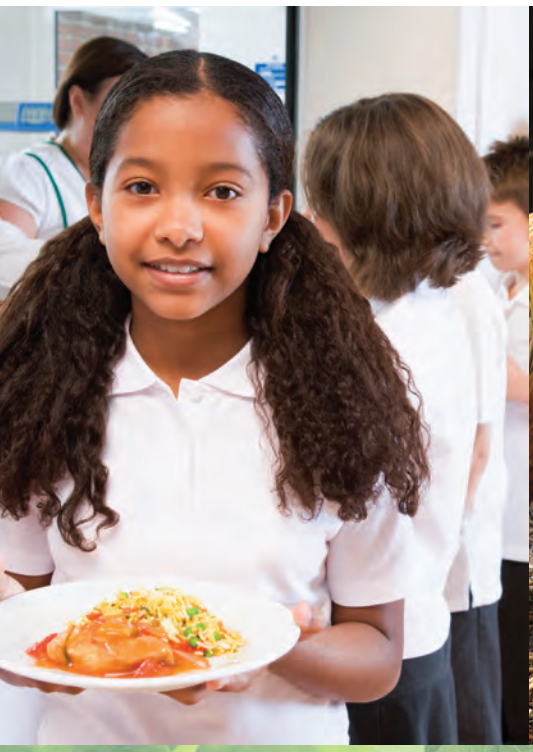
USDA

United States Department of Agriculture
Office of Inspector General

Review of Selected Controls at the National Information Technology Center



Audit Report 88401-0001-11

September 2012

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

DATE: September 26, 2012

AUDIT NUMBER: 88401-01-11

TO: Cheryl Cook
Acting Chief Information Officer
Office of the Chief Information Officer

ATTN: Denice Lotson
Audit Liaison Officer
Office of the Chief Information Officer

FROM: Gil H. Harden
Assistant Inspector General
for Audit

SUBJECT: Review of Selected Controls at the National Information Technology Center

This report presents the results of the subject review. Your written response is included in its entirety in the 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 Recommendation 1, noted in the report. 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. In regard to Recommendations 2 and 3, please furnish a reply within 60 days describing the corrective actions taken or planned, and timeframes for implementing the recommended actions. Please note that the regulation requires management decision to be reached on all recommendations within 6 months from the report issuance.

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

Table of Contents

Review of Selected Controls at the National Information Technology Center (88401-0001-11)

Executive Summary

This report presents the results of our review of selected controls at the Office of the Chief Information Officer/National Information Technology Center (OCIO/NITC). Specifically, our review was to assess whether selected controls at OCIO/NITC were in place and operating effectively in support of key Department of Agriculture (USDA) financial systems from October 1, 2011, through July 1, 2012, with a focus on the production and backup environments for the Office of the Chief Financial Officer/National Finance Center's (OCFO/NFC) EmpowHR application.[1]

OCIO/NITC's mission is to provide reliable and cost effective information technology solutions to achieve mission performance and program delivery for its USDA and non-USDA customers. As a customer of OCIO/NITC, OCFO/NFC relies on the effectiveness of the controls tested during our review.

We identified three exceptions during the course of our review. The following summarizes the exceptions identified in Finding 1 of this report.

- OCIO/NITC had not developed formal, documented policy and procedures for incident response, but instead relied on policy and procedures created for a separate entity.

- OCIO/NITC did not track critical vulnerability mitigation actions identified through monthly scanning through the use of Plan of Action and Milestones (POA&M). While we found that OCIO/NITC did use an internal system to track and remediate identified vulnerabilities, it did not meet Departmental guidelines for the Federal Information Security Management Act reporting.

- The alternate processing site at the George Washington Carver Center in Beltsville, Maryland, did not provide adequate protection from water damage.

[1] EmpowHR is a web-based human resource system for personnel action processing, position management, and training.

