U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

# Audit Report

## Office of the Chief Information Officer – Management and Security Over Information Technology Convergence – Common Computing Environment

Report No. 50501-3-FM
October 2005

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington DC 20250

October 24, 2005

REPLY TO
ATTN OF: 50501-3-FM

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

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

FROM: Robert W. Young /s/ Tracy LaPoint (for)
Assistant Inspector General
for Audit

SUBJECT: Office of Chief Information Officer - Management and Security Over Information Technology Convergence –Common Computing Environment

This report presents the results of our audit of the management and security over information technology convergence common computing environment. The report identified weaknesses in the Office of the Chief Information Officer (OCIO) - Information Technology Services' (ITS) ability to effectively manage and secure information technology. OCIO-ITS has reportedly taken significant actions to address the weaknesses we identified.

Your response to our draft report is included in its entirety in exhibit B, with excerpts incorporated in the Findings and Recommendations section of the report. Based on the information provided in the response, we have reached management decision for Recommendations 3, 5, 6, 7, 8, 10, 11, 12, 15, 16, 17, and 18. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer. For Recommendations 1, 2, 4, 9, 13, and 14, additional actions are needed to reach management decision. OCIO-ITS did not respond to the recommendations as presented and needs to provide additional information to reach management decision. Please refer to the OIG Position sections of the report for specific details.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation of the outstanding recommendations noted above. Please note that the regulation requires management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

We appreciate the courtesies and cooperation extended to us during the audit.

# Executive Summary

***Office of the Chief Information Officer – Management and Security Over Information Technology Convergence – Common Computing Environment (Audit Report No. 50501-3-FM)***

## Results in Brief

In recent years, the Department has co-located field offices of the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD) into one-stop U.S. Department of Agriculture service centers to provide seamless, quality customer service to farmers and rural residents. A key element for the success of this Service Center Modernization Initiative is the replacement of aging business and technology systems through Information Technology (IT) Convergence, that will allow FSA, NRCS, and RD, collectively referred to as the Service Center Agencies (SCA), to share data among themselves and their customers, and to streamline business processes. Additionally, IT convergence provides the infrastructure needed to ensure that customers can conduct business electronically with the SCAs.

The convergence process shifted the management and security responsibilities of the network operating environment from those individual SCAs to the Department's Office of the Chief Information Officer (OCIO), Information Technology Services (ITS). Our objective was to determine whether ITS and the SCAs had adequately implemented security within the common computing environment (CCE).

Overall, we found that ITS was beginning to implement controls over the weaknesses we identified in our audit. Many of the control weaknesses identified were caused by a lack of communication and oversight among ITS and the SCAs throughout the convergence planning and implementation process.[1] Consequently, the CCE network and systems may be exploitable, jeopardizing the integrity of the SCAs' data and ITS' system resources.

The following summarize the weaknesses we identified:

- OCIO certified and accredited the two systems we selected for review without any significant restrictions or limitations despite the fact that documents supporting the certification and accreditation (C&A) were either missing or contained inaccurate or incomplete data. OCIO did not have adequate controls in place to ensure that the documentation supported the accreditation. As a result, significant risks may have gone unidentified, and the effectiveness of existing controls may not have been fully tested. Reliance on the C&A as a tool to manage risk

[1] Formal conversion became effective in November 2004.

could create a false sense of security and leave the CCE susceptible to potentially exploitable risks.

- ITS does not have finalized operating procedures. Instead, ITS field personnel have relied on SCA operating procedures in place prior to convergence. Further, ITS had not established a formal procedure for drafting, commenting, or finalizing operating procedures and other policy documents.

- ITS implemented a memorandum of understanding (MOU) and Incidental Transfer Agreement that were too overarching to hold either ITS or the SCAs accountable for adequate security. Further, only two of the three agency representatives had signed the final MOU. As a result, clear lines of authority or accountability have not been established for carrying out security.

- ITS did not have an accurate inventory of computer equipment on the CCE network, including equipment owned by SCA partner entities. ITS field employees did not have the access authority to enter or modify inventory records in its equipment tracking system. Additionally, ITS had not implemented policies or written agreements with the SCAs regarding whether computer equipment purchased with SCA funds could be connected to the network, how it would be tracked, or who would be responsible for its security. At many locations we visited, we were unable to locate equipment recorded in its inventory records. ITS cannot effectively manage the risk of the entire CCE network without adequate tracking of computer equipment on the network, whether or not owned by ITS.

- ITS had not begun periodic scanning of the CCE network and SCAs had ceased their scanning activities after convergence in November 2004. ITS had not established policies, procedures, or controls to ensure scanning was performed. Our review disclosed that (1) a large number of risk indicators that may be exploitable, and (2) system policy settings did not provide for optimum security and were not uniform throughout the CCE network. Therefore, ITS' systems and networks may be vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of SCA applications and data.

- ITS was not prepared to take over controlling access to the CCE at the time of convergence and had allowed each SCA to continue with its current policy. Those policies were inconsistent with one another and did not provide effective security for the entire network. We identified users on the ITS network that had access privileges exceeding what they needed to perform in their assigned

responsibilities. ITS had not implemented its own access policies and controls within CCE. As a result, ITS and the agencies that it serves had reduced assurance that only authorized users had access to the CCE network and that they had access to only those network resources they need to perform their job.

- ITS had not implemented adequate physical and environmental controls over sensitive computer equipment at many of the CCE locations we visited. Discussion with SCA field office personnel disclosed that they were generally unaware of good security practices and ITS field personnel took limited steps to correct obvious weaknesses. As a result, ITS and the agencies it serves, have reduced assurance that computer resources are adequately protected from physical and environmental vulnerabilities.

**Recommendations In Brief**

We recommend that OCIO-ITS:

- Establish policies, procedures, and controls to ensure that the documentation supporting the C&A process is prepared in accordance with prescribed departmental and other Federal guidance and that the results of the review support the assessment.

- Establish clear policies and procedures for all activities and functions it has assumed, and ensure that they are not contradictory with existing policies.

- Conduct a complete inventory of items attached to the CCE network and establish policies and controls to ensure that the CCE inventory remains up-to-date.

- Establish policies, procedures, and controls to ensure that system vulnerabilities are timely identified and mitigated.

- Establish policies and controls to ensure that all employees are granted access that adheres to the concept of least privilege.

- Negotiate separate MOUs or Service Level Agreements (SLA) with each SCA, and establish policies and controls to ensure that the MOUs or SLAs are reviewed periodically and updated as necessary.

**Agency Response** OCIO-ITS generally agreed with the findings and recommendations in this report. Its response is presented in its entirety as exhibit B.

**OIG Position** We were able to reach management decision on Recommendations 3, 5, 6, 7, 8, 10, 11, 12, 15, 16, 17, and 18. Our position on what is needed to reach management decision on Recommendations 1, 2, 4, 9, 13, and 14 is outlined in the findings and recommendations sections of the report.

## *Abbreviations Used in This Report*

| | |
|---|---|
| ASAAR | Agency System Access Authorization Request |
| BPD | Bureau of Public Debt |
| C&A | Certification and Accreditation |
| CCE | Common Computing Environment |
| CIO | Chief Information Officer |
| COTR | Contracting Officer Technical Representative |
| EATS | Equipment Acquisition Tracking System |
| FSA | Farm Service Agency |
| GAO | U.S. Government Accountability Office |
| GIS | Geographic Information Systems |
| GSS | General Support System |
| ID | Identification |
| IO Lab | Interoperability Lab |
| ISA | Interconnection Security Agreement |
| ISSPM | Information System Security Program Managers |
| IT | Information Technology |
| ITA | Incidental Transfer Agreement |
| ITS | Information Technology Services, a division of the OCIO |
| MOU | Memorandum of Understanding |
| NIST | National Institute of Standards and Technology |
| NITC | National Information Technology Center |
| NRCS | Natural Resource Conservation Service |
| OMB | Office of Management and Budget |
| PMA | Performance Management Program |
| PROP | USDA's Personal Property Management System |
| RD | Rural Development |
| SAAR | System Access Authorization Request |
| SCA | Service Center Agency |
| SLA | Service Level Agreement |
| SLM | Service Line Manager |
| ST&E | Security Test & Evaluation |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| OCFO | Office of the Chief Financial Officer |
| OCIO | Office of the Chief Information Officer |
| OCIO/CS | Office of the Chief Information Officer/Cyber Security |
| OIG | Office of Inspector General |
| USDA | U.S. Department of Agriculture |
| VPN | Virtual Private Network |

## Glossary

Certification and Accreditation – A process mandated by the Office of Management and Budget Circular No. A-130 requiring that IT system controls be documented and tested by technical personnel and given the formal authority to operate by an agency official.

Network – Two or more computers connected to one another by a common communication standard.

Risk Indicators – In the context of this audit, system configuration or programming weaknesses, as identified by our scanning software that may pose a threat to the system scanned or the network of computers.

Physical Access Controls – Processes or activities that physically limit access to computer systems or networking devices. For instance, locking rooms where systems are stored.

Environmental Controls – Processes or activities that provide the optimum operating environment for computer systems and networking components. For instance, air conditioning systems that keep systems from overheating.

Local Area Network – A group of computers located in a small geographical area (such as a single office building) connected by a common communication standard.

Major Application – One or more related applications that support a critical function of the agency and/or that contains data considered sensitive by law.

Service Center Agency – Comprised of Rural Development, the Farm Service Agency, and the Natural Resources Conservation Service, three agencies of the U.S. Department of Agriculture. These agencies are generally co-located in service centers throughout the rural areas of the United States and provide the loan and conservation assistance to farmers and other eligible rural residents.

Security Testing and Evaluation – One phase of the certification and accreditation where an independent party evaluates and conducts testing of the controls established in and around a system. The purpose is to determine whether controls as stated in the system documentation are adequate and operating as prescribed.

Transmission Control Protocol/Internet Protocol – A suite of communication protocols (or rules) originally developed by the U.S. Military, but later adopted worldwide as the standard for the global Internet.

Dial-up – The process by which computers communicate via telephone lines. Both computers need a device called a Modem to convert data into sound, transmit across standard telephone lines, and convert back to data.

Virtual Private Network – The process of transferring data across public communication lines, typically the global Internet, using common protocols and encryption to maintain the confidentiality and integrity of the communications.

# Table of Contents

# Background and Objectives

## Background

Implementation of the Information Technology (IT) Convergence began in 1998 and most of its major hardware and software components are in place. It has already helped the Department implement new Farm Bill programs accurately and in a timely manner. The 2004 budget focused on realizing the full potential of the IT Convergence by funding critical investments in Geographic Information Systems (GIS). GIS promises to transform the way the Service Center Agencies (SCA), and other U.S. Department of Agriculture (USDA) agencies, do business by allowing the agencies to analyze data on land and soils electronically. For example, customers will be able to view USDA information on their land over the Internet rather than visiting the office, and soils analysis that now takes days or weeks to map by hand will take only minutes. Printing, distribution, storage, and manual updating of hard copy maps in the service centers can be eliminated.

The IT Convergence was built on a common IT investment strategy, common telecommunications capability, common office automation tools, common administrative applications, and a common IT support organization. The purpose of the IT Convergence is to:

- Optimize Data Sharing
- Optimize Equipment Sharing
- Optimize People Sharing

The IT Convergence is built on a basic infrastructure that includes network servers at each service center, desktop and portable workstations, peripherals and other related equipment, and modern commercial software that provides basic automation capabilities to field staffs.

The IT Convergence includes public access servers to provide general information of USDA services to customers and GIS data servers at State offices to make spatial information available to service center staff. The technology has been structured to provide flexibility to adapt to changes in both the IT field and the business requirements of the partner agencies. This is necessary because IT is changing at an ever-faster pace and the business of the partner agencies change frequently with new legislation.

The Office of the Chief Information Officer (OCIO) is responsible for the management of the IT Convergence for the SCAs. Complementing efforts to modernize and standardize the SCAs' technology, the Department is also taking steps to integrate the IT support functions of the SCAs into a single organization, called Information Technology Services (ITS), and will

examine whether further administrative efficiencies can be gained in these agencies.

ITS is a new organization within OCIO that incorporates the infrastructure roles of the Farm Service Agency (FSA), the Natural Resource and Conservation Service (NRCS), and the Rural Development (RD) mission area. ITS provides IT infrastructure support for the national, State, and local program delivery aspects of FSA, NRCS, and RD, including each agency's primary partners. This new organization reports to an Associate Chief Information Officer within the USDA's OCIO and is accountable to the Chief Information Officer.

## Objectives

Our objectives were to determine whether (1) ITS and SCAs had adequately implemented security within IT Convergence/common computing environment (CCE), (2) assess controls existed between ITS and the SCAs, (3) clear roles and responsibilities were defined, and (4) policies were in place governing IT Convergence/CCE operations.

# Findings and Recommendations

## Section 1. Management Oversight and Documentation

Clearly documented policies and procedures, and explicit roles and responsibilities are core elements of any internal control structure as required by the U.S. Government Accountability Office (GAO). Further, the certification and accreditation (C&A) process established by the Office of Management and Budget (OMB) should be used by agencies as a tool to manage the risk to its critical information systems. Information Technology Services (ITS) management is responsible, as a service provider for the Service Center Agencies (SCA) and as a component of the Office of the Chief Information Officer (OCIO), for ensuring that internal controls, including information security controls, are adequately designed and documented, and effectively implemented on an ongoing basis.

### Finding 1 — Certifications and Accreditations Marginally Effective as Management Tools

Two of the four ITS C&A packages we reviewed related to the common computing environment (CCE) disclosed a significant number of weaknesses compared to the requirements of guidance issued by the Department, the National Institute of Standards and Technology (NIST), and OMB.[2] Despite the inadequate C&A documentation, the systems were accredited and granted an authorization to operate without any significant restrictions or limitations. Controls to ensure the C&A process was conducted properly and in a timely manner were inadequate. Accreditations were rendered although the process was incomplete and poorly documented. Thus the C&A, intended to provide reliance that systems were materially free of significant security weaknesses, were of only limited utility. Therefore, significant risks may have gone unidentified and mitigated, and the effectiveness of controls may not have been fully tested. Reliance on the C&A as a management tool to manage risk could create a false sense of security and leave the CCE susceptible to potentially exploitable risks.

OMB[3] and NIST[4] guidance require an agency official to attest to the adequacy of an information system's security safeguards. Specifically, each

[2] We were provided a total of four C&A packages related to the CCE; however, we selected only two of those for review.
[3] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.
[4] NIST Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004.

agency's Chief Information Officer (CIO) must authorize in writing the use of each general support system (GSS) and major application used to process, store, or transmit information. Security accreditation is the official management decision, given by a senior agency official, to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.[5] The accreditation decision is to be based on management, operational, and technical controls detailed in a comprehensive evaluation, or certification, that provides the necessary information for the agency CIO to formally declare that a system is approved to operate. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation. In December 2003, OCIO issued the "U.S. Department of Agriculture (USDA) Certification and Accreditation Guide" to facilitate a comprehensive and uniform approach to the C&A process within USDA agencies.

Comparison of the two C&A packages we selected against a list of required documentation in the Department-issued C&A guide disclosed that the C&A packages did not include the "Configuration Management Plan" and "Interconnection Memoranda of Understanding." Additionally, while a single "Privacy Impact Assessment" and "Security Features User's Guide" covering all four C&A platforms existed, these documents did not address issues explicit to the two systems under review. The "Privacy Impact Assessment" stated that because the SCAs' applications and data remained the inherent responsibility of the respective SCA, no Privacy Impact Assessment needed to be completed.[6] However, ITS needs to work with SCA officials to ensure that, collectively, Privacy Act protected data is adequately maintained and transmitted. Further, due to the unique operating environments of the four platforms (network, telecommunications, data warehouse, and WEB farms) a single "Security Features User's Guide" was too generic. Finally, a Disaster Recovery Plan was completed for the Interoperability Lab (IO Lab) and the WEB farms but not for CCE. Because the C&A packages were completed prior to convergence, we could not always determine exactly why the documentation was not included in the C&A packages.

