UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S ENTERPRISE SERVER INFRASTRUCTURE GENERAL SUPPORT SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-CI-00-11-016

Date: 5/16/2011

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S ENTERPRISE SERVER INFRASTRUCTURE GENERAL SUPPORT SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-CI-00-11-016

Date: 5/16/2011

This final audit report discusses the results of our review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Enterprise Server Infrastructure General Support System (ESI). Our conclusions are detailed in the "Results" section of this report.

During this audit we documented the following opportunities for improvement:

- The ESI information system security plan (ISSP) was prepared in accordance with the format and methodology outlined in NIST guidance. However, the ESI ISSP does not contain details of the interconnections between ESI and other systems as required by NIST SP 800-18.
- Several weaknesses identified during disaster recovery exercises have not been addressed or remediated.
- The Office of the Chief Information Officer (OCIO) has not formally documented common controls provided by ESI or implemented a process to share this information with the owners of other applications relying on this support system.

We also determined that the following elements of the ESI security program appear to be in full FISMA compliance:

- A security certification and accreditation (C&A) of ESI was completed in September 2010 by the Bureau of Public Debt.
- The OIG agrees with the security categorization of "high" for ESI.
- A risk assessment was conducted for ESI in 2010 that addresses all the required elements outlined in relevant NIST guidance.
- The security controls of ESI were tested by an independent source and internally by the OCIO.
- The ESI contingency plan is routinely maintained and tested in accordance with NIST Guidance.
- A privacy threshold analysis (PTA) was conducted for ESI. The PTA revealed that ESI does not require a privacy impact assessment. We agree with this assessment.
- The ESI Plan of Action and Milestones (POA&M) follows the format of the OPM POA&M guide, and has been routinely submitted to the Office of the Chief Information Officer for evaluation.
- We independently tested 24 security controls for ESI and found that 1 of the security controls was not in place during the fieldwork phase of the audit.

Contents

Introduction

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we evaluated the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Enterprise Server Infrastructure General Support System (ESI).

Background

ESI is one of OPM's 43 critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's systems on a rotating basis.

The Office of the Chief Information Officer (OCIO) has been designated with ownership of ESI. ESI supports OPM in meeting its goals by serving as an infrastructure environment for the processing of payroll and benefit related actions for current and former federal government employees. ESI operates in a [redacted] environment. The mainframe infrastructure is supported by the agency's Data Center Group within the OCIO.

This was our second audit of the security controls surrounding ESI. The findings from the first ESI audit report, issued in 2004, were closed prior to the start of this audit. We discussed the results of our audit with OCIO representatives at an exit conference.

Objectives

Our objective was to perform an evaluation of security controls for ESI to ensure that the OCIO officials have implemented IT security policies and procedures in accordance with standards established by OPM, FISMA, and the National Institute of Standards and Technology (NIST).

OPM's IT security policies require managers of all major information systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The overall audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for ESI, including:

- Certification and Accreditation Statement;
- FIPS 199 Analysis;
- Information System Security Plan;
- Risk Assessment;
- Independent Security Control Testing;
- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment;

- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of the OCIO officials responsible for ESI, including IT security controls in place as of January 2011.

We considered the ESI internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives.

To accomplish our objective, we interviewed representatives of OPM's OCIO office and other program officials with ESI security responsibilities. We reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of ESI are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the ESI system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy Volumes 1 and 2;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from November through December 2010 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OCIO's management of ESI is consistent with applicable standards. Nothing came to the OIG's attention during this review to indicate that the OCIO is in violation of relevant laws and regulations.

Results

I. Certification and Accreditation Statement

A security certification and accreditation (C&A) of ESI was completed in September 2010.

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, provides guidance to federal agencies in meeting security accreditation requirements. The ESI C&A appears to have been conducted in compliance with NIST guidance.

The Bureau of Public Debt (BPD) was contracted by the OCIO to prepare the C&A package for ESI. OPM's Senior Agency Information Security Officer reviewed the ESI C&A package and signed the system's certification package on September 29, 2010. OPM's Chief Information Officer signed the accreditation statement and authorized the continued operation of the system on September 29, 2010.

II. FIPS 199 Analysis

Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires federal agencies to categorize all federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels.

NIST SP 800-60 Volume I, Guide for Mapping Types of Information and Information Systems to Security Categories, provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

The ESI security categorization analysis categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. ESI is categorized with a high impact level for confidentiality, high for integrity, moderate for availability, and an overall categorization of high.

The security categorization of ESI appears to be consistent with the guidance of FIPS 199 and NIST SP 800-60, and the OIG agrees with the categorization of high.