Recommendation Summary

We recommended that OCIO/NITC:

- Develop and implement formal documented incident response policy and procedures.
- Implement the Department's POA&M process for critical vulnerabilities existing more than 30 days or, alternatively, obtain a waiver.
- Develop and implement compensating controls to mitigate the risk of water damage at the George Washington Carver Data Center.

Agency Response

OCIO/NITC concurs with the finding and recommendations included in the report and has developed a plan of specific action to address Recommendation 1 including estimated completion dates. Additionally, OCIO/NITC concurs with Recommendations 2 and 3 and is currently identifying and evaluating options to ensure compliance with FISMA reporting requirements, and implementing compensating controls to mitigate the risk of water damage, respectively.

OIG Position

We accept management decision on Recommendation 1 presented in the report. With regard to Recommendations 2 and 3, management decision should be achievable upon review of the specific plans and timeframes for corrective action.

Background and Objectives

Background

The Office of the Chief Information Officer/National Information Technology Center (OCIO/NITC) has provided services as a federated data center[2] since 1973. Its mission is to provide reliable and cost-effective information technology solutions to achieve effective mission performance and program delivery for the Department of Agriculture (USDA), its agencies, and other clients. OCIO/NITC operates a Level IV data center, which utilizes state-of-the-art, enterprise class infrastructure technologies to deliver optimal yet cost effective solutions. OCIO/NITC's secure information technology infrastructure consists of virtualized mainframe and midrange platforms, as well as virtualized network and storage infrastructure. The systems and applications managed by OCIO/NITC are national in scope, mission critical, and essential for the operations of the United States Government. Data center services include infrastructure as a service, platform as a service, managed hosting, and professional services.

OCIO/NITC provides managed hosting services to many customers, internal and external to USDA, including the Office of the Chief Financial Officer/National Finance Center (OCFO/NFC). As a provider of payroll/personnel and application hosting for all of USDA, as well as approximately 130 non-USDA government entities, NFC is subject to an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Controls review. That review identifies OCIO/NITC as a subservice provider of NFC. The services provided include hosting hardware/software associated with the production and backup environments of NFC's personnel system, EmpowHR, to include access controls, configuration management, and contingency planning. The result of the SSAE 16 review, along with results of testing at any agency subservice provider, has a significant impact on the financial statements of user agencies. Financial data processed by the NFC, along with additional agency-specific financial systems hosted by OCIO/NITC, are material to the financial statements; therefore, the controls over those systems play an integral part in assessing the completeness, accuracy, and integrity of USDA financial data.

Objective

The objective of our review was to assess whether selected controls at OCIO/NITC were in place and operating effectively in support of key USDA financial systems[3] from October 1, 2011, through July 1, 2012, with a focus on the production and backup environments for the OCFO/NFC's EmpowHR application.

[2] A federated data center is a centralized data center, providing participating entities the ability to operate their own environment with a degree of independence in the overall management of their server infrastructure.
[3] Key USDA financial systems include EmpowHR, and agency specific financial systems for Rural Development, Farm Service Agency, Commodity Credit Corporation, and the Forest Service.

Section 1: Selected IT Controls Need Strengthening

Finding 1: Selected IT Controls Need Strengthening

During our review, we identified three control areas that need strengthening at OCIO/NITC. Specifically, OCIO/NITC had not developed formal written policy and procedures for incident response; it did not create, track, and mitigate critical vulnerabilities identified during monthly scans through the use of Plan of Action and Milestones (POA&M); and protection from water damage at an alternate processing site was lacking. These conditions occurred because management believed alternative policies or practices in place were sufficient. As a result, customer systems could be vulnerable for the items discussed below.

- We requested policies and procedures for incident response at OCIO/NITC. OCIO/NITC was unable to provide a formal documented incident response policy. Instead, OCIO/NITC provided the Department's Standard Operating Procedures (SOP) for Reporting Security and Personally Identifiable Information Incidents.[4] The purpose of the SOP is to document the incident management procedures for the Department's Computer Incident Response Team, which does not apply at the agency level. Departmental policy requires each agency to establish, support, and maintain their own internal policies and procedures or assign a team to support prompt, effective, and efficient resolution of computer security incidents.[5] Without a formal documented incident response policy, appropriate action for a suspected security incident could be delayed.