Additionally, our review of the Security Test & Evaluation (ST&E) Reports and the Risk Mitigation Plans disclosed significant weaknesses. The Risk Mitigation Plans for the two systems we reviewed disclosed a significant

[5] Risks to individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.
[6] The SCAs are the Farm Service Agency (FSA), the Natural Resource and Conservation Service (NRCS), and the Rural Development (RD) mission area.

number of risks for which no one was assigned responsibility to correct or mitigate, and no estimated correction date had been established.

Further, ITS accepted and closed, on a formal risk acceptance report, five security risks identified for the CCE network based on planned activity. ITS should not have accepted a risk based on future plans for implementing mitigating controls. For example, ITS' justification for acceptance of missing out-of-date security updates stated, "The identified updates are on schedule for completion. The patches/updates are not identified as being critical to CCE." However, ITS' risk acceptance justification does not describe how it determined that these security patches/updates were not critical to CCE. Instead of accepting the risks based on planned activities, ITS should have kept the risks open until mitigating controls were implemented and tested for effectiveness.

In addition, ITS accepted several more risks to the CCE network on the Risk Mitigation Plan that were in direct violation of regulations and Federal guidance. For instance, ITS accepted the risk that administrative and other users had excessive privileges to access systems within the CCE network. ITS rated this risk as "low" and accepted the risk. (See Finding 6.) Department regulations require that system owners limit users' access to the minimum necessary, and NIST guidance stresses the principle of "least privilege" - the concept that users have access to only the information and systems for which they need to perform their duties.

We also questioned the "medium" risk classification of the CCE/IO Lab as documented in the System Security Plan. NIST Federal Information Processing Standard 199 requires that the lowest overall classification that can be given is the highest classification of data or applications residing on or communicating with that system. Since several applications used by the SCAs, as well as data maintained by the SCAs, are classified as "high," ITS should have classified the CCE network as high as well.

The following tables identify other discrepancies with the C&A risk assessment and contingency planning documents.

| Risk Assessment Requirements[7] | CCE/ IO Lab | WEB Farm |
|---|---|---|
| Has the scope of the system, in terms of both system boundaries and areas to be assessed, been explained? | No | |
| Is the information infrastructure explained? | No | No |

[7] These criteria were derived from NIST SP 800-30, "Risk Management Guide for Information Technology Systems," and the "USDA Risk Assessment Methodology Guide." (Grayed-out boxes indicates the document met NIST Guidance requirements for that element.)

| Risk Assessment Requirements[7] | CCE/ IO Lab | WEB Farm |
|---|---|---|
| Has the IT assets to be assessed been identified? | No | |
| Has the data flow been explained? | No | No |
| Has the interface to other systems been explained and identified? | No | No |
| Has the software and hardware components been identified? | | No |
| Has the system security architecture been explained and identified? | No | |
| Has the system security architecture, which depicts the operating system, been explained and identified? | No | |
| Has the system security architecture, which examines the facilities where the system is contained, been explained and identified? | No | |
| Has the system security architecture, which explains the information storage requirements been explained and identified? | No | No |
| Has the applicable system security policies governing the system (agency policies, Federal requirements, laws, etc.) been explained and identified? | No | |
| Has value of the information been determined? | No | |

| Contingency Plan Requirements[8] | CCE/ IO Lab | WEB Farm |
|---|---|---|
| Are critical data files and operations identified and the frequency of file backup documented? | No | No |
| Are resources supporting critical operations identified? | No | No |
| Have processing priorities been established and approved by management? | No | No |
| Is the plan approved by key affected parties? | No | No |
| Are responsibilities for recovery assigned? | | No |
| Are there detailed instructions for restoring operations? | No | |
| Is there an alternate processing site; if so, is there a contract or interagency agreement in place? | No | No |
| Is the location of stored backups identified? | No | No |

[8] These criteria were derived from NIST SP 800-26, "Security Self Assessment Guide for Information Technology Systems." (Grayed-out boxes indicates the document met NIST Guidance requirements for that element.)

| Contingency Plan Requirements | CCE/ IO Lab | WEB Farm |
|---|---|---|
| Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? | No | No |
| Is system and application documentation maintained at the off-site location? | No | No |
| Are all system defaults reset after being restored from a backup? | No | No |
| Are the backup storage site and alternate site geographically removed from the primary site and physically protected? | No | No |
| Has the contingency plan been distributed to all appropriate personnel? | No | No |

Despite these weaknesses, the systems were accredited and granted authorization to operate without any significant restrictions or limitations. As a result, significant risks may have gone unidentified and mitigated, and the effectiveness of controls may not have been tested. Therefore, reliance on the C&A as a management tool to manage risk could create a false sense of security and leave the CCE susceptible to potentially exploitable risks.

### Recommendation No. 1

OCIO should rescind the unlimited accreditation for the two ITS systems we reviewed and place them in an interim approval to operate status pending the resubmission of an accurately completed C&A package for each system. OCIO-ITS should also review the C&As of its other systems for similar weaknesses and make the necessary corrections.

### Agency Response

This ITS recommendation is based on an accreditation cycle ST&E for CCE and the Magic Service Desk (MSD) that is ongoing and scheduled to end by September 30, 2005. Therefore, it is not realistic or cost effective now to pull and revise the C&A 2004 documents reviewed during this audit. Many of these documents have already been revised for currency and will become deliverables to the ST&E process. The risk assessment has not been updated by ITS but will be updated during the ST&E process. The ITS focus needs to be on the current C&A activities.

The purpose of the CCE C&A at the time of submission was limited to the CCE GSS, as was the WEB farm limited to the WEB farm GSS, and other GSSs under the Service Center Modernization Initiative (SCMI); they were

not intended to reflect the ITS, as the re-organization did not occur until November 28, 2004. We followed all of the regulations per Department policies that were in effect at the time of our C&A activities.

**OIG Position**

While we agree that ITS' focus should be on its current C&A efforts, our recommendation was not limited to the CCE and MSD. ITS did not respond to the recommendation about their process for reviewing the other C&As under their control to identify and correct the same issues we found in our review of two ITS' systems. For management decision on this recommendation ITS needs to provide a time-phased plan for either reviewing or reaccrediting all systems under its control.

**Recommendation No. 2**

ITS should establish policies, procedures, and controls to ensure that the documentation supporting the C&A process is prepared in accordance with prescribed departmental and other Federal guidance and that the results of the review support the assessment.

**Agency Response**

The CCE C&A process began in August 2003 using NIST guidelines since USDA policy was not current. Within a few months, revised USDA policy became available so we re-aligned our C&A procedures to meet the revised USDA policy, which held precedence over NIST guidance. That Department policy was still current at the time of submission of C&A materials to the C&A Certification Official/Team at USDA.

It is the standard practice of the Infrastructure Governance Division, Security Policy Branch to keep all ITS policies current and aligned to USDA policies. This is an ongoing effort. Refer to Recommendation 3 for additional information.

**OIG Position**

OIG identified several deficiencies that did not meet either the NIST or USDA guidelines. Therefore, for management decision on this recommendation ITS needs to develop a specific policy and establish controls, such as second party review or other controls deemed necessary by management, to ensure that the C&A documentation complies with applicable laws, regulations, and NIST guidance.

---

**Finding 2** **Operating Procedures Not Finalized and Implemented**

ITS did not have finalized operating procedures. Instead, ITS field personnel relied on SCA operating procedures in place prior to convergence. Further,

ITS had not established a formal procedure for drafting, commenting, or finalizing operating procedures and other policy documents. While ITS recognized the lack of finalized operating procedures, officials informed us that they did not believe that this caused significant harm to the CCE operations. This means, in conjunction with ineffective memorandum of understanding (MOU) between ITS and the SCAs (see Finding 3), a broad array of potentially obsolete and ad-hoc operating procedures are being used throughout the CCE network that may not serve the best interest of securing the CCE operating environment.

NIST guidance requires the formulation of procedures, standards, and guidelines and procedures that specify the responsibilities of organization personnel in the program.[9] Further, to be effective, policies and procedures should be consistent with other existing directives and visible throughout the organization. Further, internal control standards for the Federal Government require that management controls be documented in the form of policies, directives, or operating manuals, and readily be available for examination.[10]

ITS was able to provide us with only one finalized written policy, outlining security policy, which was signed 2 months after convergence took place. Further, ITS provided draft policies that contradicted both ITS and SCA personnel's knowledge of the planned course of action. For instance, ITS' draft policy on vulnerability scanning states that SCAs are responsible for (1) continued scanning of their regions; (2) tracking action plans on high and medium vulnerabilities identified; and (3) collecting and maintaining a catalog of all servers, networks, routers, switches, Internet Protocol addresses, databases, data warehouses, workstations, and laptops that will be scanned on a monthly basis. However, this directly contradicts ITS and SCA agency personnel's statements that they had been informed that ITS would be scanning from the first day of convergence. Discussions with ITS personnel confirmed that ITS would be conducting vulnerability scanning. ITS confirmed that they would be performing all vulnerability scanning, but only after a centralized vulnerability scanning process is put in place.

Additionally, SCAs' Information System Security Program Managers (ISSPM) informed us that they remained confused about what parts of their responsibilities will remain within the SCAs and which are transferred to ITS. Further, ISSPMs informed us that they had not seen any draft policies or procedures from ITS and were concerned with several sections of the existing security policy manual. The SCA ISSPMs we talked with expressed frustration of what appears to be ITS' inaction or oral promises to address

[9] NIST SP 800-6, "Automated Tools for Testing Computer System Vulnerability," dated December 1992. NIST SP 800-10, "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls," dated December 1994.
[10] GAO's "Standards for Internal Control in the Federal Government," dated November 1999.

SCA concerns. In addition, the SCA ISSPMs did not know of any ITS established formal evaluation process where their concerns could be resolved.

Our review of ITS documentation also disclosed that SCA ISSPMs had been provided copies of draft policies and procedures from ITS for their review and comment. ITS informed us that there was a formal process for SCA ISSPMs to raise their concerns. However, ITS responds to all issues formally documented and issued by only the SCA CIO to ensure that all issues have the SCAs' senior management support. Therefore, there appears to be a significant break down in communication between the SCAs and ITS resulting in significant frustration on both sides. Without clear written procedures and responsibilities (see Finding 3) spelled out for both sides, this miscommunication will most likely continue, increasing both the frustration and the potential for security weaknesses.

ITS agreed that additional work was required on the security policy and procedures comments and the documentation process. ITS plans additional work to implement a formal directives process in conjunctions with OCIO. ITS stated that the security branches within ITS are actively reviewing and updating the draft procedures.

### Recommendation No. 3

ITS should establish clear policies and procedures for all activities and functions it has assumed and include input from the SCAs when established policies impact their operations.

### Agency Response

The ITS Infrastructure Governance Division, Security Policy Branch concurs that establishing clear policies and procedures, with input from interested parties, is critical to efficient operation of any organization. The Security Policy Branch is currently working to develop a comprehensive set of policies and procedures relating to those security-related functional areas that have become ITS responsibility in the transition. The Security Policy Branch is actively seeking the input of the affected SCAs to ensure a symbiotic relationship with them to develop a comprehensive set of security policies and procedures.

As of August 2, 2005, the Security Policy Branch has published the following procedure guides: Patch Deployment, Vulnerability Scanning, Incident Response and Access and Password Management security procedures as an addendum to the OCIO-ITS Security Policy Manual. Also, since the completion of the OIG audit, chapter 29, "Personnel Clearance Security Policy," and chapter 30, "Licensed Software Security Policy of the OCIO-ITS Security Policy Manual" have been published for use. Additional policies and procedures are being developed and finalized as the Department

develops and publishes its policies and procedures and as resources are available and committed to the effort.

**OIG Position**

We concur with ITS' management decision.

---

## Finding 3 — Roles and Responsibilities Need to be Established and Communicated

The MOU and the Incidental Transfer Agreement (ITA) were too overarching to hold either ITS or the SCAs accountable for adequate security, and have not been updated since convergence with specific roles and responsibilities. This left security staffs at the SCAs unclear about their responsibilities for security issues under this new arrangement. Further, one agency had not signed the final MOU. IT officials informed us that they believed that this was not a significant weakness since most ITS employees were transferred from the SCAs and already knew their responsibilities. As a result, neither ITS nor SCAs are effectively carrying out security within the CCE. (See Findings 2, 5, and 6.)

OMB requires that written management authorization (often in the form of an MOU or Service Level Agreements (SLA)) be obtained prior to connecting with other systems or when sharing sensitive data.[11] The written authorization should detail the rules of behavior and controls that must be maintained by the interconnecting systems. Additionally, management controls include assuring that performance measures are complete and accurate by aligning staff and authority with the program responsibilities to be carried out protecting the integrity of Federal programs.

ITS instituted a single MOU between it and all three SCAs with the stated purpose of outlining the roles and responsibilities that will transfer to ITS; however, as of more than 3 months after convergence, ITS still had not instituted individual MOUs or SLA between ITS and the individual SCAs that specifically define who were responsible for specific activities or how selected activities would transition from the SCA to the converged ITS. The following examples describe the types of ambiguity we discovered.

- The MOU stated that ITS will develop a strategy and procedure to provide security incident response handling for all IT equipment. However, the MOU did not address how incidents would be handled, reported, or resolved while ITS developed these procedures.

[11] OMB Circular No. A-123, "Internal Control Systems," dated June 1995. OMB Circular No. A-130, appendix III, "Security of Federal Automated Information Resources," dated February 1996.

Additionally, the MOU did not address how to report suspected incidents during this transition period or how long it would be until procedures were in place.

- The MOU stated that employees transferred to ITS were to retain access to the SCA computer networks, systems, and applications they had prior to the convergence. However, the MOU was silent on issues such as how long this continued access was needed, or how the SCAs would be notified when a user identification (ID) was no longer needed.

- The MOU stated that ITS employees would retain access to SCA applications until the "agency" deemed the support no longer required. However, the MOU did not define whether the "agency" was ITS or the SCAs, leaving responsibilities vague and possibly contradictory.

ITS informed us that the MOU and ITA documented only the logistical support and agreements in place between ITS and the SCAs to support the convergence of personnel. These documents were not intended to define the program-level roles and responsibilities. Post-convergence, the ITS Service Line Managers (SLM) would be coordinating the detailed SLAs based on the five ITS service lines. ITS also stated that the ITS security SLM has initiated the agreement with the SCA ISSPMs and that all parties have agreed to prioritize the security areas that must be addressed in the SLA. Specifically, four areas (vulnerability scanning, patching, logical access controls, and incident response) will be addressed in the first edition of the document, which was expected to be issued in May 2005. ITS stated that many of OIG's concerns would be addressed in this first version.

However, the MOU specifically stated:

> ITA transferred personnel, authorities, responsibilities, resources, and functions for IT infrastructure management and service delivery from the SCAs to ITS ... and established a framework for service delivery to the SCA from ITS. ... This MOU supplements the ITA by documenting agreements between the SCA and ITS that define the details of how selected resources and responsibilities will be transferred to ITS, and how ITS and the SCA will collaboratively share financial and operational responsibilities to continue day to day operations during a transitional period.

Therefore, OIG would have expected to see the details of resources and responsibilities assumed by ITS in these documents.