III. Information System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in an Information System Security Plan (ISSP) for each system, and provides guidance for doing so.

The ISSP for ESI was created using the template outlined in NIST SP 800-18. The template requires that the following elements be documented within the ISSP:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing;
- Laws, Regulations, and Policies Affecting the System;
- Minimum Security Controls;
- Plan Completion Date; and
- Plan Approval Date

The ESI ISSP contains the majority of the elements outlined by NIST. However, the ESI ISSP does not contain details of the interconnections between ESI and other systems.

The ISSP correctly states that NIST does not require systems to list interconnections with internal organizations, but the ISSP also indicates that ESI interfaces with several systems owned by external entities. The details of these external interfaces are not disclosed in the ISSP as required by the NIST guide. Specifically, the ESI ISSP does not detail the following information about each interfacing system: name, organization, type of interconnection, authorizations, dates of agreement, FIPS 199 category, C&A status, and name and title of authorizing official.

Recommendation 1

We recommend that the ESI ISSP be revised to include identifiers of the external systems that interconnect with ESI (name, organization, type of interconnection, authorizations, dates of agreement, FIPS 199 category, C&A status, name and title of authorizing official).

OCIO Response:

"We concur."

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide OPM's Internal Oversight and Compliance (IOC) with evidence indicating this recommendation has been implemented.

IV. Risk Assessment

A risk management methodology focused on protecting core business operations and processes is a key component of an efficient IT security program. A risk assessment is used as a tool to identify security threats, vulnerabilities, potential impacts, and probability of occurrence. In addition, a risk assessment is used to evaluate the effectiveness of security policies and recommend countermeasures to ensure adequate protection of information technology resources.

As part of the C&A process, BPD conducted a vulnerability assessment of ESI and evaluated the risk of each vulnerability in accordance with NIST SP 800-30 standards. BPD identified 18 vulnerabilities during this assessment, and for each one documented:

- Vulnerability Description;
- Threat Source;
- Existing Controls;
- Likelihood, Impact, and Risk Rating; and
- Control Recommendations.

ESI provided BPD sufficient evidence to close findings for five vulnerabilities and determined that one vulnerability was due to a false positive test result. Remediation activities for the remaining 12 vulnerabilities are appropriately tracked with the ESI Plan of Action and Milestones (POA&M) (see section IX below).

V. Independent Security Control Testing

A security test and evaluation (ST&E) was completed for ESI as a part of the system's C&A process in September 2010. The ST&E was conducted by BPD, an OPM contractor that was operating independently from the OCIO. The OIG reviewed the controls tested to ensure that they included a review of the appropriate management, operational, and technical controls required for a system with a "high" security categorization according to NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems.

The ST&E labeled each security control as common, system-specific, or hybrid. A common control is a security control that is inherited from another system or physical environment. A system-specific control is a control that is implemented directly on an individual application. A hybrid control is where part of the control is deemed common and part is deemed system specific. All types of controls were tested as part of the ST&E due to the fact that ESI is a general support system that both inherits and provides common security controls.

The possible outcomes for each control test were fully satisfied, partially satisfied, and not satisfied. BPD reviewed and tested over 200 controls as part of the ST&E and concluded that 33 were partially satisfied and the rest were fully satisfied. The 33 partially satisfied control tests were condensed into the 18 security weakness findings discussed in Section IV above.

VI. Security Control Self-Assessment

FISMA requires that IT security controls of each major application owned by a federal agency be tested on an annual basis. In the years that an independent ST&E is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls.

The designated security officer for ESI conducted a self-assessment of the system's controls in April 2010. The assessment included a review of the relevant management, operational, and technical security controls outlined in the NIST SP 800-53 Revision 3. The OCIO attempts to perform a complete and thorough security self-assessment each year. The OCIO did not detect any security weaknesses in the FY 2010 self-assessment.

Although the ESI self-assessment indicated that there were zero security weaknesses in the system, an OIG review of the same security controls indicated that a weakness does exist (see section X, below).

VII. Contingency Planning and Contingency Plan Testing

NIST SP 800-34, Contingency Planning Guide for IT Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. The OPM IT security policy requires that OPM general support systems and major applications have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The ESI Disaster Recovery (DR) Plan documents the functions, operations, and resources necessary to restore and resume mainframe operations when unexpected events or disasters occur. The ESI DR plan is reviewed and updated annually and contains the majority of elements recommended by NIST SP 800-34 guidelines, including:

- System background information;
- Concept of operations;
- Notification/activation phase;
- Recovery operations; and
- Procedures to return to normal operations.