- We analyzed monthly scan results of EmpowHR devices[6] and subsequent remediation activities for identified vulnerabilities and found that OCIO/NITC does not track and mitigate critical vulnerabilities through the use of POA&Ms. Departmental policy requires all USDA agencies to perform vulnerability scans on a monthly basis. It further requires a POA&M to be developed, in accordance with Federal Information Security Management Act (FISMA) reporting requirements, for any unresolved critical vulnerabilities existing more than 30 days from the date of the scan.[7] While we found that OCIO/NITC used its internal Remedy system to track and remediate identified vulnerabilities, Remedy does not meet departmental guidelines for FISMA reporting. Additionally, all policy exceptions must be submitted directly to the Associate Chief Information Officer for Cyber Security. OCIO/NITC had not obtained a waiver from the requirement to create POA&Ms. Without tracking vulnerabilities in POA&Ms, departmental oversight can be hindered.

- Additionally, we performed testing of OCIO/NITC's contingency planning controls for OCFO/NFC's EmpowHR application and found the potential for water damage to system devices at OCIO/NITC's alternate processing site, located at the George Washington Carver Data Center, in Beltsville, Maryland. During a walk-through of the data center, we noted overhead water pipes were present and staff did not have access to the water shut-offs.

[4] SOP-ASOC-001, *Agriculture Security Operations Center Computer Incident Response Team: Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents* (June 9, 2009).
[5] Department Manual (DM) 3505-001, *USDA Cyber Security Incident Response Procedures* (March 20, 2006).
[6] Scan reports from October 2011 through February 2012.
[7] DM 3530-001, *USDA Vulnerability Scan Procedures* (July 20, 2005).

Without access to a shut-off valve by data center staff or alternative compensating controls in place, the risk of damage to system equipment is increased.

Recommendation 1

Develop and implement formal documented incident response policy and procedures.

Agency Response

OCIO/NITC concurs and has created a POA&M to address this recommendation by December 21, 2012.

OIG Position

We concur with management decision.

Recommendation 2

Implement the Department's POA&M process for critical vulnerabilities existing more than 30 days or, alternatively, obtain a waiver.

Agency Response

OCIO/NITC concurs and is currently identifying and evaluating vulnerability POA&M options that ensure continued compliance with FISMA reporting requirements.

OIG Position

Management decision should be achievable upon review of the specific plans and timeframes for corrective action.

Recommendation 3

Develop and implement compensating controls to mitigate the risk of water damage at the George Washington Carver Data Center.

Agency Response

OCIO/NITC concurs and is currently implementing compensating controls to mitigate the risk of water damage at the George Washington Carver Data Center.

OIG Position

Management decision should be achievable upon review of the specific plans and timeframes for corrective action.

Scope and Methodology

The period of our review was from October 1, 2011, through July 1, 2012. OCIO/NITC provides managed hosting services to many customers internal and external to USDA, including the OCFO/NFC. As a provider of payroll/personnel and application hosting for all of USDA, as well as approximately 130 non-USDA government agencies, NFC is subject to an annual Statement on Standards for Attestation Engagement No. 16 (SSAE 16) Controls review. The result of the SSAE 16 review, along with results of testing at any subservice provider, has a significant impact on the financial statements of user agencies. Financial data processed by the NFC, along with additional agency-specific financial systems hosted by OCIO/NITC, are material to the financial statements; therefore, controls over those systems play an integral part in assessing the completeness, accuracy, and integrity of USDA financial data.

