related to identification and authentication of information system users and devices. We reviewed and verified baseline configurations. We observed logins to ensure passwords were not displayed.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.
Incident Response	Organizations must (1) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (2) track, document, and report incidents to appropriate organizational officials and/or authorities.	OCIO/NITC follows Cyber Security incident response policy and procedures as described in Departmental regulations. OCIO/NITC is developing policies and procedures to formally document OCIO/NITC controls. Information system security incidents are tracked and documented based on procedures in Departmental regulations.	We obtained and reviewed policies and procedures for Incident Response. We reviewed security training information to determine if personnel were trained in incident response roles and responsibilities. We reviewed incident response reports to determine if incidents were accurately and promptly reported.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		OCIO/NITC promptly reports incident information to OCIO Cyber Security.	We interviewed staff to determine who provides advice and assistance to users and administrators.	
Maintenance	Organizations must (1) perform periodic and timely maintenance on organizational information systems; and (2) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	OCIO/NITC follows maintenance policies and procedures provided by OCIO Cyber Security and NIST guidelines. OCIO/NITC schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. Hardware maintenance processes are included in hardware contracts. Software maintenance procedures and upgrades are included in software contracts. Access to OCIO/NITC systems is monitored, and both physical and logical access is controlled. OCIO/NITC utilizes "phone home" connections to vendors for diagnostic activities. Additionally, personnel authorizations are documented in the OCIO/NITC *Personnel*	We examined several documents regarding maintenance of hardware and software. We examined the remote administration systems regarding responsibilities, review of system logs and documentation, and the method of communication used by the system. We examined policy documents regarding procedures for authorizing staff to perform maintenance and the circumstances allowing access. We examined purchase order documents for the maintenance of information system hardware.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		Security Plan. Background checks are performed on all workers. Visitors to controlled areas are escorted.		
Media Protection	Organizations must (1) protect information system media, both paper and digital, (2) limit access to information on information system media to authorized users, and (3) sanitize or destroy information system media before disposal or release for reuse.	OCIO/NITC follows policies and procedures provided by OCIO Cyber Security and NIST guidelines. OCIO/NITC also has a security directive which provides for additional control for protection, control, and disposal of documents, media, and other sensitive materials. Access to storage of media is restricted to authorized personnel. Sanitation of equipment and media prior to disposal or reuse is enforced through OCIO/NITC's security directive. All information is treated as though it is sensitive.	We reviewed security directive documentation for verification of system and system media categorization and control. We reviewed security directive and control documentation for verification of system media sanitization and control.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
Physical and Environmental Protection	Organizations must (1) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (2) protect the physical plant and support infrastructure for information systems; (3) provide supporting utilities for information systems; (4) protect information systems against environmental hazards; and (5) provide appropriate environmental controls in facilities containing information systems.	OCIO/NITC follows physical and environmental policies and procedures provided by OCIO Cyber Security and NIST guidelines. In addition to those guidelines, OCIO/NITC has a physical security plan and procedures included within their general controls that documents physical control details. OCIO/NITC keeps up-to-date lists of personnel with authorized access using the facility security system, known as On-Guard, to control access and issue badges. Access to restricted computer operations is granted through an OCIO/NITC administrative directive. All physical access points, including access to systems, are controlled by On-Guard and guards. For systems in the data center, physical access is recorded on digital video recorders. Visitors must present proper Identification (ID), sign a log, and wear a visitor's badge. OCIO/NITC employs various equipment to physically protect the information systems. This includes an uninterruptible power supply that provides constant power, sprinkler system in the office spaces	We reviewed policies and procedures related to physical and environmental protection. We reviewed employee lists and access lists and other documentation to verify access and annual reviews of access. We tested the functionality and observed proper operation of card readers and cameras. We interviewed staff regarding the monitoring of physical access to the facility and access log documentation. We reviewed samples of video taken from three access points. We reviewed the administrative policy regarding the verification and admittance of visitors to information systems areas. We obtained and examined the documentation for maintenance/testing of the uninterruptible power supply, fire suppression system, and temperature and humidity controls. We examined policy and documentation regarding control of information systems items entering and exiting the facility.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		and a fire suppression system in the data center, temperature and humidity level monitoring, and employing master shutoff water valves. Information system-related items entering and exiting the facility are controlled by the System Network Control Center, who maintains appropriate records of those items.		
Planning	Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.	System security plans are reviewed and updated by the system owner annually or whenever a significant change to the systems, facilities, or other conditions occurs. The security staff directs and manages a security program, which is documented in the *OCIO/NITC Security Plan*. The Plan is reviewed and updated as needed, at least annually. OCIO/NITC develops and distributes *Security Features User Guides* (SFUG) for each system. SFUGs are updated as systems evolve. Each worker, both Federal and contracted, must read and sign a user agreement, which outlines rules of behavior before they are allowed access to OCIO/NITC information systems. PIAs are documented for each system, following	We reviewed security plans, SFUGs, and PIAs for Customer Information Management Systems, Infrastructure Support System, Network, and Mainframe. We reviewed selected signed user agreements for employees/contractors.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives. .