Additionally, ITS stated that they understood and shared OIG concerns for post-convergence operation without clear responsibilities within some shared security programs. In spite of this, ITS stated that it felt confident that the lack of formal documentation had not weakened the security controls over the environment. ITS was confident that the lack of clarity over a few security issues had not undermined the integrity of the entire infrastructure, since ITS was made up of the same group of individuals that managed a majority of the infrastructure and security controls prior to convergence. However, OIG does not share that confidence. OIG scans of only a limited portion of the CCE network disclosed 1,458 vulnerabilities (see Finding 5) and system settings that did not meet departmental guidance (see Finding 6). Internal control standards for the Federal Government require that management controls be documented in the form of policies, directives, or operating manuals, and readily be available for examination.[12]

In addition to the MOU being vague about system access by ITS employees, ITS was unable to provide a listing of which SCA applications ITS employees had access to. Therefore, ITS does not have a centralized record of its newly transferred employees to know what application or network accounts to terminate. Since the individual no longer reports to any of the SCAs, it was difficult for the SCA security staff to determine when access is no longer required. Access controls and the transfer of agency employees is critical to security of any system and should have been agreed to by ITS and the SCAs and clearly described in the MOU.

Finally, we also identified a lack of defined roles and responsibilities at the field personnel level in the three States we visited. Despite the fact that employees and equipment transferred to ITS in November 2004, field service personnel had not received their job descriptions and standards. ITS employees repeatedly told us that they continued to operate under the same SCA-issued procedures they had been subject to prior to convergence. Further, ITS field personnel informed us that they were unaware of their specific job responsibilities under OCIO. For example, ITS employees were unaware of their role in the event of an emergency or disaster at a service center, and the MOU did not mention the roles and responsibilities in the event of an emergency or disaster. Finally, ITS employees were unaware of their responsibility for such activities as inventories, access controls, and security awareness, and were unaware of any specific ITS-issued procedures.

[12] GAO's "Standards for Internal Control in the Federal Government," dated November 1999.

**Recommendation No. 4**

ITS should negotiate separate MOUs or SLAs with each SCA, and establish policies and controls to ensure that the MOUs or SLAs are reviewed periodically and updated as necessary.

**Agency Response**

ITS has already negotiated SLAs covering major aspects of security separately with each of the SCA. These SLAs have been in place since June of 2005. ITS is currently reviewing these SLAs, updating them as needed, and incorporating them into new and more comprehensive SLAs covering the full range of ITS services with each of the SCAs. This full range of services is currently under development and will be incorporated into the ITS Service Catalog. These SLAs will be embodied in separate MOUs to be negotiated with each of the SCAs – and will supersede many of the interim terms included in the comprehensive MOU that was signed by all three SCAs in December, 2004. We expect to complete this negotiation process and to have these new and more comprehensive SLAs in place no later than the end of calendar year 2005 prior to the start of our initial informational billing process. The policies and controls will be formalized by December 31, 2005.

**OIG Position**

We concur with ITS' progress in establishing a more comprehensive SLA with each SCA. However, ITS needs to provide us the specifics of the policy and controls ITS intends to establish to ensure that SLAs are periodically reviewed and updated.

**Recommendation No. 5**

ITS should establish policies and controls to ensure that clearly defined roles and responsibilities are identified, documented, and relate to specific job performance standards.

**Agency Response**

ITS has developed job descriptions for all ITS employees, including all security staff and field personnel. The process by which these job descriptions clearly identify, define, and document the responsibilities of each role is supported by ITS Policy, "USDA/OCIO/ITS Performance Management Program" Directive of May 18, 2005. The Performance Management Program has been developed and implemented, and this program clearly defines the performance standards required for each assigned role. Since convergence, 240 position descriptions have been developed by the ITS management and standardized for use across the ITS organization. These performance standards have been reviewed with all staff, signed, and formally put into place. Together, these documents clearly identify and document the roles and responsibilities of all staff and document job performance standards. As with any new organization, there will be some overlap before staff is familiar with new documentation and programs, but

these issues are being systematically addressed through the customized job descriptions, policies and controls which ITS has already put into place.

**OIG Position**

We concur with the management decision.

---

## Finding 4 System Inventory Needs to be Updated and Maintained Properly

ITS did not have an accurate inventory of computer equipment on the CCE network. This occurred because ITS field employees did not have the access authority to enter or modify inventory records in the system that ITS relies upon to track equipment on the CCE network. Further, ITS had no formal policies and controls to ensure inventory was maintained effectively. Additionally, ITS had not issued written agreements or policy with the SCAs regarding whether computer equipment purchased with SCA funds could be connected to the network or how they would be tracked. As a result, ITS' ability to effectively secure the CCE network environment is at risk.

Departmental guidance requires agencies to keep an inventory of their network.[13] NIST encourages an organization to maintain adequate inventory of its hardware and software.[14] This inventory will enable the organization to ensure that applicable patches and vulnerabilities are timely addressed. Once created, the organization should maintain the inventory by ensuring it is timely updated.

ITS' tracking system inventory reports did not accurately reflect the network devices actually on site in the State and SCA offices we visited. Our physical inventory conducted at 6 State offices and 19 SCAs in 3 States identified network devices not recorded in the tracking system and network equipment that could not be found at those locations. For example:

- At 1 State office we found 542 network devices recorded in the tracking system; however, our physical inventory disclosed that 181 (33 percent) of those items could not be found on site.[15] The inventory also identified 140 network devices that were not recorded in the tracking system for that location.

- At 1 SCA we identified 60 network devices recorded in the tracking system. However, our inventory disclosed that 24 (40 percent) of the

[13] Departmental Manual 3500, "Cyber Security Manual," Chapter 6, Part 1, dated April 2003.
[14] NIST SP 800-40, "Procedures for Handling Security Patches," dated August 2002.
[15] Network devices include computers, servers, printers, routers, and other devices that physically attach to the CCE network.

items could not be found. Our inventory also identified 11 network devices not recorded in the tracking system for that location.

When reconciling the discrepancies we found, ITS field personnel would often inform us that the missing items had been moved to other locations. For example, at one State office ITS field personnel informed us that four missing items were transferred to other service centers. However, our physical inventory conducted at those service centers found only two of the four missing items. ITS field employees informed us that they did not have the proper access to the tracking system to enter or modify equipment inventory records. We also found that SCAs had purchased computer equipment after convergence and attached them to the network, but they had not been entered into the tracking system.

Our discussions with the ITS tracking system representative disclosed that ITS had limited update access to the system by central office personnel in order to maintain database integrity. Network devices in the State and service center offices purchased with CCE funds were automatically loaded into the tracking system from automated inventory records provided by the vendor as part of the purchase agreement. However, ITS had not issued written procedures or policy on how network devices purchased by the SCAs were to be recorded. One of the ITS field employees we spoke to notified the central office of SCA purchased computer equipment and validated that the tracking system was updated with this information. However, the remaining offices visited did not rely on the ITS tracking system and tracked manually the differences between the ITS tracking system and equipment on hand.

ITS indicated that they were not surprised by the discrepancies identified by OIG. Specifically, ITS stated that its tracking system was designed and implemented only for property purchased with CCE funds. The ITS tracking system was not intended for utilization for all agency equipment procured. Instead, funding source was the driving force as to which equipment was and was not entered. However, OIG was specifically told by ITS personnel during the course of the audit that all equipment connected to the CCE network was to be tracked in the system. Additionally, our visit to one location disclosed that SCA purchased equipment was being loaded into the tracking system, thereby confirming what we were told. Therefore, it is apparent that there is a break down in communication on exactly what equipment is to be tracked in which systems. Additionally, we were informed by personnel at one State office that they had stopped entering all equipment procured with SCA funds into the inventory system because it was their understanding ITS now owned and tracked all equipment connected to the network.

Without proper inventory records, ITS cannot secure the CCE environment effectively. For instance, our network security scans at one location identified three systems connected to the network that did not appear on the tracking system inventory report.[16] Our scans disclosed 61 high and medium risk vulnerabilities that should have been addressed in a timely manner.[17] Some of those vulnerabilities would have allowed us to gain administrator access to all three of these systems.

### Recommendation No. 6

ITS should conduct a complete inventory of items attached to the CCE network and develop policies, procedures, and controls to ensure that inventory records are adequately maintained.

### Agency Response

Attachment E of the Incidental Transfer Agreement signed in September of 2004 provides a listing of the type of equipment that is to be inventoried in Equipment Acquisition Tracking System (EATS). After reviewing the list it is apparent that OCIO-ITS needs to re-evaluate the listing to ensure that that we are capturing the equipment necessary for the mission of the organization. Upon completion of the review we will develop written policy and procedures that defines those items to be tracked and how they should be tracked. Once this is completed we will conduct a complete physical inventory of all items that have been defined as inventorial in EATS and also a complete physical inventory of all items in the Department's Personal Property System (PROP). A complete inventory of EATS and PROP was completed in April 2005.

### OIG Position

We concur with the management decision.

### Recommendation No. 7

ITS should, through discussions with the SCAs, establish who owns information technology (IT) equipment purchased by the SCAs after convergence. Once ownership is established, either (a) renegotiate the ITA to clearly address ITS ownership of this equipment or (b) enter into an Interconnectivity Service Agreement (ISA) with the SCAs to ensure network security is maintained. [18]

---

[16] See Finding 5 for a complete description of scan results and related recommendations.

[17] We ran pre-defined scans for the 10 most common types of exploits during the time of our audit, against these three systems; therefore, additional vulnerabilities may exist that our scan was not designed to detect. High risk vulnerabilities are those that provide access to the computer, and possibly the network of computers. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those that provide access to sensitive, but less significant network data.

[18] An ISA is outlined in NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," dated August 2002. An ISA documents the requirements for connecting to networks/systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line.

**Agency Response** Although OCIO-ITS has had discussions with the SCAs as it relates to ownership of equipment purchased after convergence, we have not formally documented our position on this issue. OCIO-ITS will develop a written supplement to the ITA that addresses the ownership issue of property that is purchased after the convergence. The OCIO-ITS position is that any equipment that is purchased after the convergence by the SCAs that is IT, telecommunications, or connects to the network is owned by ITS. OCIO-ITS plans to finalize a policy regarding ownership of equipment by November 2005.

**OIG Position** We concur with the management decision.

The SCAs rely on computer-based information systems to carry out agency programs, manage resources, and report financial statement data. The reliability of its systems is critical to the SCAs in meeting their mission. Logical access controls should provide reasonable assurance that critical resources are protected against unauthorized modification, disclosure, loss, or impairment. Further, timely identification and mitigation of system vulnerabilities on ITS' network resources help ensure that critical IT resources are protected from possible malicious attacks from both internal and external threats. ITS must implement and enforce sound access control, vulnerability assessments, and mitigation of vulnerabilities identified to ensure the integrity, confidentiality, and availability of the SCA data maintained on its systems.

## Finding 5 — Vulnerability Scanning Processes and Controls Need to be Established

We found that (1) scans of selected network devices connected to the CCE network disclosed a large number of risk indicators that could be exploited, and (2) system policy settings did not provide for optimum security and were not uniform throughout the CCE network. ITS had not begun periodic scanning of the CCE network and SCAs had ceased their scanning activities after CCE convergence in November 2004. Therefore, ITS' systems and networks may be vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of the program and financial data, some of which is Privacy Act-protected.

OMB requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce the threat or amount of potential loss.[19] NIST expands on this by requiring the formulation of guidelines and procedures that specify the responsibilities of organization personnel for vulnerability testing.[20] This process should begin by reviewing the organization's systems and developing vulnerability testing requirements in accordance with system functionality. Finally, Cyber Security requires USDA agencies to conduct vulnerability scanning on a monthly basis and take the necessary steps to mitigate vulnerabilities identified.[21]

[19] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.
[20] NIST SP 800-6, "Automated Tools for Testing Computer System Vulnerabilities," dated December 1992.
[21] Cyber Security 007, "Security Vulnerability Scan Procedures," dated September 2001.

We assessed selected CCE networks, including the CCE local area networks in three States and one WEB farm between January 24 and March 22, 2005. We used a commercially available software product designed to identify over 1,400 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP).[22]

We included 957 CCE network components in the vulnerability scans we performed. Our scans identified a total of 639 high and medium risk vulnerabilities. In addition, we identified 1,458 low risk vulnerabilities. Copies of scan results were provided to ITS immediately following scanning. The high and medium vulnerabilities, if left uncorrected, could allow unauthorized users access to critical and sensitive data. Additionally, we attribute the large number of low risk vulnerabilities to the need to strengthen general system administration. We identified similar vulnerabilities when the individual SCAs were responsible for their own vulnerability identification.[23]

Detailed below are examples of the high risk vulnerabilities disclosed during our current vulnerability scans.

- Our scanning software was able to easily guess a weak administrator password; for instance, where the password is the same as the user ID. The "administrator" account is the most trusted user account and has complete control over the computer. This could allow an attacker to obtain, or possibly alter, the information being stored on ITS' networks.

- A machine was improperly configured and did not have up-to-date patches installed which could allow an attacker to easily obtain or change system information and gain information about open connections with other CCE systems.

- Configuration problems exist which allow automatic log on and allow readable system user passwords. As a result, an attacker could execute commands to freely access a system and take over or destroy any critical or sensitive information maintained on the systems.

- Systems allowed users IDs to be easily acquired, providing the foundation for a brute force attack.

[22] TCP/IP is a series of protocols originally developed for use by the U.S. Military and now used on the Internet as the primary standard for the movement of data on multiple, diverse platforms.
[23] Audit Report Nos. 85099-2-FM, 85099-4-FM, 10099-1-TE, and 03099-47-KC.

- Guest user accounts had a blank password. Any individual can log in to these accounts without a password. This issue applies for both enabled and disabled guest accounts. Although disabled accounts are less of a concern, an attacker may be able to enable the guest account at a later time if they have already succeeded in compromising the network.

These conditions occurred because ITS had not fully implemented processes and controls over vulnerability scanning of the CCE network. Additionally, plans and draft procedures for scanning computer equipment on the CCE network were incomplete and did not address all the necessary requirements for conducting vulnerability scanning.

According to ITS and the SCAs, ITS assumed responsibility for scanning the CCE network, three WEB farms, and large offices when convergence took place in November 2004. Previously, the SCAs were each responsible for scanning their own WEB farm and large offices as well as one of the three CCE network regions. However, ITS stated that they were currently scanning only the three WEB farms and two of the large offices while plans were being tested to add scanning the remaining large offices and the CCE network. At these five locations, ITS had set up automatic scanning monthly. However, OIG found that one of the two large offices had not been scanned in 8 months and that the automated scan had been turned off in one of the WEB farms. Further, despite the fact that ITS had assumed responsibility for monthly scanning, the ITS draft vulnerability scanning procedures stated that the SCAs were still responsible for continued scanning of their regions and tracking action plans on high and medium vulnerabilities identified.

Discussions with ITS personnel and review of its vulnerability scanning architecture disclosed that ITS planned on implementing a single centralized scanning methodology that would scan the CCE network. However, ITS personnel did not believe that they had the ability to scan the entire CCE network monthly. Therefore, ITS had explored scanning a rotating one-sixth of the CCE network on a monthly basis. ITS' justified its approach by stating that its patch and configuration management was sufficient to ensure all computers were adequately protected even though only one-sixth would be scanned in any single month. Despite these claims, ITS could not provide evidence that it had performed sufficient testing to determine exactly how many computers could be effectively scanned monthly, or how placement of the scanning hardware or the time of day of the scan would affect the volume of scans. Further, ITS could provide minimal evidence that its patch and configuration management were adequate to address the concerns about poor patch and configuration management, which lead to the requirement for monthly scanning.