Contingency Plan Test

NIST SP 800-34 provides guidance for conducting and documenting contingency plan tests. Contingency plan testing is a critical element of a viable disaster response capability.

In May 2010, the OCIO conducted its annual disaster recovery test. The test involved restoring all mission critical functions at a remote facility. The documentation resulting from the testing activity contains the majority of the items required by the NIST guide including the scope, objectives, participants, and logistics of the test.

The test summary included a section of "areas for further review" that documents the issues or concerns that were discovered during the test. There were 19 issues detected during the FY 2010 test, several of which were considered "major" in nature. The majority of the issues were also identified in the disaster recovery tests from FY 2008 and FY 2009. Although the OCIO has documented the fact that issues exist, it does not appear that they have attempted to remediate these weaknesses. We acknowledge the fact that remediation activity for several of these issues requires support from OPM program offices outside of the OCIO. However, we believe that the OCIO should take primary responsibility for coordinating remediation activity since ESI is a critical general support system that many other OPM applications rely on for common controls.

Recommendation 2

We recommend that the OCIO develop and implement a plan to remediate weaknesses identified during ESI disaster recovery tests; remediation activities should be tracked on the ESI POA&M.

OCIO Response:

"We disagree in part with the recommendation. Clearly there are not 19 weaknesses. However, the list of observations should be reviewed to determine which, if any, of the items are actual weaknesses. The Data Center agrees that any items found to be actual weaknesses need to be documented in a POA&M and a plan developed to remediate them. However, the Data Center does not control infrastructures outside the ESI, nor does it determine which tests will be conducted by the Lines of Business or other organizations. During the ESI DR exercise the Data Center recovers the ESI environment and executes tests to ensure the platform is wholly recovered. While the Data Center can make test recommendations, decisions regarding the testing of infrastructure external to the ESI and customer applications are outside the control of the Data Center. Any weaknesses found during the review of the list should be documented and tracked in the POA&M of the organization responsible for taking corrective actions; not necessarily the ESI POAM. Likewise, plans to remediate any weaknesses should be developed by the parties responsible for taking corrective actions."

OIG Reply:

After reviewing the OCIO's response to the draft report, we acknowledge that there may be fewer than 19 weaknesses identified during the most recent disaster recovery exercise. The intent of our recommendation is to encourage the OCIO to use the formal POA&M process to track *any* weaknesses that are identified; a statement to which the OCIO agrees. As part of the audit resolution process, we recommend that the OCIO provide IOC with evidence indicating that weaknesses identified during the FY 2011 disaster recovery exercise are tracked on the ESI POA&M.

VIII. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to perform a screening of federal information systems to determine if a Privacy Impact Assessment (PIA) is required for that

system. OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate any vulnerabilities of privacy in information systems and to document any privacy issues that have been identified and addressed.

The OCIO completed an initial privacy screening of ESI and determined that a PIA was not required for this system because it does not contain Personally Identifiable Information (PII). Although several applications residing on the ESI mainframe contain PII, the OCIO staff supporting ESI does not have access to this data.

IX. Plan of Action and Milestones Process

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

The OIG evaluated the ESI POA&M and verified that it follows the format of OPM's standard template, and has been routinely submitted to the OCIO's Security and Privacy Group for evaluation. Nothing came to our attention to indicate that there are any current weaknesses in the management of the ESI POA&M.

X. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated the degree to which a subset of these controls had been implemented for ESI, including:

- AC-2 Account Management
- AC-5 Separation of Duties
- AC-6 Least Privilege
- AC-7 Unsuccessful Login Attempts
- AC-11 Session Lock
- AT-3 Security Training
- AU-2 Auditable Events
- AU-3 Contents of Audit Records
- AU-6 Audit Review, Analysis, Reporting
- CA-7 Continuous Monitoring
- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- IA-1 Identification and Authentication
- IA-5 Authenticator Management
- MA-1 Maintenance Policy and Procedures
- MA-2 Controlled Maintenance
- MP-6 Media Sanitization and Disposal
- PE-1 – 18 Physical and Environmental Controls
- PL-4 Rules of Behavior
- PM-1 Information Security Program Plan
- PS-4 Personnel Termination
- RA-5 Vulnerability Scanning
- SC-5 Denial of Service Protection
- SI-2 Flaw Remediation

These controls were evaluated by interviewing individuals with ESI security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system.