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		USDA and NIST guidelines. The PIAs are updated annually.		
Personnel Security	Organizations must (1) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions, (2) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers, and (3) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.	OCIO/NITC has a formal, documented personnel security plan that addresses purpose, scope, roles, responsibilities, and compliance. A risk designation is assigned to each position, and is documented in the *OCIO/NITC Personnel Security Plan*. All workers, both Federal and contracted, must complete a favorable Special Agreement Check (SAC) which includes a Federal Bureau of Investigations fingerprint check. All Federal and contract employees are given a Federal Protective Service check and/or a SAC prior to having access to the facility, and further background checks are completed to establish the correct level of security clearance commensurate with the position they occupy. OCIO/NITC also has an administrative directive which is utilized for each employee who leaves OCIO/NITC whether it is through removal, termination, reassignment, or retirement. Federal and contract personnel must read and sign a user agreement before they are allowed	We obtained and reviewed *Personnel Security Policy and Procedures*. We obtained and reviewed a personnel listing to verify status of background investigations/ reinvestigations. We reviewed the System User ID check list and request to remove access to verify departing is out processed correctly. We reviewed contractor statements of work to ensure personnel security requirements were properly identified and documented.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		access to the OCIO/NITC information systems. Personnel Security requirements are also part of all statements of work for all third-party providers.		
Risk Assessment	Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	OCIO/NITC performs risk assessments as part of the security management process. Currently, OCIO/NITC follows USDA and NIST guidelines for risk management policies and procedures. Final risk determinations and related management approvals are documented and maintained in the Department's Automated Security Self-Evaluation and Remediation Tracking (ASSERT) database. The information systems are categorized as part of the security management process using the system categorization tool within the ASSERT system. Risk assessments are performed as part of the security management process following USDA and NIST guidelines. OCIO/NITC conducts risk assessments every 3 years per USDA and NIST guidance or when there has been a major change to the system or its environment. Vulnerability scans are performed monthly on appropriate systems. Ad-hoc scans can be run if	We reviewed risk assessments to ensure systems were properly categorized. We reviewed the scan database.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		new vulnerabilities are identified.		
System and Services Acquisition	Organizations must (1) allocate sufficient resources to adequately protect organizational information systems; (2) employ system development life cycle processes that incorporate information security considerations; (3) employ software usage and installation restrictions; and (4) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization. .	OCIO/NITC complies with software usage restrictions mandated by USDA Departmental memoranda. The rules are enforced through signed user agreements. In addition, all OCIO/NITC personnel must complete annual "Ethics" and "Security" training. OCIO/NITC also includes requirements for employing adequate security controls in all Statements of Work for all third-party providers.	We reviewed user agreements to verify software usage restrictions were documented. We reviewed the Request for Procurement (RFP) for the off-site storage vendor to ensure that physical and personnel related security controls were documented.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.
System and Communications Protection	Organizations must (1) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (2) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	Each OCIO/NITC information system is responsible for ensuring unauthorized and unintended information transfer does not occur. A security directive implemented by OCIO/NITC establishes the security boundaries and responsibilities of OCIO/NITC and its customers. OCIO/NITC separates publicly accessible information system components through the use of firewalls and separate network nodes. OCIO/NITC employs various integrity checking	We interviewed staff to determine if information systems prevent unauthorized and unintended information transfer via shared system resources. We interviewed staff to ensure the external boundary is properly protected. We interviewed staff to determine the integrity of transmitted information. We interviewed and observed system administrators regarding network disconnections.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.

NIST Control Area	Control Objective	Control Activities	Tests Performed	Conclusion
		methods, depending on the system to ensure the integrity of data transmissions. Network disconnects are also utilized to provide additional system and communication protection.		
System and Information Integrity	Organizations must (1) identify, report, and correct information and information system flaws in a timely manner; (2) provide protection from malicious code at appropriate locations within organizational information systems; and (3) monitor information system security alerts and advisories and take appropriate actions in response.	OCIO/NITC identifies flaws through several processes, including scans, assessments, audits, and the security management process. Flaws are reported and corrected using POA&Ms, which are tracked in the ASSERT tool. OCIO/NITC receives information system security alerts from the Federal Computer Incident Response Center, OCIO Cyber Security, and from vendors regularly, and responds appropriately. Each OCIO/NITC information system verifies the correct operation of security functions based on its capabilities.	We obtained and reviewed documentation of the subscription to security alert systems. We reviewed and verified system administrators input related to the verification of operation of security functions.	OCIO/NITC controls were suitably designed and operating effectively to achieve the control objectives.