United States Department of Agriculture
Office of Inspector General

International Technology Services Selected Controls Audit

Audit Report 88501-0001-IT

March 2012

United States Department of Agriculture
Office of Inspector General
Washington, D.C. 20250

DATE: March 20, 2012

AUDIT NUMBER: 88501-0001-IT

TO: Christopher L. Smith
Chief Information Officer
Office of the Chief Information Officer

ATTN: Denice Lotson
Acting Agency Audit Liaison

FROM: Gil H. Harden
Assistant Inspector General
for Audit

SUBJECT: International Technology Services Selected Controls Audit

This report presents the results of the subject review. Your written response to the official draft, dated February 23, 2012, is included in its entirety in an exhibit in this report. Excerpts of your response and the Office of Inspector General's position are incorporated into the applicable sections of the report.

We accept management decision for Recommendations 1 through 7, all of the recommendations noted in this audit. In accordance with Departmental Regulation 1720-1, final action needs to be taken within 1 year of each management decision to prevent being listed in the Department's annual Performance and Accountability Report.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions.

Table of Contents

Executive Summary 1
Recommendation Summary 2
Background and Objectives 3
Section 1: Communication and Oversight 4
Finding 1: Lack of Communication and Oversight 4
Recommendation 1 5
Recommendation 2 5
Recommendation 3 5
Recommendation 4 6
Recommendation 5 6
Recommendation 6 6
Recommendation 7 7
Scope and Methodology 8
Abbreviations 9
Exhibit A: ITS Field Sites Visited by OIG 10
Exhibit B: Guidance 11
Exhibit C: Review of Selected Controls 12
Agency's Response 25

International Technology Services Selected Controls Audit – 88501-0001-IT

Executive Summary

This report represents the results of our review of the selected controls at the Office of the Chief Information Officer (OCIO)/International Technology Services (ITS). Specifically, we reviewed selected controls as needed for the fiscal year (FY) 2010 financial statement audits. The controls were selected by the Office of the Inspector General (OIG) contracted Independent Professional Auditors (IPA) in order to meet financial statement standards. Our audit was intended to provide the IPAs with an analysis of the selected controls for their use in the FY 2010 financial statement audits. We issued the findings from our control testing (see exhibit C) to the IPAs and ITS in October 2010. This report is to finalize the recommendation portion of the review for Department of Agriculture's (USDA) tracking and closure.

ITS was established to oversee the general support system for the co-located field offices of the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD), collectively referred to as the Service Center Agencies (SCA).[1] A key element for the success of the Service Center Modernization Initiative was the replacement of aging business and technology systems through information technology (IT) convergence. This IT convergence would provide a common IT infrastructure for FSA, NRCS, and RD allowing them to share data among themselves and their customers, and to streamline business processes. Additionally, the IT convergence project was to provide the infrastructure needed to ensure that customers could conduct business electronically with the SCA.

Many of the exceptions identified in this report were caused by a lack of communication and oversight between ITS and the SCA. This occurred because Service Level Agreements (SLA) between ITS and the SCA did not meet National Institute of Standards and Technology (NIST) guidelines.[2] For example, the agreements did not contain explicit definitions of both ITS' and SCA's roles and responsibilities. As a result, the network and systems may be exploitable, jeopardizing the integrity of SCA data and ITS system resources.

Although ITS made improvements in documenting policies and procedures, we found that ITS' issues noted in our previous audit continued to exist.[3] We found that policies and procedures were lacking in some areas and/or were not being followed. We found policies and procedures lacking in critical areas such as: scanning of computer systems for known vulnerabilities, disaster recovery, physical security, and user access to computer systems. Policies and procedures

---

[1] OMB Circular No. A-130, Appendix III (December 24, 1985), defines a general support system as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
[2] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems* (December 2007).
[3] Audit Report No. 88501-7-FM, *General Controls Review-Fiscal Year 2006 Office of the Chief Information Officer-Information Technology Services* (March 2007).

addressing these areas need to be developed in accordance with Federal guidelines and need to include implementation plans.

Recommendation Summary

OCIO/ITS needs to develop and/or implement effective controls over security scanning, access authorization, and two-factor authentication.

Agency Response

OCIO concurred with the finding contained in this report and stated that a Plan of Action and Milestones (POA&M) was created to address each of the seven recommendations.

OIG Position

We accept management decision for all seven recommendations presented in this report.

Background and Objectives

Background

OCIO/ITS' common computing environment was implemented in November 2004. The environment was built on a common IT investment strategy, telecommunications capability, office automation tools, administrative applications, and an IT support organization. ITS' purpose is to optimize data, equipment, and people sharing. ITS' common computing environment 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.