During discussions with ITS on this issue, ITS stated that they had not had sufficient time since convergence to identify and address all the 'legacy' systems that were inherited by ITS from the SCAs and take the necessary action to address their configuration and continued viability. ITS defines 'legacy' systems as those systems the SCAs have historically operated and maintained and they define the 'CCE' systems as those servers and workstations that are built with the IO Lab's standard image. While OIG agrees that many of the high and medium vulnerabilities were found on what ITS terms as SCA 'legacy' systems, all devices scanned were part of the CCE network environment and now fall under ITS control. Therefore, whether the vulnerability is on a 'legacy' or 'CCE' system, it still represents a threat to the entire CCE network and ITS is responsible for its mitigation. Until all vulnerabilities on the network are mitigated, ITS' offices and networks may be exploitable through unidentified and uncorrected vulnerabilities that may jeopardize the integrity of the data on ITS computer resources.

**Recommendation No. 8**

ITS should immediately address the high and medium vulnerabilities identified during our audit.

**Agency Response**

OCIO-ITS provided all scan findings to the appropriate system administrators for immediate mitigation upon receipt from OIG. Actions were taken to mitigate many of the vulnerabilities found within the offices visited and similar actions were implemented as necessary to mitigate vulnerabilities across the enterprise.

As OIG stated, the majority of the vulnerabilities found were on 'legacy' systems not previously managed by the Information Technology Working Group (ITWG) as a part of the CCE environment. Some of the vulnerabilities identified could not be immediately addressed and will require further coordination with the SCAs.

The residual risks posed by these 'legacy' systems will be monitored during monthly scan activity. OCIO-ITS will actively work with the SCAs to address upgrading the 'legacy' systems or taking additional action to mitigate the risks posed by the current system.

Future action to address outstanding issues can be monitored under Recommendation 9 and/or Recommendation 16 as all outstanding issues are relevant to 'legacy' equipment and/or third-party network devices.

**OIG Position**

We concur with the management decision.

### Recommendation No. 9

ITS should (1) work with SCAs to identify and assume control over 'legacy' systems, (2) establish policies identifying minimum security requirements to be met for all devices attached to the CCE network, and (3) establish controls to ensure those policies are being followed.

**Agency Response**

OCIO-ITS began the process of identifying 'rogue' servers with the SCA representatives as a part of the large office migration process to the SCA network. This process was further developed with the help of the SCA ISSPMs during May and June 2005 as a part of the President's Management Agenda (PMA) taskforce.

OCIO-ITS and the SCAs conducted several meetings to discuss the future approach in transitioning the responsibility for the 'rogue' servers and the timeframes for implementation. It was agreed that each server/platform presented unique requirements and therefore each transition would have to be treated as a separate project.

In addition to the server/application identification and transition initiatives started as the "rogue' server" project, OCIO-ITS is also continuing to work with NRCS leadership to retire legacy UNIX platforms that still reside in the State and county offices. The migration to exchange email removed the dependency on the legacy UNIX mail servers, and a vast number have been taken out of service. However, a few pockets of users are continuing to rely on the UNIX platform for other purposes, so OCIO-ITS is addressing that situation in conjunction with NRCS management. OCIO-ITS anticipates retirement of all remaining UNIX mail servers by December 2005.

**OIG Position**

While we agree with the actions proposed, ITS needs to address all components of the recommendation. While assuming control over legacy systems, ITS' response did not address the actions or timeframes for establishing minimum security requirements for all systems attached to the network and what controls it intends to establish to ensure compliance with the requirements.

### Recommendation No. 10

ITS should establish policies, procedures, and controls to ensure that system vulnerabilities are timely identified and mitigated.

**Agency Response**

Upon convergence, OCIO-ITS assumed the responsibility for identifying and managing vulnerabilities within the network. Implementing a comprehensive, consistent process for vulnerability assessment is security

priority for the new organization. Although OCIO Cyber Security and the ITWG had security policies which defined the need to perform scans every 30 days, no formal infrastructure existed for the SCAs to consistently and uniformly scan the networks prior to convergence.

Vulnerability scanning will be performed every 30 days per security policy which will encompass the OCIO-ITS networks, and include all workstations, servers, routers, switches, and printers for each GSS. Standardized scanning servers and vulnerability scanning software was implemented throughout the existing OCIO-ITS network. Additionally, a centralized management system with well-defined reporting capabilities was implemented to track the prompt remediation of medium and high-level vulnerabilities discovered during the scanning process.

**OIG Position** We concur with the management decision.

**Recommendation No. 11**

ITS should establish policies, procedures, and controls to ensure that systems are properly maintained with patch management and post-implementation configuration management.

**Agency Response** OCIO-ITS developed a series of documents outlining patch and configuration management policies and procedures. The OCIO-ITS Security Policy and the Change Control Board Charter establish the baseline for these initiatives. Over time, and as a result of the PMA taskforce, additional documentation has been formalized.

OCIO-ITS conducted a review of the patch strategies in-place throughout the environment to ensure proper notification, testing, and timely application of vendor patches.

OCIO-ITS implemented the enterprise vulnerability scan capability for use as a tool to actively manage and monitor security risks within the environment. The vulnerability scan methodology allows for management oversight and control to ensure that all applicable security measures, including patch management and configuration management, have been taken to mitigate risks.

**OIG Position** We concur with the management decision.

## Finding 6 Logical Access Controls Need Strengthening

ITS had not implemented effective access policies and controls within CCE. ITS was not prepared to take over controlling access to the CCE at the time of convergence and has allowed each SCA to continue with their current access control policies. As a result, ITS and the SCAs that it serves have reduced assurance that only authorized users have access to the CCE network and that they have access to only those network resources they need to perform their job.

OMB requires the use of individual accountability, least privilege, and separation of duties controls in every application and GSS. To achieve these requirements, OCIO issued a departmental manual with detailed instructions requiring security staff to maintain files of users including names, office addresses, and telephone numbers.[24] Therefore, OCIO was not following its own prescribed policy. Additionally, user ID and passwords are to be assigned only to authorized individuals, and no generic or shared user IDs are to be created. Finally, security staffs are to remove user accounts when the employee is no longer with the agency. To ensure removal, formal procedures should be established for agency personnel to notify security staff of all separations.

We assessed selected CCE servers and workstations in 12 locations in 2 States between February 23 and March 5, 2005. We used a commercially available software product designed to identify access control and other security configuration settings on computers in a network. We then compared the network's security settings to Federal guidance and industry "best-practices." Some weaknesses we found included:

- Password policies not set in accordance with departmental regulation,
- stale user accounts,
- user accounts with excessive bad logon attempts,
- user accounts logged in for more than 1 day, and
- user accounts with non-expiring passwords.

This condition occurred because, despite the transfer of equipment and personnel to ITS, the three SCAs continued to grant and terminate access to the CCE network, including dial-up and Virtual Private Network (VPN) access, in accordance with their own unique policies and procedures. Dial-up and VPN access information remained with the SCA that originally granted

[24] Departmental Manual 3140-001, "Management of ADP Security Manual," dated July 1984.

the access; therefore, ITS was not able to provide us with a list of newly transferred ITS employees with dial-up or VPN access. OIG recognizes that SCA managers are in a better position to know who should have access to the CCE network and SCA applications. However, due to the shared nature of the computing environment, ITS has a shared responsibility with the SCAs to ensure that access controls are limited to only the access needed to perform job functions, that accounts maintain effective security parameters, and that accounts are removed when no longer needed.

Our review also disclosed that the ITS field employees with full administrator privileges had access to CCE servers outside the scope of their job responsibilities. In 1 State, the 7 ITS field employees we interviewed had full administrator access to all the servers in the 11 States of that region. According to that State's ITS coordinator, there were approximately 40 ITS field employees in the State that had full administrator privileges over the servers in the entire 11-State region.

One reason for the excessive administrator privileges was that ITS had only three network authorization access levels: (1) "user" with access to the local computer; (2) "local administrator" which allowed the installation of software; and (3) "full administrator" which allowed full access rights to all computers in the region. We found that when one SCA employee's job duties required access to data on another service center's server, that SCA employee was granted "full administrator" privileges over the entire region.

We also found that ITS had not instituted formal review procedures for performing a periodic review of CCE user accounts to validate that only current employees had access. ITS field personnel in three States we visited disclosed that ITS had not yet established procedures to ensure that only current employees had access to the CCE network. Further, in 8 of the 25 locations visited, separated employees still had active user accounts.

Finally, we identified active generic user and training accounts on service center servers in all three States we visited. The center employees, including the ITS field employee accompanying us, did not know why the generic accounts existed, what they were used for, or who had the password.

In its response to this issue, ITS stated that limitations within the operating system dictated that domain administrator level accounts be established for all ITS support staff. While ITS conceded that individual staff may not be involved on a daily basis with location outside their immediate area, they were required to provide support during leave, travel, emergencies, or for work load balancing. ITS felt that the fact that they had been operating and supporting the network for 3 years without any significant incident demonstrated that there was no real problem with their current access

methodology. Additionally, ITS believed that all the accounts, with their associated privileges, were established and being maintained with the objective of maximizing availability of the ITS support of the SCA services required to deliver USDA programs to their customers.

The operating system in use by ITS has the ability to assign administrative privileges to specific organizational levels. ITS' inability to assign these scoped privileges may be related to the overall environment design rather than the operating system capabilities. Further, ITS' statement that the CCE network has functioned effectively under the current configuration for the past 3 years without incident does not justify non-compliance with OMB, Department, and NIST requirements.

**Recommendation No. 12**

ITS should identify all individuals authorized dial-up and VPN access to the CCE network, and establish policies and controls to ensure that dial-up and VPN access are controlled as effectively as regular access permissions.

**Agency Response** The access control process for remote connections transitioned from the SCAs to OCIO-ITS on June 30, 2005. While, OCIO-ITS hosted the capability for remote connectivity since inception, access management was still controlled by the agency security offices post-convergence. OCIO-ITS began a review of the accounts in conjunction with the agency ISSPMs in July 2005. During this initial review, individual accounts were correlated to the employing agency to assist in future reporting efforts. OCIO-ITS is also analyzing the security controls in-place on the different VPN servers to develop a common set of security controls for the enterprise.

OCIO-ITS implemented an Agency System Access Authorization Request (ASAAR) process, including documentation, to control all future account activity for dial-up and VPN account creation, modification, and deletion.

**OIG Position** We concur with the management decision.

**Recommendation No. 13**

ITS should establish policies and controls to ensure that all employees, including employees with full administrative access, are granted access that adheres to the concept of least privilege.

**Agency Response** OCIO-ITS has completed several projects to address the OIG concerns regarding account management and excessive privileges. OCIO-ITS initiated a 100 percent review of all administrative accounts throughout the enterprise. A process for future periodic reviews is under development.

- Active roles were implemented. Domain administrator rights have been restricted, so that administrators now only have authority within the group with which they are assigned.

- The SCAs were provided a listing of accounts from active directory for a 100 percent account validation in April 2005. Changes were implemented in June 2005. One agency alone identified over 650 accounts that were removed from the system.

- OCIO-ITS implemented the System Access Authorization Request process to control all future account creations, modifications, and deletions on July 1, 2005. Account requests must be submitted to OCIO-ITS via the approved automated form from an agency designated point of contact. A request for elevated/administrative privileges requires a secondary approval from the agency security staff, and concurrence from OCIO-ITS management.

In addition, controls were put into place to review and verify account changes by performing management reviews of the monthly access listings.

**OIG Position**

While we agree with OCIO-ITS' completed and proposed corrective actions, ITS needs to provide a date when it will implement a policy that documents the processes and controls outlined in its response.

**Recommendation No. 14**

ITS should establish policies and controls to ensure that the accounts of separated employees are timely identified and removed.

**Agency Response**

The OCIO-ITS management staff is responsible for initiating the termination of employee access upon separation. The contracting officer technical representative is responsible for notification of contractor separation. Notifications can be submitted using the ASAAR process, and immediate removals can be escalated via the ITS service desk and direct contact to system administrators.

OCIO-ITS also has a process with the Bureau of Public Debt (BPD) to ensure timely confirmation of ITS employee separation. BPD provides a weekly notice to OCIO-ITS of all e52 actions; that list is culled to identify termination/separation actions. The Operations Security Branch is notified and access removal is confirmed as a compensating control.

Agency employee and contractor separations are managed by the agency security offices, who notify OCIO-ITS via the ASAAR process. In the event of an immediate separation, the agencies can expedite account removal by contacting the ITS service desk. The agencies utilize the monthly user account reports as a compensating control to ensure all accounts are removed from the system.

**OIG Position**

While we agree with OCIO-ITS' completed and proposed corrective actions, ITS needs to provide a date when it will implement a policy that documents the processes and controls outlined in its response.

**Recommendation No. 15**

ITS should remove all generic user accounts and establish policies and controls to ensure that no new generic user accounts are created.

**Agency Response**

OCIO-ITS is currently reviewing all instances of generic and service accounts across the enterprise. OCIO-ITS held internal meetings with the Key Stakeholders who currently require generic/service accounts beginning in Feb of 2005. The Operations Security Branch and the IO Lab worked collectively to identify and document all of these accounts across the active directory domain. During this review, OCIO-ITS identified 14 active directory administrator-level service accounts and 60 domain administrator level service accounts.

A review of existing generic and service accounts is underway to determine alternative solutions for service accounts. All OCIO-ITS generic accounts follow a secure naming structure with enhanced passwords following security best practices. In certain instances where alterative accounts or methods can not be utilized OCIO-ITS will use our internal risk acceptance process, to accept these risks as they are critical to ensuring certain applications across the enterprise continue to function. OCIO-ITS plans to have policies and controls over generic accounts finalized by January 2006.

OCIO-ITS will perform research, identify any generic user accounts and implement any necessary controls on these accounts.

**OIG Position**

We concur with the management decision.

## Finding 7 — Third Party Connectivity to the CCE Network Requires Oversight

ITS had not ensured effective controls over computer equipment attached to the CCE network by SCA partner organizations. Further, ITS had not maintained a record of the computer equipment connected under these partnership agreements. ITS had not established written procedures or agreements on whether computer equipment not belonging to ITS or the SCAs could be connected to the network, how they would be connected, or how they would be tracked. As a result, vulnerabilities could be introduced into the CCE network unnecessarily.

OMB requires a written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. [25] Where connection is authorized, controls are to be established which are consistent with the rules of the system in accordance with guidance from NIST. NIST provides guidance for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated by different organizations.[26] The guide states that it is critical that the organizations establish a formal written agreement outlining management, operation, and the use of any interconnections. These agreements usually take the form of an Interconnection Security Agreement (ISA). An ISA documents the requirements for connecting to networks/systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line.

ITS' ITA with the SCAs states that all computer equipment connected to the CCE network became the property of ITS at convergence and was to be recorded in its electronic inventory tracking system. However, not all computer equipment identified by OIG as connected to the CCE network belonged to the SCAs or was properly tracked in inventory (see Finding 4). Specifically, we found:

- Several SCA offices we visited were co-located with State Government controlled conservation district offices under informal partnership agreements with USDA's NRCS. At these locations, the State Government computer equipment was connected to the CCE network.

[25] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.
[26] NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," dated August 2002.

- One State SCA office we visited allowed the Office of General Counsel to connect its computer equipment to the CCE network.

ITS officials informed us there was no written agreement between ITS and the third-party organizations utilizing the CCE network. Therefore, no formal agreement existed outlining what services were to be provided, the type and quantity of network equipment that could be connected, or what network security practices were to be complied with. Further, ITS officials were unable to provide a listing of exactly how many computers these other organizations had connected to the CCE network and at which locations.