Our review focused on the specific controls[8] managed by OCIO/NITC as a subservice provider for OCFO/NFC's EmpowHR system. These controls, which are identified in Exhibit A, include access controls, configuration management, and contingency planning. The controls tested were also applicable to other key financial systems hosted at OCIO/NITC. We performed our review at the OCIO/NITC Data Center in Kansas City, Missouri and two alternate centers located in St. Louis, Missouri and Beltsville, Maryland.

We obtained supporting documentation in the form of server settings, access logs/reviews, training records, and agency policies and procedures, as well as physical observations and interviews with agency personnel. Our results were discussed with OCIO/NITC as we worked to obtain concurrence on exceptions noted.

Various Departmental Regulations and Manuals related to information technology security were utilized for this review. We compared the results of the audit tests against departmental, agency, and National Institute of Standards and Technology (NIST) guidance. Guidance used during the course of the audit included:

- NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009
- DM 3505-001, USDA Cyber Security Incident Response Procedures (March 20, 2006)
- DM 3530-001, USDA Vulnerability Scan Procedures (July 20, 2005)

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.

[8] Controls listed in OCFO/NFC's System Description as managed by OCIO/NITC.

Abbreviations

DM ..... Department Manual

FISMA ..... Federal Information Security Management Act

NFC ..... National Finance Center

NIST ..... National Institute of Standards and Technology

NITC ..... National Information Technology Center

OCFO ..... Office of the Chief Financial Officer

OCIO ..... Office of the Chief Information Officer

OIG ..... Office of Inspector General

POA&M ..... Plan of Action & Milestones

SOP ..... Standard Operating Procedures

SSAE ..... Statements on Standards for Attestation Engagements

USDA ..... Department of Agriculture

Exhibit A: Office of Inspector General Tests of the Office of the Chief Information Officer/National Information Technology Center Controls

The subsequent sections of the report's exhibit A (pages 8 through 13) are not being publicly released due to the sensitive security content.

USDA'S NATIONAL INFORMATION TECHNOLOGY CENTER RESPONSE TO AUDIT REPORT

United States Department of Agriculture

Office of the Chief Information Officer

National Information Technology Center

8930 Ward Parkway
Kansas City, MO
64114-3363

P.O. Box 419205
Kansas City, MO
64141-6205

September 21, 2012

TO: Tracy A. LaPoint
Deputy Assistant Inspector General for Audit
Office of the Inspector General

FROM: Kent W. Armstrong /s/
Associate Chief Information Officer
National Information Technology Center

SUBJECT: OIG Audit Number 88401-0001-11
Review of Selected Controls at the National Information Technology Center

The National Information Technology Center (NITC) has reviewed the draft report on the subject audit. Responses for the three recommendations follow.

Recommendation 1:

Develop and implement formal documented incident response policy and procedures.

NITC Response: We concur with this finding. The NITC is in the process of documenting and implementing formal cyber incident response policy and procedures. NITC has created POAM number 18042 with an expected date of completion of December 21, 2012 to remediate the issue.

Recommendation 2:

Implement the Department's POA&M process for critical vulnerabilities more than 30 days old or, alternatively, obtain a waiver.

NITC Response: We concur with this finding. The NITC is currently identifying and evaluating vulnerability POA&M options that ensure continued compliance with FISMA reporting requirements.

Recommendation 3:

Develop and implement compensating controls to mitigate the risk of water damage at the George Washington Carver Data Center.

NITC Response: We concur with this finding. The NITC will implement compensating controls to mitigate the risk of water damage at the George Washington Carver Data Center. Estimated date of completion is 10/30/12.

If you have any questions, you may contact me at (816) 926-6501 or have a member of your staff contact Greg Schmitz at (816) 926-2356.

cc: Jim Steven, Deputy Associate Chief Information Officer, NITC
cc: Denice A. Lotson, Audit Liaison, OCIO
cc: Kathy Donaldson, OCFO

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

Email: usda.hotline@oig.usda.gov
Phone: 800-424-9121 Fax: 202-690-2474

Bribes or Gratuities:
202-720-7257 (24 hours a day)