ITS provides IT service and support to over 40,000 USDA SCA employees and their networked computers, IT equipment, and the environment that the SCA networks and applications operate on. The SCA retained responsibility for its applications. Therefore, review and/or testing of the SCA applications were not covered in this audit. However, the general support system owned by ITS has a material impact on the security of SCA applications.

In March 2007, OIG issued Audit Report No. 88501-7-FM, *General Controls Review-Fiscal Year 2006 Office of the Chief Information Officer-Information Technology Services*, which contained 13 recommendations. ITS generally concurred with our findings and agreed to implement the recommendations.

Objectives

The audit objectives were to perform testing necessary to express an opinion regarding:

- Whether the policies and procedures were suitably designed to provide reasonable assurance that the specified control objectives were complied with satisfactorily; and

- The operating effectiveness of the specified control structure policies and procedures in achieving specified control objectives.

Section 1: Communication and Oversight

Finding 1: Lack of Communication and Oversight

This report presents the results of our review of selected controls at OCIO/ITS. Specifically, we reviewed selected controls as needed for the FY 2010 financial statement audits. The controls were selected by the contracted IPAs in order to meet financial statement standards. Our audit was intended to provide the IPAs with an analysis of the selected controls for their use in the FY 2010 financial statement audits. We discussed the results of our control testing in detail with ITS on October 4, 2010. ITS generally concurred with the issues noted and we incorporated the agreed upon changes. We issued the findings from our control testing (see exhibit C) to the IPAs and ITS in October 2010. This report is to finalize the recommendation portion of the review for USDA's tracking and closure.

ITS was established to oversee the general support system for the co-located field offices of FSA, NRCS, and RD, collectively referred to as the SCA.[4] A key element for the success of the Service Center Modernization Initiative was the replacement of aging business and technology systems through IT convergence. This IT convergence would provide a common IT infrastructure for FSA, NRCS, and RD allowing them to share data among themselves and their customers, and to streamline business processes. Additionally, the IT convergence project was to provide the infrastructure needed to ensure that customers could conduct business electronically with the SCA.

Many of the exceptions identified in this report were caused by a lack of communication and oversight between ITS and the SCA. This occurred because SLAs between ITS and the SCAs did not meet NIST guidelines.[5] For example, the agreements did not contain explicit definitions of both ITS' and the SCAs' roles and responsibilities. As a result, the network and systems may be exploitable, jeopardizing the integrity of the SCAs' data and ITS' system resources.

Although ITS made improvements in documenting policies and procedures, we found that ITS' issues noted in our previous audit continued to exist.[6] We found that policies and procedures were lacking in some areas and/or were not being followed. We found policies and procedures lacking in critical areas such as: scanning of computer systems for known vulnerabilities, disaster recovery, physical security, and user access to computer systems. Policies and procedures addressing these areas need to be developed in accordance with Federal guidelines and need to include implementation plans.

---

[4] OMB Circular No. A-130, Appendix III (December 24, 1985), defines a general support system as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
[5] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems* (December 2007).
[6] Audit Report No. 88501-7-FM, *General Controls Review-Fiscal Year 2006 Office of the Chief Information Officer/Information Technology Services* (March 2007).

The seven recommendations below have not been identified in previous audits. Our previous report on ITS controls issued in 2007,[7] contained 13 recommendations; all of which have been closed and are considered implemented.[8] However, we noted several areas that warrant corrective action. Based on our test of controls, we recommend the following.

Recommendation 1

Implement effective controls to guarantee that all SCAs are conducting vulnerability scanning on a monthly basis.

Agency Response

OCIO has created a POA&M to address this recommendation.[9]

OIG Position

We concur with management decision.

Recommendation 2

Develop and implement formal procedures for antivirus scanning, including procedures for verifying that antivirus scans are being conducted on all systems in a timely manner.

Agency Response

OCIO has created a POA&M to address this recommendation.

OIG Position

We concur with management decision.

Recommendation 3

Develop and implement policies and procedures establishing firewall controls that specify user access, rule set review, and configuration testing.

---

[7] Audit Report No. 88501-7-FM, *General Controls Review-Fiscal Year 2006 Office of the Chief Information Officer-Information Technology Services* (March 2007).
[8] Departmental Regulation 1720-001, *Audit Follow-up and Management Decision* (November 2, 2011)
[9] Office of Management and Budget (OMB) Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004) requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been found. POA&Ms identify tasks needing to be accomplished to assist agencies in assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. It details resources required to accomplish the elements of the plan, milestones for meeting the task, and scheduled completion dates for the milestones.

Agency Response

OCIO has created a POA&M to address this recommendation.