ITS officials acknowledged that this was a problem, but had difficulty in identifying and removing the access for these other organizations. Specifically, ITS stated that it was essential that local Conservation Districts be able to communicate with and share NRCS applications to carry out their functions, often including a bulk of the conservations programs in some counties. Further, ITS stated that they had consistently provided CCE guidance that describes how computer systems owned by partner agencies can be connected to the CCE network – including a requirement for up-to-date patches and anti-virus protection. However, ITS also estimated that 70 percent of the recent security incidents were the result of vulnerabilities on computer systems owned and operated by third-parties. These weaknesses put the security of the entire CCE network at risk of unauthorized access.

ITS also stated that before they could engage setting standards for IT and security requirements with these other organizations, the SCAs needed to enter into formal business partnership agreements, documented in a MOU, with these other organizations that outline the roles and responsibilities of the business relationship. Once these were established, ITS planned to have an ISA as an attachment to the MOU. While ITS could establish the criteria and would provide the actual IT services, the agreements themselves by NRCS are the only mechanisms that can be used to enforce compliance to the minimum standards. ITS did not believe they were in a position to negotiate directly with the conservation districts without NRCS coordination.

To correct this problem, the OCIO tasked the SCAs in April 2005 to start the process of formalizing the business partnerships by creating MOUs, beginning with the conservation districts. While OIG agrees this is a good first step, this process could take several months and overall CCE network security – including security for the other two SCAs - remains at risk without ISAs and enforcement policies in place.

## Recommendation No. 16

ITS should establish policies, procedures, and controls to ensure that third-party network devices (1) meet minimum security standards, and (2) are scanned for vulnerabilities and malicious code prior to being connected to the CCE network.

**Agency Response**

The SCAs have business relationships with outside agencies and organizations that require connectivity to the SCA network. In order for these staffs to successfully perform this work they need access to data and automated applications that are on the SCA network.

Limited protection for the SCA network is currently provided using capabilities that are in place to insure that connected systems are updated with virus protection. ITS has deployed and uses McAfee ePolicy Orchestrator for monitoring and updating antivirus protection on the over 50,000 workstations in the ITS active directory. The McAfee software product can be configured to monitor — in real time — for third party, "rogue" or unprotected systems that connect to the internal SCA network. While this capability is not yet fully functional, plans are in place to implement this protection within the SCA network.

Further, ITS is completing an analysis for establishing an enterprise-wide network access control solution for the USDA service center infrastructure. The USDA ITS manages and operates the service center infrastructure for FSA, NRCS, and RD. The service center infrastructure consists of over 2,900 service centers, State offices, large offices, and national headquarters. Network access control will benefit all three agencies, as it protects the shared network.

A network access control solution will ensure all endpoints meet security compliance requirements defined by OCIO-ITS before being granted access to the local area network and wide area network. Non-compliant endpoints will be quarantined and provided a means for mitigation. This defense will greatly reduce the insertion and propagation of viruses and worms in the service center infrastructure.

**OIG Position**

We concur with the management decision.

## Finding 8

## Physical and Environmental Controls Have Improved but Additional Steps are Still Needed

While improvements have been made since our prior audits of the individual SCAs', ITS needs to take additional actions to implement adequate physical and environmental controls over sensitive computer equipment located in field offices. SCA field office personnel in the offices we visited were generally unaware of good security practices and ITS field personnel took limited steps to correct obvious weaknesses. Further, ITS had no formal policies governing the physical and environment controls over its systems. As a result, ITS, and the SCAs they service, have reduced assurance that computer resources are adequately protected from physical and environmental vulnerabilities.

Security plans should address both physical and environmental controls according to NIST.[27] NIST goes on to state that security of information and the systems that process it is the fundamental management responsibility.[28] Specifically, physical and environment security measures should be taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. For example, NIST specifically requires physical access controls to address areas containing systems hardware (i.e., server cabinets or server rooms) and wiring used to connect systems, electric power service, air conditioning and heating, telephone lines, and data lines.[29]

Our visits to the State offices and 19 service centers in 3 States disclosed significant improvement in the physical security of servers in the field offices since 2003. In the 2003 audit, OIG identified servers stored in high traffic areas and lunchrooms without any physical protection.[30] During our current audit, however, all servers were either in server cabinets or dedicated server rooms. While this was a significant improvement over the servers being kept in the open, the server cabinets' backs were left off the server cabinet in almost every location. Additionally, the server cabinets were often used as storage areas for manuals, boxes, and office decorations, thereby potentially blocking airflow to the network equipment and increasing the risk of accidental damage to the servers and exposed cabling. Further, several servers, telephone panels, and computer line entry points were located under leaking sprinkler lines, next to hot water tanks, or near janitorial closets with

[27] NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems," dated December 1998.
[28] NIST SP 800-26, "Computer Security," dated November 2001.
[29] NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook," issued in October 1995.
[30] Audit Report No. 50401-50-FM, RD and FSA Financial Statement Field Confirmations for fiscal year 2003.

sinks further jeopardizing the physical security of the sensitive computer equipment. (See pictures in exhibit A.)

Additionally, our visit to one of the three WEB farms also disclosed inadequate physical and environmental controls over computer equipment. We found that ITS was not limiting access to the WEB farm server room to only those individuals with a need for access. For example, one individual with unrestricted access to the WEB farm server room told us that he had not accessed the computer room in almost a year and had no job responsibilities requiring him to access the server room. We also found that the air conditioning units were unable to cool the room adequately, resulting in several servers needing to be shut down. To help compensate for this deficiency, ITS used large industrial fans to provide additional cooling and each server had been assigned a shut down priority for use on days when the room exceeded acceptable temperature levels.

The SCAs field office personnel we interviewed were generally unaware of good physical security practices and did not see anything wrong with storing items on and around the server cabinets. At only 16 of the 25 locations we visited, had the SCAs prepared a security plan and risk assessment; however, those documents did not address physical security. Further, ITS field personnel were either unaware of the vulnerabilities, or were unsure what corrective steps to take. We found that almost all physical control weaknesses identified had existed before convergence; therefore, ITS field personnel were unsure of their authority to correct the vulnerabilities.

Limiting physical access to network systems and equipment should be the first step in securing any network. Physical access controls guard against theft, disablement, accidental damage, or other modification of network hardware that could lead to the loss of operation or critical data that resides on that hardware.

**Recommendation No. 17**

ITS should establish minimum physical security standards and implement controls to reasonably ensure that the standards are being followed.

**Agency Response**

As acknowledged by OIG, OCIO-ITS and the SCA worked together to mitigate the physical security issues in the service centers. ITWG procured and coordinated the installation of server cabinets in the local offices. However, due to the office layout, sometimes the server cabinets had to be placed into storage areas in less than optimal conditions. The ITWG and SCA diligently tried to remove sensitive equipment from high-traffic areas, but were not always able to get the cabinets out of common office space frequented by local staff. After the installation of the server cabinets there

was a period of time in which many servers overheated. To compensate for the heat build-up and to minimize service disruption, ITWG approved the removal of the cabinet backs. ITWG accepts this risk, and relies upon compensating controls such as the physical security of the building and the removal of the equipment from high-traffic public areas.

Regarding the WEB farm weaknesses, OCIO-ITS recognized that the server room visited by OIG has reached maximum capacity in regards to the cooling and humidity controls. OCIO-ITS conducted a feasibility study on the WEB farm locations this past spring and determined that the Fort Collins WEB farm will be relocated to the National Information Technology Center (NITC) location in Kansas City by the end of the year.

ITS has established minimum security controls as outlined in chapter 17 of the OCIO-ITS Security Policy Manual (Refer to Recommendation 2-1 Support Material). ITS will develop additional procedures and guidance for the design of proper space allowing for physical and environmental controls. The ITS Asset Management Branch will work with agencies during the renegotiation of leases for office space that will require providing adequately designed IT space with proper physical and environmental controls.

**OIG Position** We concur with the management decision.

**Recommendation No. 18**

ITS should provide guidance to its field personnel on actions to be taken when physical and environmental risks are identified during their site visits.

**Agency Response** OCIO-ITS also finds this situation where cabinets are being used as storage and that office storage was on top of or behind the cabinets unacceptable and will provide additional physical security guidance to the local IT staff to correct this deficiency. ITS will incorporate this guidance into that as explained in Recommendation 17.

**OIG Position** We concur with the management decision.

# Scope and Methodology

The scope of our review was nation-wide. We conducted this audit in accordance with "Government Auditing Standards."

Fieldwork for this audit was performed in Washington D.C., Kansas City, Missouri, Fort Collins, Colorado, and select State and service center offices in the states of Kansas, Texas, and Kentucky. Fieldwork was performed from January through May 2005.

To accomplish our audit objectives, we performed the following procedures:

- Interviewed key Information Technology Services and Service Center Agencies personnel at the national, State, and service center offices regarding policies, procedures, and controls over the convergence process and the management and security over Information Technology (IT) equipment.

- Reviewed existing policies and procedures governing the convergence process and security.

- Conducted a physical inventory of IT equipment at selected offices we visited and compared our results to ITS equipment tracking system.

- Evaluated the effectiveness of physical and environmental controls over IT equipment at select State and service center offices we visited.

- Conducted vulnerability scans using two commercially available software products that identify potential risk indicators in various operating systems.

# Exhibit A – Photos Taken at Various Service Center Agency Offices



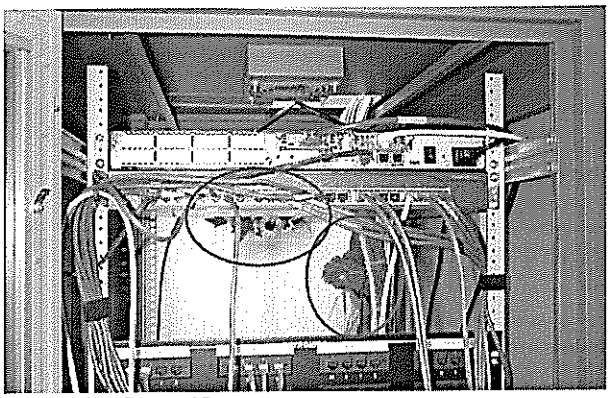


Photo 1 - Service Center 12:
The server cabinet's back is off and office decorations (hanging flowers and scare crow) are stored behind the cabinet.

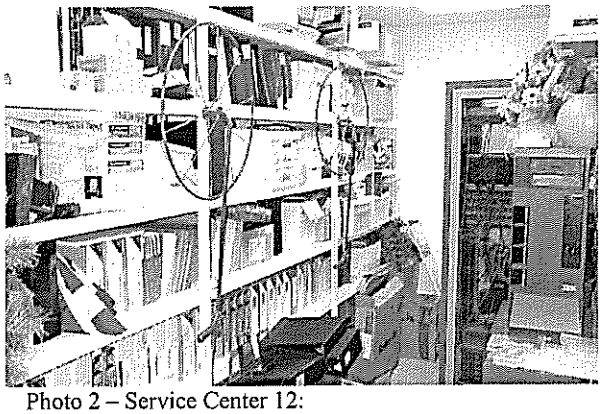


Photo 2 – Service Center 12:
The server cabinet is in the office storage/supply room. Office decorations are on top of the AS/400, blocking the cabinet door.

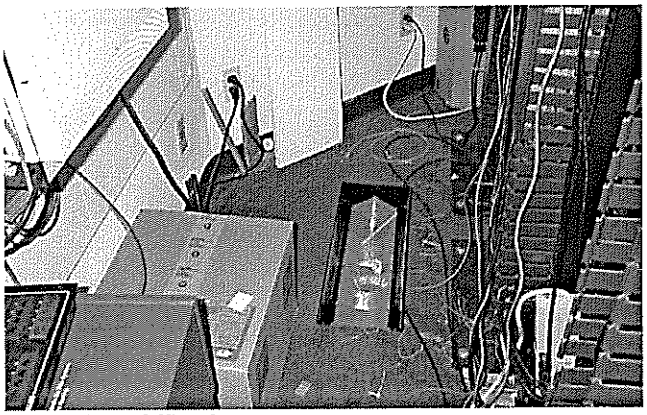


Photo 3 – State Office 6:
Behind the server racks is again used for storage. Employees walk over server plugs and cables to get to storage items.

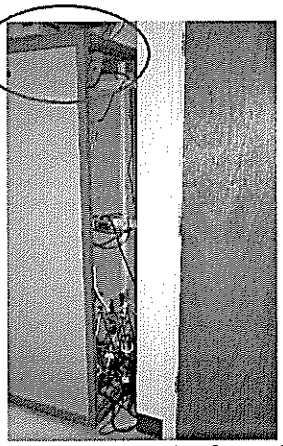


Photo 4 – Service Center 13:
The server cabinet's back is off. The janitor's closet is behind the server. Boxes are stored on top of the server cabinet.

Photo 5 – State Office 6:
Water sprinkler is leaking directly above the telephone, power, and computer lines.

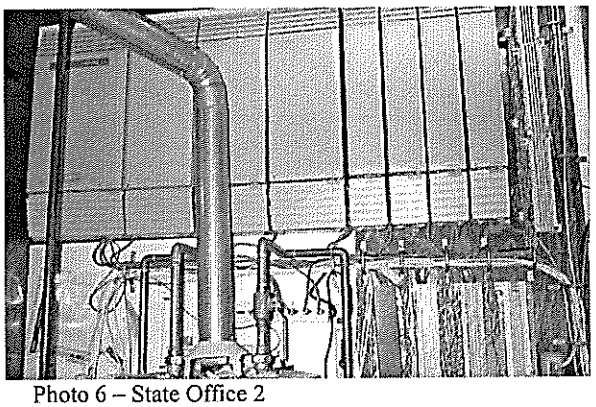


Photo 6 – State Office 2
Hot water tank and water supply lines are in front of the telephone and power lines.

USDA

United States
Department of
Agriculture

Office of the Chief
Information Officer

400 Independence
Avenue S.W.

Washington, DC
20250

August 15, 2005

TO: Robert W. Young
Assistant Inspector General for Audit
Office of Inspector General

FROM: Jerry E. Williams /s/
Deputy Chief Information Officer

SUBJECT: Office of Inspector General Audit Report #50501-3-FM
"Office of the Chief Information Officer Management and Security Over Information Technology Convergence – Common Computing Environment"

The Office of the Chief Information Officer (OCIO) is requesting management decision and closure on the following recommendations:

**Recommendation 1 – OCIO should rescind the unlimited accreditation for the two ITS systems we reviewed and place them in an Interim Approval to Operate status pending the resubmission of an accurately completed C&A package for each system. OCIO-ITS should also review the C&As of its other systems for similar weaknesses and make the necessary corrections.**

This ITS recommendation is based on an accreditation cycle Security Test & Evaluation (ST&E) for CCE and the Magic Service Desk (MSD) that is ongoing and scheduled to end by 09/30/2005. Therefore, it is not realistic or cost effective now to pull and revise the C&A 2004 documents reviewed during this audit. Many of these documents have already been revised for currency and will become deliverables to the ST&E process. The Risk Assessment has not been updated by ITS but will be updated during the ST&E process. The ITS focus needs to be on the current C&A activities.

The purpose of the CCE C&A at the time of submission was limited to the CCE General Support System, as was the Web Farm limited to the Web Farm GSS, and other GSSs under the Service Center Modernization Initiative (SCMI); they were not intended to reflect the ITS, as the re-organization did not occur until November 28, 2004. The CCE C&A documentation was reviewed by OIG and found as "incomplete and poorly documented". This was probably due in part to: 1) not all documents were reviewed by OIG, 2) the scope of the CCE GSS only covers the CCE portion, not the legacy hardware inherited by the ITS at convergence, 3) points of contact used during the OIG questioning session were not always those with technical knowledge, 4) the evolution of NIST

guidelines and USDA policy, and 5) CCE has been in a build-and-grow mode since the Information Technology Working Group (ITWG) was formed approximately four years ago and we see this as a developmental process that will respond to needs of our customers. Additionally, we followed all of the regulations per Department policies that were in effect at the time of our C&A activities. Also, there seems to be some misconceptions on the part of OIG in regard to terminology of the CCE GSS in relation to the other GSSs under the ITS umbrella.

Specifically, the risks identified in the Risk Mitigation Plan were entered into the Plan of Action and Milestones (POA&M) database, where responsibility was assigned and progress tracked, and target mitigation dates entered. The POA&M items are closed out as the mitigation efforts are completed. Upon migration of that data, the Risk Mitigation Plans were no longer kept current.

It must also be mentioned that, in general, with some comments being more specific than others, that the SCA ISSPMs, as well as some agency employees were not in favor with the concept of the move to the ITS organization and could have painted some negative concepts. If these issues had been discussed with the security personnel associated with the C&A documents, some of these issues may have been eliminated from the discussion draft.

Refer to the Certification and Accreditation General Support System Documentation for a list of all documents that were submitted to the OCIO C&A certification team. This document represents a table of contents for all the materials submitted during the C&A process. The first group of listed documents covers information that is common to all GSSs while the remaining documents listed are unique to each GSS.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 1-1 | Certification and Accreditation General Support System Documentation |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 2 – <u>ITS should establish policies, procedures and controls to ensure that the documentation supporting the C&A process is prepared in accordance with prescribed departmental and other Federal guidance and that the results of the review support the assessment.</u>**

The CCE C&A process began in August 2003 using NIST guidelines since USDA policy was not current. Within a few months, revised USDA policy became available so we re-

aligned our C&A procedures to meet the revised USDA policy, which held precedence over NIST guidance. That Department policy was still current at the time of submission of C&A materials to the C&A Certification Official/Team at USDA.

USDA has again recently revised their policy, DM 3555-000, Chapter 11, Part 1 (DM 3555-001) dated 07/01/2005. This policy, provided that no further changes are made as the result of a review period, will become a deliverable to the current ST&E process, which means that the latest USDA C&A procedures will be used in this C&A process which is scheduled for a 09/30/2005 completion.

ITS has performed a cross comparison of the policies which were used during our initial C&A 2004 against the policy in our current OCIO-ITS Security Policy Manual, Chapter 5, (Administrative Bulletin DR 3602-001) and to the latest USDA policy change. In the event that the USDA policy undergoes further revision during the ST&E process, those revisions will be implemented into the current ST&E process in as much as practical.

It is the standard practice of the Infrastructure Governance Division, Security Policy Branch to keep all ITS policies current and aligned to USDA policies. This is an ongoing effort. Refer to Recommendation No. 3 for additional information.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 2-1 | OCIO-ITS Security Policy Manual |
| 2-2 | Chapter 29 – Addition to OCIO-ITS Security Policy Manual with signature page. |
| 2-3 | Chapter 30 – Addition to OCIO-ITS Security Policy Manual with signature page. |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 3 – ITS should establish clear policies and procedures for all activities and functions it has assumed and include input from the SCAs when established policies impact their operations.**

The ITS Infrastructure Governance Division, Security Policy Branch concurs that establishing clear policies and procedures, with input from interested parties, is critical to efficient operation of any organization. The Security Policy Branch is currently working to develop a comprehensive set of policies and procedures relating to those security-related functional areas that have become ITS responsibility in the transition. The Security Policy Branch is actively seeking the input of the affected SCAs to ensure a symbiotic relationship with them to develop a comprehensive set of security policies and

procedures.

As of August 2, 2005, the Security Policy Branch has published the following procedure guides: Patch Deployment, Vulnerability Scanning, Incident Response and Access and Password Management security procedures as an addendum to the OCIO-ITS Security Policy Manual. Also, since the completion of the OIG audit, Chapter 29, Personnel Clearance Security Policy and Chapter 30, Licensed Software Security Policy of the OCIO-ITS Security Policy Manual have been published for use. Additional policies and procedures are being developed and finalized as the department develops and publishes its policies and procedures and as resources are available and committed to the effort.

Furthermore, examples of recent ITS and SCA joint ventures and information exchange include the Acting Associate CIO for OCIO-ITS monthly meetings with the Executive Board which include the CIO, ACIO and Agency Heads. He also meets with the Advisory Board which includes the CIOs and one state leader per Agency, normally on a monthly basis. These groups are demonstrated in the ITS organizational structure. Other cooperative efforts include training that is structured by ITS specifically for the agencies to use regarding access control where ITS provided the application training and the SCAs provided agency specific instruction. Other examples of cooperative efforts are included in document 3-5 listed below.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 3-1 | Patch Deployment Security Procedures Guide |
| 3-2 | Vulnerability Scan Security Procedures Guide |
| 3-3 | Incident Reporting, Handling and Response Security Procedures Guide |
| 3-4 | Access Control and Password Management Procedures Guide |
| 3-5 | Compilation of cooperative OCIO-ITS and SCA efforts |
| 2-1 | OCIO-ITS Security Policy Manual |
| 2-2 | Chapter 29 – Addition to OCIO-ITS Security Policy Manual with signature page. |
| 2-3 | Chapter 30 – Addition to OCIO-ITS Security Policy Manual with signature page. |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 4 – <u>ITS should negotiate separate MOUs or SLAs with each SCA.</u>**

**and establish policies and controls to ensure that the MOUs or SLAs are reviewed periodically and updated as necessary.**

ITS has already negotiated SLAs covering major aspects of security separately with each of the SCA. These SLAs have been in place since June of 2005. ITS is currently reviewing these SLAs, updating them as needed, and incorporating them into new and more comprehensive SLAs covering the full range of ITS services with each of the SCAs. This full range of services is currently under development and will be incorporated into the ITS Service Catalog. These SLAs will be embodied in separate MOUs to be negotiated with each of the SCA – and will supersede many of the interim terms included in the comprehensive MOU that was signed by all three SCAs in December, 2004. We expect to complete this negotiation process and to have these new and more comprehensive SLAs in place no later than the end of calendar year 2005 prior to the start of our initial informational billing process.

The periodic review process described above has been implemented and updated on a semi-annual basis. After the comprehensive SLAs have been negotiated with each SCA, the process that we have used to review and update the existing SLAs will be reviewed, modified as necessary, and incorporated into a formal policy and a set of procedures to ensure that all SLAs are reviewed periodically and updated as necessary. The following table shows planned actions and the associated anticipated completion dates that will address OIG concerns.

| Action | Completion Date |
|---|---|
| Updated SLAs completed (Draft) | 10/14/2005 |
| Separate MOUs/SLAs signed by SCA | 12/31/2005 |
| Periodic Review/Update Policies & Controls Formalized | 12/31/2005 |

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 4-1 | Service Level Agreement, Sanders |
| 4-2 | Service Level Agreement, Hannah |
| 4-3 | Service Level Agreement, Thomas |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 5 – ITS should establish policies and controls to ensure that clearly defined roles and responsibilities are identified, documented and relate to specific job performance standards.**

ITS has developed job descriptions for all ITS employees, including all security staff and field personnel. The process by which these job descriptions clearly identify, define and document the responsibilities of each role is supported by ITS Policy, "USDA/OCIO/ITS Performance Management Program Directive of May 18, 2005. The Performance Management Program has been developed and implemented, and this program clearly defines the performance standards required for each assigned role. Since convergence, 240 position descriptions have been developed by the ITS management and standardized for use across the ITS organization. These performance standards have been reviewed with all staff, signed, and formally put into place. Together, these documents clearly identify and document the roles and responsibilities of all staff and document job performance standards. As with any new organization, there will be some overlap before staff is familiar with new documentation and programs, but these issues are being systematically addressed through the customized job descriptions, policies and controls which ITS has already put into place.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 5-1 | ITS Performance Management Program Directive |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 6 – <u>ITS should conduct a complete inventory of items attached to the CCE network and develop policies, procedures and controls to ensure that inventory records are adequately maintained.</u>**

The ITS refers to the network as the Service Center Agency (SCA) Network, not necessarily the 'CCE Network'.

The Office of the Chief Information Officer, Information Technology Services recognizes the Department's Personal Property System (PROP) as the official tracking system for all accountable personal property. EATS is ITS' system for the ordering and deployment of information technology resources it was never intended to be an inventory tracking system. As a result of the audit, ITS recognizes the need to clearly define those items which will be tracked in EATS.

Attachment E of the Incidental Transfer Agreement (ITA)' signed in September of 2004 provides a listing of the type of equipment that is to be inventoried in EATS. After reviewing the list it is apparent that OCIO-ITS needs to re-evaluate the listing to ensure that that we are capturing the equipment necessary for the mission of the organization. Upon completion of the review we will develop written policy and procedures that

defines those items to be tracked and how they should be tracked. Once this is completed we will conduct a complete physical inventory of all items that have been defined as inventorial in EATS and also a complete physical inventory of all items in PROP. The following table shows planned actions and associated anticipated completion dates that will address OIG concerns.

| Action | Completion Date |
|---|---|
| Re-evaluate listing of those items to be tracked in EATS | October 2005 |
| Develop ITS policy as it relates to items to be tracked in EATS | January 2006 |
| Complete physical inventory of EATS and PROP | April 2006 |

OCIO-ITS requests Management Decision for this recommendation.

**Recommendation 7 – ITS should, through discussions with the SCAs, establish who owns IT equipment purchased by the SCAs after convergence. Once ownership is established, either (a) renegotiate the ITA to clearly address ITS ownership of this equipment or (b) enter into an Interconnectivity Service Agreement with the SCAs to ensure network security is maintained.**

Although OCIO-ITS has had discussions with the SCAs as it relates to ownership of equipment purchased after convergence, we have not formally documented our position on this issue. OCIO-ITS will develop a written supplement to the ITA that addresses the ownership issue of property that is purchased after the convergence. The OCIO-ITS position is that any equipment that is purchased after the convergence by the SCAs that is IT, telecommunications, or connects to the network is owned by ITS. The following table shows the planned action and associated anticipated completion dates that will address this OIG concern.

| Action | Completion Date |
|---|---|
| Write Supplement and Distribute | November 2005 |

OCIO-ITS requests Management Decision for this recommendation.

**Recommendation 8 – ITS should immediately address the high and medium vulnerabilities identified during our audit.**

OCIO-ITS provided all scan findings to the appropriate system administrators for immediate mitigation upon receipt from OIG. Actions were taken to mitigate many of the vulnerabilities found within the offices visited and similar actions were implemented as necessary to mitigate vulnerabilities across the enterprise.

As OIG stated, the majority of the vulnerabilities found were on "legacy" systems not previously managed by the Information Technology Working Group (ITWG) as a part of the CCE environment. Some of the vulnerabilities identified could not be immediately addressed and will require further coordination with the Service Center Agencies. For example, OIG found vulnerabilities on the UNIX platform currently still in-use by Natural Resources Conservation Service (NRCS) that can no longer be upgraded without adverse impact to the data stored on these systems. A second example, OIG found vulnerabilities on networked Xerox copiers. The maintenance agreements currently in effect on these devices are still managed by the Service Center Agencies.

The residual risks posed by these legacy systems will be monitored during monthly scan activity. OCIO-ITS will actively work with the Service Center Agencies to address upgrading the legacy systems or taking additional action to mitigate the risks posed by the current system. The action plan and timeframe for coordination are further explained in Recommendation 9 and 16.

Future action to address outstanding issues can be monitored under Recommendation 9 and/or 16 as all outstanding issues are relevant to legacy equipment and/or third-party network devices.

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 9 – ITS should (1) work with SCAs to identify and assume control over 'legacy' systems, (2) establish policies identifying minimum security requirements to be met for all devices attached to the CCE network, and (3) establish controls to ensure those policies are being followed.**

The ITS refers to the network as the Service Center Agency (SCA) Network, not necessarily the 'CCE Network'.

OCIO-ITS began the process of identifying "rogue" servers with the Service Center Agency representatives as a part of the Large Office migration process to the SCA network. This process was further developed with the help of the Service Center Agency Information Systems Security Program Managers (ISSPMs) during May and June, 2005 as a part of the President's Management Agenda (PMA) taskforce.

The OCIO-ITS Large Office team was focused on identifying and upgrading servers to ensure compatibility with the OCIO-ITS AgLO domain. The system administrators within each large office compiled a list of known servers within their respective locations. During the PMA initiative, each Agency ISSPM received the list of servers for the offices in which they previously oversaw for validation. OCIO-ITS also provided up-to-date scan information to correlate the inventory listings. The ISSPMs canvassed agency system administrators and relied on historical information to identify remaining servers and desktops which hosted production applications.

OCIO-ITS and the Service Center Agencies conducted several meetings to discuss the future approach in transitioning the responsibility for the rogue servers and the timeframes for implementation. It was agreed that each server/platform presented unique requirements and therefore each transition would have to be treated as a separate project. OCIO-ITS developed a server/application survey to gather additional information regarding the purpose of the server/application that could not be migrated, the current platform/patch level, current placement in the enterprise, etc. Based on this information, OCIO-ITS will develop an appropriate strategy.

As the rogue equipment is transitioned to OCIO-ITS administrators, the *OCIO-ITS Security Policy Manual* and applicable security procedures will establish the minimally acceptable security controls. Exceptions to the policy will be documented for formal waiver approval. Optimally, all equipment hosting production applications will be migrated to an existing web farm and will be managed under the current web farm security requirements. However, servers or applications that cannot be hosted securely will be quarantined from the rest of the enterprise and will be secured to the best of our ability given system limitations. OCIO-ITS will engage the SCAs in the placement decisions, will require the SCAs to formally accept residual risk associated with continuing to operate the applications hosted on non-confirming equipment, and will require the SCAs to apply for OCIO-Cyber Security and OCIO-ITS waivers as needed to cover the application and platform limitations. OCIO-ITS will monitor the security controls using the monthly vulnerability scan process recently established. Below is a summary of the OCIO-ITS action plan:

- OCIO-ITS and the Service Center Agencies identified and agreed upon a list of rogue servers/applications prior to June 30, 2005.
- OCIO-ITS provided the survey to the Service Center Agencies on July 8, 2005 for completion (See "Server Inventory Profile for ITS Hosting.")
- To date, OCIO-ITS is awaiting completion of the surveys for the servers/applications within the Washington area. (OCIO-ITS is focused on transitioning the production application equipment currently hosted by Rural Development in the Washington, D.C. offices as a priority, due to the volume and the pending network reconfigurations in that location. )
- Upon receipt of the completed surveys, OCIO-ITS is assessing the current situation to identify a feasible solution, and present it to Service Center Agency senior management for concurrence. A solution and associated timeframe will be presented by server/application for the WDC surveys by September 30, 2005.
- OCIO-ITS hopes to transition all equipment either into the Web Farm or a quarantined area by the end of the calendar year. However, until all information is gathered, it is difficult to develop solid timeframes.
- Actions within the additional large offices will follow the solutions developed to support the Washington, D.C. transition throughout FY 06. Based on the initial identification efforts, a small number of systems are hosted outside the Web Farm environments within the remaining large office locations.

In addition to the server/application identification and transition initiatives started as the "Rogue Server" project, OCIO-ITS is also continuing to work with Natural Resources Conservation Service (NRCS) leadership to retire legacy UNIX platforms that still reside in the State and County offices. The migration to Exchange email removed the dependency on the legacy UNIX mail servers, and a vast number have been taken out of service. However, a few pockets of users are continuing to rely on the UNIX platform for other purposes, so OCIO-ITS is addressing that situation in conjunction with NRCS management. OCIO-ITS anticipates retirement of all remaining UNIX mail servers by December 2005.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 9-1 | Server Inventory Profile for ITS Hosting |

OCIO-ITS requests Management Decision for this recommendation.