OIG Position

We concur with management decision.

Recommendation 4

Develop and implement policy and procedures for user access authorization.

Agency Response

OCIO has created a POA&M to address this recommendation.

OIG Position

We concur with management decision.

Recommendation 5

Enforce the implementation of encryption for removable media.

Agency Response

OCIO has created a POA&M to address this recommendation.

OIG Position

We concur with management decision.

Recommendation 6

Update policy and procedures to mandate the use of two-factor authentication for remote access.

Agency Response

OCIO had created a POA&M to address the issue noted in this recommendation and has, as part of the management decision process, provided evidence that supports closing the POA&M.

OIG Position

Based on the information provided to OIG in its February 23, 2012 response and subsequent correspondence, OIG concurs with management decision.

Recommendation 7

Develop a plan to deploy Homeland Security Presidential Directive-12 (HSPD-12) identification cards for two-factor authentication.

Agency Response

OCIO had created a POA&M to address the issue noted in this recommendation and has, as part of the management decision process, provided evidence that supports closing the POA&M.

OIG Position

Based on the information provided to OIG in its February 23, 2012 response and subsequent correspondence, OIG concurs with management decision.

Scope and Methodology

The period of our review was FY 2010. We performed a review of selected controls as prescribed by the IPAs performing the FY 2010 financial statement audits. We also assessed ITS' implementation of prior OIG audit recommendations related to the scope of the audit. The population of the audit consists of all ITS locations and a group of locations were selected from the total population by geographic location and SCA presence where field tests were performed. We also performed a review to determine whether the policies and procedures had been placed in operation, and whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified. Evidence to support our findings was gathered in the form of audit logs, access logs, physical observations, agency policies, and agency procedures. This audit did not involve any review and/or testing of SCA applications since ownership and responsibility for the applications remained with the SCA.

Various Departmental Regulations and Manuals related to IT security were used as a guideline for this review. Also, Government-wide publications such as HSPD-12, *Critical Infrastructure Identification, Prioritization, Protection*, and various Government Accountability Office (GAO) security reviews were used as needed. We compared existing policies and procedures to NIST SP 800-53 controls to determine whether the procedures have been implemented, and if so, are being followed. For a detailed listing of guidance refer to exhibit B.

We conducted this review in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Abbreviations

CCB..... Change Control Board
CM ..... Capacity Management
FSA ..... Farm Service Agency
FY ..... Fiscal Year
GAO..... Government Accountability Office
HSPD-12..... Homeland Security Presidential Directive-12
ID ..... User Identification
IDS ..... Intrusion Detection System
IPA ..... Independent Professional Auditors
IT..... Information Technology
ITS..... International Technology Services
NIST..... National Institute of Standards and Technology
NRCS ..... Natural Resources Conservation Service
OCFO..... Office of the Chief Financial Officer
OCIO..... Office of the Chief Information Officer
OIG ..... Office of Inspector General
OMB ..... Office of Management and Budget
OS ..... Operating System
POA&Ms ..... Plan of Action and Milestones
RD..... Rural Development
SAAR..... System Authorization Access Request
SCA..... Service Center Agencies
SLA..... Service Level Agreement
UPS ..... Uninterruptible Power Supply
USDA..... Department of Agriculture
VPN..... Virtual Private Network

Exhibit A: ITS Field Sites Visited by OIG

- Conway, Arkansas
- Ft. Smith, Arkansas
- Russellville, Arkansas
- Butler, Missouri
- Carthage, Missouri
- Springfield, Missouri
- Billings, Montana
- Bozeman, Montana
- Enid, Oklahoma
- Muskogee, Oklahoma
- Stillwater, Oklahoma
- Oregon City, Oregon
- Portland, Oregon
- Tualatin, Oregon
- Brush Prairie, Washington
- Casper, Wyoming

Exhibit B: Guidance

The following GAO, Department Manuals, OMB Directives, and NIST Special Publications were used as criteria for the ITS Selected Controls Review audit.**GAO**

- *GAO's Standards for Internal Control in the Federal Government* (November 1999)
- Title 5, C.F.R., Section 731.106

NIST Guidance

- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook* (October 1995)
- NIST SP 800-35, *Guide to Information Technology Services* (October 2003)
- NIST SP 800-40, *Creating a Patch and Vulnerability Management Program* (November 2005)
- NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy* (September 2009)
- NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security* (June 2009)
- NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems* (December 2007)
- NIST SP 800-61 rev. 1, *Computer Security Incident Handling Guide* (March 2008)
- NIST SP 800-92, *Guide to Computer Security Log management* (September 2006)