**Recommendation 10 – ITS should establish policies, procedures, and controls to ensure that system vulnerabilities are timely identified and mitigated.**

Upon convergence, OCIO-ITS assumed the responsibility for identifying and managing vulnerabilities within the network. Implementing a comprehensive, consistent process for vulnerability assessment is security priority for the new organization. Although OCIO Cyber Security and the Information Technology Working Group (ITWG) had security policies which defined the need to perform scans every 30 days, no formal infrastructure existed for the Service Center Agencies to consistently and uniformly scan the networks prior to convergence.

To resolve this important issue, OCIO-ITS developed a strategic architectural design to cover the OCIO-ITS network, including Large Offices and Field Service Centers, to ensure a uniform approach to scanning within the enterprise. Vulnerability scanning will be performed every 30 days per security policy which will encompass the OCIO-ITS networks, and include all workstations, servers, routers, switches, and printers for each General Support System (GSS). Standardized scanning servers and vulnerability scanning software was implemented throughout the existing OCIO-ITS network. Additionally, a centralized management system with well-defined reporting capabilities was implemented to track the prompt remediation of medium and high-level vulnerabilities discovered during the scanning process. A summary of the design is included below. For additional technical information see "Vulnerability Assessment Infrastructure Security Detailed Design Document" enclosed with this submission.

- **Field Service Center environment:**
  A total of twenty-six scanners were used to ensure comprehensive coverage without adversely affecting the network. Three scanners were deployed at each head end outside of the firewall. These scanners conduct concurrent scans for each domain (AgEast, AgCentral, AgWest, and AgLO) depending on the location of each scanner. Inside of the firewall a single scanner was deployed for scanning CCE infrastructure servers. Additionally, the large offices have Internet Scanner deployed locally. These servers will only scan resources within the specific large office networks in which they are deployed.

- **Web Farm Environment:**
  A total of nine scanners cover the Web Farm infrastructure; deployment consists of three scanners at each Web Farm site. This equipment deployed under the Service Center Agency management, and has been reviewed and updated to ensure consistency with the OCIO-ITS requirements.

- **Vulnerability Management System and Database:**
  Two servers reside within the Kansas City Web Farm that are used to centrally manage scan initiation, progress monitoring, and data collection for the enterprise.

OCIO-ITS has taken the following steps to address this vulnerability within the security program.

- OCIO-ITS Security Policy Manual formally issued in January 2005. Chapter 28 specifically outlines the requirements for Vulnerability scanning. (See OCIO-ITS Security Policy Manual Audit Extracts: Vulnerability Scan.")
- OCIO-ITS Operations Security received approval of the architecture and secured funds to procure the additional hardware in May 2005.
- OCIO-ITS issued approved Vulnerability Scanning Procedures in May 2005. (See "Vulnerability Scan Security Procedures Guide.")
- Architecture was implemented and proof-of-concept enterprise scans were completed in June 2005. (See "Discovery and Operating System Fingerprint Scan Executive Summary.")
- Full vulnerability scanning of the enterprise began in June 2005.
- Criteria testing for the ISS scan policy (standards the software product invokes when performing the assessment) concludes August 2005.
  - Continual testing and refinement of the scan policy will minimize false-findings.
  - Continual monitoring of network utilization based on scan policy settings will allow optimization of the scan schedule.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 10-1 | OCIO-ITS Security Policy Manual Audit Extracts: Vulnerability Scan |
| 10-2 | Vulnerability Scan Security Procedures Guide |
| 10-3 | Incident Reporting, Handling, and Response Security Procedures Guide |
| 10-4 | Vulnerability Assessment Infrastructure Security Detailed Design Document |
| 10-5 | Risk Acceptance Form with Instructions |
| 10-6 | Discovery and Operating System Fingerprint Scan Executive Summary for June, 2005 |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 11 – <u>ITS should establish policies, procedures, and controls to ensure that systems are properly maintained with patch management and post-implementation configuration management.</u>**

OCIO-ITS developed a series of documents outlining patch and configuration management policies and procedures. The OCIO-ITS Security Policy Manual (see "OCIO-ITS Security Policy Manual Audit Extracts: Server Management" and "OCIO-ITS Security Policy Manual Audit Extracts: Patch Management") and the Change Control Board (CCB) Charter establish the baseline for these initiatives. Over time, and as a result of the PMA taskforce, additional documentation has been formalized and is attached.

OCIO-ITS conducted a review of the patch strategies in-place throughout the environment to ensure proper notification, testing, and timely application of vendor patches. The enclosed whitepaper documents the current-state patch management methodologies used to update the General Support Systems managed by OCIO-ITS. (See "Patch Management Methodologies OCIO-ITS.")

The OCIO-ITS CCB oversees the change control process for OCIO-ITS by managing and providing direction for changes to baselines, architecture and their environments. Any specific changes that might affect or interface with the baselines are considered by the CCB. The objective of the OCIO-ITS CCB is to ensure that changes submitted for review follow the established Change Management Process, and contain all information necessary to determine the impact of the proposed change. It is the goal of the CCB to ensure that changes to the OCIO-ITS environment are well developed, well tested and well documented.

OCIO-ITS implemented the enterprise vulnerability scan capability for use as a tool to actively manage and monitor security risks within the environment. The vulnerability scan methodology allows for management oversight and control to ensure that all applicable security measures, including patch management and configuration management, have been taken to mitigate risks.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 11-1 | OCIO-ITS Security Policy Manual Audit Extracts: Server Management |
| 11-2 | OCIO-ITS Security Policy Manual Audit Extracts: Patch Management |
| 11-3 | Patch Deployment Security Procedures Guide |
| 11-4 | IOL Patch Activity Detail Template v2.12 |
| 11-5 | Standard Patch Management Process |
| 11-6 | Patch Management Methodologies OCIO-ITS |
| 11-7 | Change Control Board Charter |
| 11-8 | ITS Enterprise Change Management Team Charter |
| 11-9 | Change Management Procedure Manual |
| 11-10 | Release Management Process (Draft) |
| 11-11 | Request for Change Form (RFC) |
| 11-12 | Service Support Processes Change Management, Release Management, and Configuration Management |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 12 – ITS should identify all individuals authorized dial-up and VPN access to the CCE network, and establish policies and controls to ensure that dial-up and VPN accesses are controlled as effectively as regular access permissions.**

The ITS refers to the network as the Service Center Agency (SCA) Network, not necessarily the 'CCE Network'.

The access control process for remote connections transitioned from the Service Center Agencies to OCIO-ITS on June 30, 2005. While, OCIO-ITS hosted the capability for remote connectivity since inception, access management was still controlled by the agency security offices post-convergence. OCIO-ITS began a review of the accounts in conjunction with the Agency ISSPMs in July 2005. During this initial review, individual

accounts were correlated to the employing agency to assist in future reporting efforts. OCIO-ITS is also analyzing the security controls in-place on the different VPN servers to develop a common set of security controls for the enterprise.

OCIO-ITS implemented an Agency System Access Authorization Request (ASAAR) process, including documentation, to control all future account activity for dial-up and VPN account creation, modification, and deletion. (See "OCIO-ITS Security Operations Center Remote Access Procedure Detail.")

OCIO-ITS has the following plan of action:

- Assumed responsibility for access management for VPN and dial-up users on June 30, 2005
- Implemented an account management process on July 1, 2005.
- Provided a list of VPN/Dial-up users to agency ISSPMs - July 2005
- Update account identification (agency affiliation) – August 2005
- Implement a process to provide monthly reports by Agency for management review – September 2005.
- Update and finalize VPN/Dial-up security controls documentation – October 2005.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 12-1 | OCIO-ITS Security Operations Center Remote Access Procedure Detail (Draft) |

OCIO-ITS requests Management Decision for this recommendation.

**Recommendation 13 – <u>ITS should establish policies and controls to ensure that all employees, including employees with full administrative access, are granted access that adheres to the concept of least privilege.</u>**

OCIO-ITS has completed several projects to address the OIG concerns regarding account management and excessive privileges.

- OCIO-ITS initiated a 100% review of all administrative accounts throughout the enterprise (See "Memorandum, Data Call for Administrative Privileges.") A process for future periodic reviews is under development.
  - The Technical Services Division reviewed all administrative accounts within Active Directory and removed administrative permissions from all non-ITS employee accounts.

- The Infrastructure Operations Division reviewed administrative account privileges within the Web Farm, Geospatial Data Centers, and Telecommunications environment and removed accounts as appropriate.

- Active Roles was implemented. Domain administrator rights have been restricted, so that administrators now only have authority within the Group with which they are assigned. (See "State IT Post-ActiveRoles Procedures FINAL" and "News Flash State IT Admin Roles project.")
- The Service Center Agencies were provided a listing of accounts from Active Directory for a 100% account validation in April 2005. Changes were implemented in June 2005. One agency alone identified over 650 accounts that were removed from the system. A process has been implemented to provide the SCA ISSPMs monthly reports on user accounts to ensure timely review by agency management. (See "OCIO-ITS Access Account Verification.")
- OCIO-ITS implemented the SAAR process to control all future account creations, modifications, and deletions on July 1, 2005. Account requests must be submitted to OCIO-ITS via the approved automated form from an agency designated point of contact (POC). A request for elevated/administrative privileges requires a secondary approval from the Agency security staff, and concurrence from OCIO-ITS management. (See "Magic Service Desk ASAAR Form Screen Shots" and "Access Process Diagram.")

OCIO-ITS required the 100% account reviews both internally, and to our Customer Agencies to establish a secure baseline for account management. A process was implemented to control all future account management requests, and administrative privileges were significantly reduced throughout the enterprise. In addition, controls were put into place to review and verify account changes by performing management reviews of the monthly access listings.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 13-1 | OCIO-ITS Security Policy Manual Audit Extracts: Authorization and Access Control |
| 13-2 | Access and Password Management (Users, Non-Users, and Administrative Accounts) Security Procedures Guide |
| 13-3 | Access Process Diagram |
| 13-4 | State IT Post-ActiveRoles Procedures FINAL |
| 13-5 | News Flash State IT Admin Roles project |
| 13-6 | Access Control Training Methods |
| 13-7 | Agency System Authorization Access Request User's Guide (Draft) |

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 13-8 | OCIO-ITS Access Account Verification |
| 13-9 | Magic Service Desk ASAAR Form Screen Shots |
| 13-10 | Memorandum, Data Call for Administrative Privileges |
| 13-11 | Data Call Template |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 14 – ITS should establish policies and controls to ensure that the accounts of separated employees are timely identified and removed.**

The OCIO-ITS management staff is responsible for initiating the termination of employee access upon separation. The contracting officer technical representative (COTR) is responsible for notification of contractor separation. Notifications can be submitted using the ASAAR process, and immediate removals can be escalated via the ITS Service Desk and direct contact to system administrators.

OCIO-ITS also has a process with the Bureau of Public Debt (BPD) to ensure timely confirmation of ITS employee separation. BPD provides a weekly notice to OCIO-ITS of all e52 actions; that list is culled to identify termination/separation actions. The Operations Security Branch is notified and access removal is confirmed as a compensating control.

Agency employee and contractor separations are managed by the Agency security offices, who notify OCIO-ITS via the ASAAR process. In the event of an immediate separation, the Agencies can expedite account removal by contacting the ITS Service Desk. The Agencies utilize the monthly user account reports as a compensating control to ensure all accounts are removed from the system.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 14-1 | Service Level Agreement, Sanders |
| 14-2 | Service Level Agreement, Hannah |
| 14-3 | Service Level Agreement, Thomas |
| 14-4 | All USDA Moves Report 07/19/2005 |
| 14-5 | ITS Contractor Spreadsheet 06/22/05 |
| 14-6 | Notification of Employee on LWOP 5/5/2005 |

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 14-7 | Notification of Employee Resignations 5/18/2005 |
| 14-8 | Notification of Employee Retirements 6/3/2005 |
| 14-9 | Notification of Security Employee Retirement or Termination 8/1/2005 |

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Recommendation 15 – ITS should remove all generic user accounts and establish policies and controls to ensure that no new generic user accounts are created.**

OCIO-ITS is currently reviewing all instances of generic and service accounts across the enterprise. OCIO-ITS held internal meetings with the Key Stakeholders who currently require generic/service accounts beginning in Feb of 2005. The Operations Security Branch (OSB) and the Interoperability Lab (IOL) worked collectively to identify and document all of these accounts across the Active Directory domain. During this review, OCIO-ITS identified 14 Active Directory administrator-level service accounts and 60 Domain administrator level service accounts. (See "Guide, Service Accounts.")

A review of existing generic and service accounts is underway to determine alternative solutions for service accounts. All OCIO-ITS generic accounts follow a secure naming structure with enhanced passwords following security best practices In certain instances where alterative accounts, or methods can not be utilized OCIO-ITS will use our internal Rick Acceptance Process, to accept these risk as they are critical to ensuring certain applications across the enterprise continue to function.

OCIO-ITS has the following plan of action:

- OCIO-ITS is reviewing policies and procedures to guide the enterprise in the use of service and other non-user account management. – September, 2005
- OCIO-ITS will continually produce monthly reports off all know Generic/Service Level accounts. – October, 2005
- OCIO-ITS will leverage our enterprise scanning solution to validate these accounts as well as identify non-certified or accepted accounts. – October, 2005
- OCIO-ITS will perform research, identify any generic user accounts and implement any necessary controls on these accounts. – January, 2006

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 15-1 | Guide, Service Accounts |

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 2-1 | OCIO-ITS Security Policy Manual |

OCIO-ITS requests Management Decision for this recommendation.

**Recommendation 16 – ITS should establish policies, procedures and controls to ensure that that third-party devices (1) meet minimum security standards, and (2) are scanned for vulnerabilities and malicious code prior to being connected to the CCE network.**

The ITS refers to the network as the Service Center Agency (SCA) Network, not necessarily the 'CCE Network'.

**Background**

The Service Center Agencies have business relationships with outside agencies and organizations that require connectivity to the SCA Network. For example, NRCS has an established partnership with local Conservation Districts in each county where NRCS provides services. In many counties the Conservation Districts (a unit of county government) have staffs that work alongside the NRCS employees and perform the same work activities. In order for these staffs to successfully perform this work they need access to data and automated applications that are on the SCA Network. Memorandums of Understanding (MOUs) are in effect between each of these county Conservation Districts and the NRCS state management that supports that county. The MOUs define general working relationships and the basis for sharing of resources between NRCS and the Conservation Districts. Although they currently do not specifically address access to the SCA Network, the MOUs provide the framework under which this access is currently provided. Both Rural Development and the Farm Service Agency also work with external organizations which must access the SCA Network to complete critical business activities to support USDA program delivery. Under this basis, third party connectivity to the SCA Network has been permitted in order to further the capabilities of the Service Center Agencies to conduct their business activities in cooperation with these organizations.

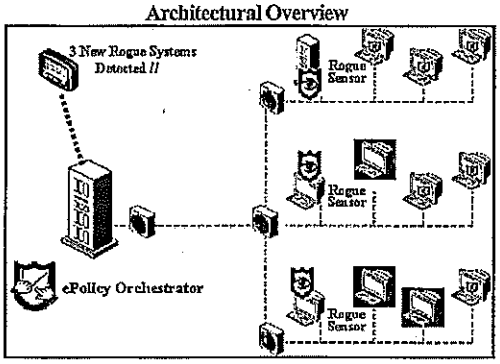
**Current Capabilities**

Limited protection for the SCA Network is currently provided using capabilities that are in place to insure that connected systems are updated with virus protection. ITS has deployed and uses McAfee ePolicy Orchestrator for monitoring and updating antivirus protection on the over 50,000 workstations in the ITS Active Directory. The McAfee software product can be configured to monitor — in real time — for third party, rogue or unprotected systems that connect to the internal SCA Network. This feature is designed to improve policy compliance within enterprises by identifying all rogue or unprotected systems and allowing ePolicy Orchestrator to invoke a policy-based response on that system. While this capability is not yet fully functional, plans are in place to implement this protection within the SCA Network.

At the heart of this solution is a software-based sensor that uses passive monitoring to detect all systems participating in the network. Specifically, the sensor listens for L2 broadcasts. Computers participating on a network tend to broadcast frequently, especially when first joining a network, so new systems are usually detected by the sensor within seconds of first connecting to the network. Sensors deployed throughout the enterprise report all detected systems to the ePolicy Orchestrator server, and the server determines which of those devices are rogue.

The following diagram gives an overview of rogue system detection architecture.

Architectural Overview




At least one rogue system sensor must be deployed in each L2 segment throughout the enterprise, because sensors detect systems by broadcasts (which are only propagated through an L2 segment). As systems are detected, the sensor uses HTTPS protocol to send messages describing the systems to the ePolicy Orchestrator server. The sensor makes no attempt to classify systems as rogue or managed; it simply reports everything it sees.

When the ePolicy Orchestrator server receives a **system detected** message, it inspects the database to determine whether the system should be classified as rogue or managed. A system is considered rogue if:

1. It is not present in ePolicy Orchestrator's database of managed systems, and
2. The system's ePolicy Orchestrator agent is not actively communicating with the server.

ePolicy Orchestrator enforces policy on systems through a small software agent running on managed systems. Those agents are responsible for periodically checking in with the ePolicy Orchestrator server to obtain the most recent policy settings. Failure of an agent to check in and confirm its policy settings is considered a breach of policy because the ePolicy Orchestrator server cannot confirm that the system's settings are up to date.

The detected system's MAC (Media Access Control) address is used as the primary key when searching through ePolicy Orchestrator's managed system database; the hostname can also be used to reduce false-positives in cases when a system uses multiple network interfaces, such as a laptop with both wireless and Ethernet.

A sensor reports on a given system the first time it is detected (for example, when the first broadcast packet containing that system's MAC address is received by the sensor) and then no more frequently than once per a configurable time period (set to one hour by default). Each time the server receives a **system detected** message for a previously detected system, it recalculates and updates the rogue status and other information associated with the system.

**Future Plans**

ITS is completing an analysis for establishing an enterprise-wide network access control solution for the USDA Service Center Infrastructure. The USDA Information Technology Services (ITS) manages and operates the Service Center Infrastructure for the Farm Service Agency (FSA), Natural Resource and Conservation Service (NRCS), and Rural Development (RD). The Service Center Infrastructure consists of over 2,900 Service Centers, state offices, large offices, and national headquarters. Network access control will benefit all three agencies, as it protects the shared network.

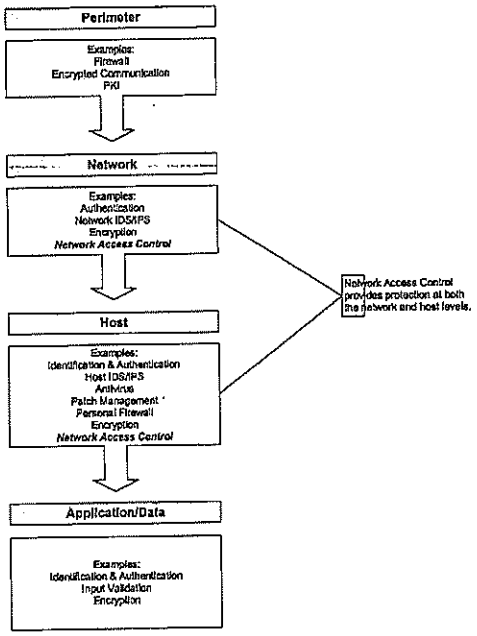
A network access control solution will ensure all endpoints meet security compliance requirements defined by OCIO-ITS before being granted access to the Local Area Network and Wide Area Network. Non-compliant endpoints will be quarantined and provided a means for mitigation. This defense will greatly reduce the insertion and propagation of viruses and worms in the Service Center Infrastructure.

The following core functions define the network access control:

- **Policy management** – Defines security configuration requirements for endpoints attempting to access the network.
- **Baseline comparison** – Determines the security state of an endpoint that is attempting network access.
- **Access control** – Based on the results of the baseline comparison, places the endpoint in a network access state (e.g., full access, quarantine).
- **Mitigation** – Updates a blocked or quarantined endpoint to an acceptable status.

ITS will use a layered security model to identify the protection a network access control solution. In a layered security model, one layer provides support for the layer above it and protection for the layer below it. Different types of attacks, vulnerabilities, and threats exist at differing layers within the computing environment. A layered approach provides an organization the flexibility to implement the level of security corresponding with the objectives of the system, thus resulting in a cost-effective security program. This approach presents the layers that defend an organization's resources. Within this model, there are four basic layers: perimeter, network, host, and the applications/data.

Diagram below illustrates a layered approach to enterprise security architecture. The model is not a comprehensive model to endpoint security, rather a tool to illustrate how network access control will fit in.




The perimeter layer provides the logical boundary of what the organization can control. Conventional security strategies have focused on protecting the perimeter and controlling what traffic is allowed into enterprise networks. This can be accomplished with firewalls, encryption, and public key infrastructures.

The next layer is the network, which refers to the internal LAN and WAN. Within the network there are many different types of hardware and software running to protect the network, including network virus filters, intrusion detection/prevention systems, and authentication servers. Network access control solutions protect the LAN and the WAN by only allowing compliant endpoints from gaining access to the network. This defense protects the network from being attacked by comprised machines.

The host layer includes servers, workstations, mobile devices, printers, and any other devices connecting to the network. Typically, an organization has the least amount of control over its hosts. Protection strategies include antivirus, host-base intrusion detection systems, and personal firewalls. Network access control solutions protect the host by

verifying that required endpoint security measures, such as antivirus configurations meet the organizations policies.

The last layer is the application and data layer; which is crucial as it contains the information required to achieve business objectives. Technologies used to secure this layer include identification and authentication, access control and encryption.

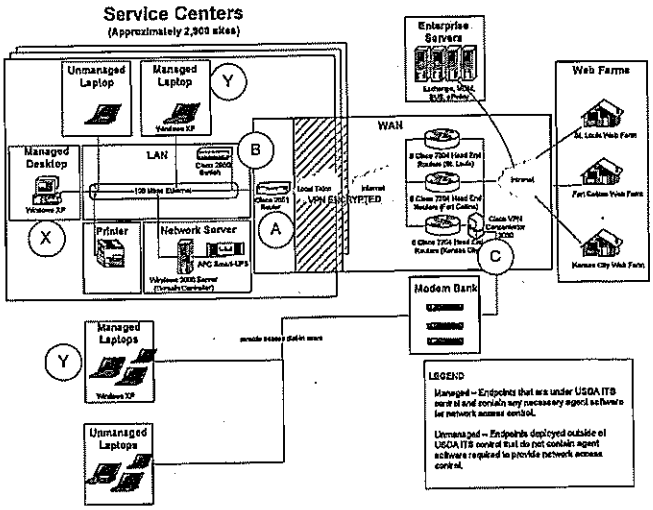
In summary, the diagram above illustrates that a network access control solution provides protection for both the network and the hosts. A solution will also protect at the network level by blocking non-compliant endpoints at entry points. Any non-compliant endpoints will be quarantined until mitigated. This defense will greatly reduce the number of viruses and worms introduced to the network. Network access control will also protect endpoints by enforcing the organization's security policy, such as antivirus configurations and operating system levels. This host protection will prevent the corruption of endpoints from viruses and worms.

Network access control will provide significant protection within the Service Center Infrastructure, specifically at the host and network levels. This section illustrates the protection provided by network access control in the Service Center Infrastructure.

As the Service Centers work with several partners outside of the USDA, it is necessary for a network access control solutions to provide functionality for both USDA-owned endpoints and endpoints that are considered guests to the network. This market survey differentiates managed and unmanaged endpoints through the following definitions:

- **Managed** – A managed system is under OCIO-ITS control and contains any necessary agent software for network access control. Managed systems also receive regular operating system and anti-virus updates.
- **Unmanaged** – An unmanaged system is outside of OCIO-ITS control and does not contain agent software required to provide network access control. OCIO-ITS is totally dependent on the system owner to manage the operating system and anti-virus updates because ITS cannot manage that system since it is beyond ITS control.

Agent software is installed on managed endpoints to gather security compliance credentials. In the case of unmanaged endpoints, agent software is not installed. To provide functionality for unmanaged endpoints, a solution may provide either an ActiveX download or Java applet to collect credentials of the endpoint for baseline comparison testing. The intended network access solution will ensure that any endpoint, managed or unmanaged, meets OCIO-ITS policies before gaining access to the network.
In the a diagram below of the Service Center Infrastructure, this figure is used to illustrate the position of a network access control solution in the Service Center Infrastructure.




A network access control solution will protect both the Service Center Agency Network and OCIO-ITS desktops and laptops. A solution protects the network by blocking non-compliant endpoints at entry points. Network access control protects the endpoints by enforcing security policy, for example, antivirus software must be installed, and configurations are up to date.

A network access control solution secures the Service Center Agency Network by permitting only compliant endpoints to access the internal network. An ideal solution will provide protection for both managed and unmanaged endpoints. While solutions vary, access control can be enforced at the router level (point A) or switch level (point B) for the users connecting through the Service Centers. For users connecting through the Service Centers, non-compliant endpoints (managed and unmanaged) will be quarantined to a separate network subnet. Solutions that enforce access control at the router level will allow non-compliant endpoints to be on the LAN; however, these endpoints will not gain access to the WAN and will not infect other Service Centers. Solutions that enforce at the switch level, will not gain access to the LAN, and cannot infect other endpoints connected to the LAN.

For remote access users, access control can be enforced after the modem bank through an inline device or on the VPN concentrator (point C). Before gaining access to the internal network, endpoints will be scanned for compliance and any non-compliant endpoint will not be quarantined.

Because only those endpoints equipped with antivirus configurations and operating

system levels will access to the Service Center Agency Network, theoretically the number of viruses and worms introduced to the network will be significantly reduced.
In addition to securing the network, a network access control solution will ensure that USDA workstations (point X) and laptops (point Y) are compliant with security policies. If a managed endpoint falls out of compliance, a network access control solution will remediate an endpoint into compliance. This added protection will prevent viruses from corrupting USDA endpoints and will limit the frequency of disruptions to business operations.

**Estimated Completion Date:** March, 2006

As OCIO-ITS selects an approach to establishing an enterprise network access solution, the following steps should be considered:

- **Design session with vendors – September, 2005**
  Network access control solutions are complex in their designs and integrate closely with several components of architecture. It is necessary for OCIO-ITS to engage in design discussions with vendors to confirm the feasibility of the solutions in the Service Center Infrastructure. Deployment options and functionality for each solution should be confirmed with the vendor.
- **Pilot – October, 2005**
  Based on the design sessions, the OCIO-ITS should pilot at least two of the five vendor solutions identified.
- **Cost analysis – November, 2005**
  There are several components in network access control solutions and consequently, multiple pieces of the infrastructure are affected. OCIO-ITS should perform a cost analysis to determine the full expense of each network access control solution, including any necessary changes to the infrastructure such as IOS upgrades for network hardware.
- **Short and long-term plans – March, 2006**
  Acquisition of the network access control solution is expected to be completed by the end of this calendar year, or by December, 2005. Implementation of the solution will then be carried out so that the solution is fully functional by March, 2006.

In the long term the complete network access control solution will be monitored and evaluated for effectiveness after implementation. In addition, new products or solutions that are introduced into the marketplace will be evaluated for their applicability to meeting the business needs of ITS and the Service Center Agencies. The initial solution will be replaced if a more economical and functional solution becomes available.

OCIO-ITS requests Management Decision for this recommendation.

**Recommendation 17 – <u>ITS should establish minimum physical security standards and implement controls to reasonably ensure that the standards are being followed.</u>**

As acknowledged by Office of Inspector General (OIG), OCIO-ITS (formerly Information Technology Working Group (ITWG)) and the Service Center Agencies (SCA) worked together to mitigate the physical security issues in the Service Centers. ITWG procured and coordinated the installation of server cabinets in the local offices. However, due to the office layout, sometimes the server cabinets had to be placed into storage areas in less than optimal conditions. The ITWG and SCA diligently tried to remove sensitive equipment from high-traffic areas, but were not always able to get the cabinets out of common office space frequented by local staff. After the installation of the server cabinets there was a period of time in which many servers overheated. To compensate for the heat build-up and to minimize service disruption, ITWG approved the removal of the cabinet backs. ITWG (and now OCIO-ITS) accepts this risk, and relies upon compensating controls such as the physical security of the building and the removal of the equipment from high-traffic public areas.

Regarding the Web Farm weaknesses, OCIO-ITS recognized that the server room visited by OIG has reached maximum capacity in regards to the cooling and humidity controls. OCIO-ITS conducted a feasibility study on the Web Farm locations this past spring and determined that the Fort Collins Web Farm will be relocated to the National Information Technology Center (NITC) location in Kansas City by the end of the year.

ITS has established minimum security controls as outlined in Chapter 17 of the OCIO-ITS Security Policy Manual (Refer to Recommendation 2-1 Support Material). ITS will develop additional procedures and guidance for the design of proper space allowing for physical and environmental controls. The ITS Asset Management Branch will work with agencies during the renegotiation of leases for office space that will require providing adequately designed IT space with proper physical and environmental controls. This guidance document will be developed by February 28, 2006.

The following is a list of supporting documents to this response:

| Supporting Documentation | |
|---|---|
| **Document Number** | **Document Title** |
| 2-1 | OCIO-ITS Security Policy Manual |

OCIO-ITS requests Management Decision for this recommendation.

**Recommendation 18 – <u>ITS should provide guidance to its field personnel on actions to be taken when physical and environmental risks are identified during their site visits.</u>**

OCIO-ITS also finds this situation where cabinets are being used as storage and that office storage was on top of or behind the cabinets unacceptable and will provide additional physical security guidance to the local information technology (IT) staff to

correct this deficiency. ITS will incorporate this guidance into that explained in recommendation 17.

Future action to address outstanding issues can be monitored under Recommendation 17 as all outstanding issues are relevant to the physical security standards.

OCIO-ITS requests Management Decision and Closure for this recommendation.

**Summary of Actions**
Below is a summary of the OCIO-ITS requested response actions to the OIG recommendations for the subject audit report.

| OCIO-ITS Summary of Recommendations | |
|---|---|
| **Recommendation Number** | **Requested Action** |
| 1 | Closure |
| 2 | Closure |
| 3 | Closure |
| 4 | Closure |
| 5 | Closure |
| 6 | Management Decision |
| 7 | Management Decision |
| 8 | Closure, but roll part into 9 |
| 9 | Management Decision |
| 10 | Closure |
| 11 | Closure |
| 12 | Management Decision |
| 13 | Closure |
| 14 | Closure |
| 15 | Management Decision |
| 16 | Management Decision |
| 17 | Management Decision |
| 18 | Closure, but roll part into 17 |

If additional information is needed, please have a member of your staff contact Sherry Linkins, OCIO Audit Liaison, on telephone number (202) 720-9293.

Attachments

cc: Bryce Eckland, Assistant Regional Inspector General, OIG-FIO, Kansas City, MO
Richard K. Roberts, Acting Associate CIO, OCIO-ITS, Washington, D.C.
Sherry Linkins, Audit Liaison, OCIO, Washington, D.C.