Department Manuals

- Department Manual 3505-001, *USDA Cyber Security Incident Handling Procedures* (March 20, 2006)
- Department Manual 3530-001, *USDA Vulnerability Scan Procedures* (July 20, 2005)

Departmental Regulations

- Departmental Regulation 3170-001, *End User Workstation Stnds* (December 12, 2007)
- Departmental Regulation 1720-001, *Audit Follow-up and Management Decision* (November 2, 2011)

ITS Special Publications

- ITS SPB 29-001, *Personnel Clearance (ITS)* (June 25, 2005)
- ITS SPB 28-001, *ITS Vulnerability Scan and Assessment Policy* (September 2007)

ITS Regulations

- ITS Regulation 8003-001-R, *Access Account Provisioning and Password Policy* (December 16, 2008)
- ITS Regulation 8007-001-R, *Data Management Policy* (December 16, 2008)
- ITS Regulation 8203-003-R, *ITS Incident Response, Handling, and Reporting Procedure* (April 17, 2009)

Exhibit C (pages 12 through 24) is not being publicly released due to its sensitive security content.

USDA'S
OFFICE OF THE CHIEF INFORMATION OFFICER'S
RESPONSE TO AUDIT REPORT

United States Department of Agriculture

Office of the Chief Information Officer

1400 Independence Avenue S.W.

Washington, DC 20250

February 23, 2012

TO: Gil H. Harden,
Assistant Inspector General for Audit
Office of the Inspector General

FROM: Christopher L. Smith /s/
Chief Information Officer

SUBJECT: OIG Audit No. 88501-0001-IT
International Technology Services Selected Control Audit

International Technology Services (ITS) has reviewed the discussion draft report on the subject audit. Responses for each of the seven (7) recommendations follow.

Recommendation 1:

Implement effective controls to guarantee that all SCAs are conducting vulnerability scanning on a monthly basis.
ITS Response: We concur with this finding. A POA&M has been created.
The number is 16815.

Recommendation 2:

Develop and implement formal procedures for antivirus scanning, including procedures for verifying that antivirus scans are being conducted on all systems in a timely manner.
ITS Response: We concur with this finding. A POA&M has been created.
The number is 16822.

Recommendation 3:

Develop and implement policies and procedures establishing firewall controls that specify user access, rule set review, and configuration testing.
ITS Response: We concur with this finding. A POA&M has been created.
The number is 16816.

Recommendation 4:

Develop and implement policy and procedures for user access authorization.
ITS Response: We concur with this finding. A POA&M has been created.
The number is 16812.

Recommendation 5:

Enforce the implementation of encryption for removable media.
ITS Response: We concur with this finding. A POA&M has been created. The number is 16813.

Recommendation 6:

Update policy and procedures to mandate the use of two-factor authentication for remote access.
ITS Response: We concur with this finding. POA&M 8656 was open on 4/1/2008 and closed on 8/15/2011.

Recommendation 7:

Develop a plan to deploy Homeland Security Presidential Direction-12 (HSPD-12) identification cards for two-factor authentication.
ITS Response: We concur with this finding. POA&M 8656 was open on 4/1/2008 and closed on 8/15/2011.

Activities taken to address Recommendations 6 & 7:

- ITS Deployed Linc Pass cards services. See artifact titled, "HI STE Results Report Excerpt of Weaknesses. doc" for IA-02 testing results.
- Completed rollout of Enterprise AC/NAC 2-Factor Remote Access.
- OCIO-SSP ST&E FY07 IA-2 -- Designed and implemented multi factor authentication to ensure that remote access conforms to OMB 06-16.
- ActivClient client deployed to all ITS managed workstations.

If you have any questions concerning this report, please contact Barry Lipscombe, ISSPM, at (970) 295-5460; or Nancy Herbert, Deputy ISSPM at (816) 926-3836.

cc: Denice A. Lotson, Audit Liaison, OCIO

Informational copies of this report have been distributed to:

Government Accountability Office (1)

Office of Management and Budget (1)

Office of the Chief Financial Officer (1)
Director, Planning and Accountability Division

To learn more about OIG, visit our website at
www.usda.gov/oig/index.htm

How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
In Washington, DC 202-690-1622
Outside DC 800-424-9121
TDD (Call Collect) 202-690-1202

Bribes or Gratuities
202-720-7257 (Monday–Friday, 9:00 a.m.– 3 p.m. ET)

The U.S. Department of Agriculture (USDA) prohibits discrimination in all of its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex (including gender identity and expression), marital status, familial status, parental status, religion, sexual orientation, political beliefs, genetic information, reprisal, or because all or part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD). USDA is an equal opportunity provider and employer.