Although it appears that the majority of NIST SP 800-53 Revision 3 security controls have been successfully implemented for ESI, one tested control was not fully satisfied.

a) PM-1 Information Security Program Plan

ESI is a general support system that provides common security controls to other information systems and applications. ESI also inherits several security controls from program offices outside the OCIO (primarily physical controls related to building security).

Although the OCIO's Security and Privacy Group is currently developing a list of common controls that ESI shares with other systems, this information has not been formally documented and shared with other OPM program offices. Without a well defined list of common controls, the owners of other systems must use their own judgment to determine which security controls are inherited from ESI, increasing the risk that these systems have controls that are not adequately implemented or tested.

NIST SP 800-53 Revision 3 control PM-1 states that an organization should develop an agency-wide Information Security Program Plan that documents the program management controls and organization-defined common controls.

Recommendation 3

We recommend that the OCIO formally document common controls provided by ESI and implement a process to share this information with the owners of other applications relying on this support system.

OCIO Response:

"We concur. This work is in progress."

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide OPM's IOC with evidence indicating this recommendation has been implemented.

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Group Chief
- [redacted], Senior Team Leader
- [redacted], IT Auditor

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

MEMORANDUM FOR [redacted]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP

FROM: MATTHEW E. PERRY
CHIEF INFORMATION OFFICER
02/03/2011

Subject: Response to the Draft Audit Report No. 4A-CI-00-11-016
FY 2011 IT Security Controls of OPM's Enterprise Server
Infrastructure General Support System

Thank you for the opportunity to comment on the subject report. The results provided in the draft report consist of a number of recommendations. The recommendations are valuable to our program improvement efforts and after a careful review of the report, we offer the following comments.

III. Information System Security Plan

The 2010 OIG Audit report states: "The ESI ISSP contains the majority of the elements outlined by NIST. However, the ESI ISSP does not contain details of the interconnections between ESI and other systems."

CIO Comment:
We concur.

The 2010 OIG Audit report recommends: "Recommendation 1 We recommend that the ESI ISSP be revised to include identifiers of the external systems that interconnect with ESI (name, organization, type of interconnection, authorizations, dates of agreement, FIPS 199 category, C&A status, name and title of authorizing official)."

CIO Comment:
We concur.

VII. Contingency Planning and Contingency Plan Testing

The 2010 OIG Audit report states: "There were 19 issues detected during the FY 2010 test, several of which were considered "major" in nature. The majority of the issues were also identified in the disaster recovery tests from FY 2008 and FY 2009. Although OCIO has documented the fact that issues exist, it does not appear that that they have attempted to remediate these weaknesses."

CIO Comment:
We disagree with this finding as it appears to reflect a misunderstanding of the 19 issues referenced. The 19 issues referenced are from a list titled "Areas for Further Review" that was part of a Data Center internal document. This list documents observations (good and bad) from the 2010 ESI DR exercise. The document was not intended for publication; it was simply an internal record, and as such it had not been edited for language or for use by personnel not intimately familiar with the ESI DR test process. The 19 observations in the list can be grouped as follows depending upon their nature:

Observations 4, 5, 10, 12, and 13 were included on the list simply to document that these functions, which may not have been tested in previous exercises, were in fact successfully tested in the 2010 ESI DR exercise. Their inclusion on the list was a positive not a negative comment. They require no further attention.

Observations 1, 6, and 16 were included on the list to document that these functions that may not have been tested in previous exercises were in fact successfully tested on a small scale in the FY 2010 ESI DR exercise. Their inclusion on the list was intended to document their successful tests and suggest that broader testing might be appropriate in the future. Responsibility for expanding the testing of these three functions lies outside the purview of the Data Center.

Observation 3 documents the fact that the capacity of circuit between the Sterling Forest DR site and Boyers needed to be increased. This upgrade has since been completed and the new circuit tested. The new circuit will be employed in the upcoming 2011 ESI DR exercise.

Observations 2, 9, 11, 14, 15, and 17 were included on the list to document the fact that the parties responsible for these functions chose not to test them during the 2010 ESI DR exercise. Organizations outside the Data Center decide which functions to test based upon their priorities, resources, and previous tests. These specific functions may have been tested at other times independent of the ESI DR exercise. Their inclusion on the list was intended to document functions which the responsible parties may wish to consider testing during future ESI exercises. Responsibility for testing these six functions lies outside the purview of the Data Center.

Observations 7 and 8 were included on the list to document network related configuration changes needed to provide or improve disaster recovery access from specific functional areas. These changes are recommended by the Data Center but are outside the control of the Data Center.

Observations 18 and 19 were included on the list to document the continuous need to work as a team with other organizations in refining the ESI DR *test* environment preparation process. These items do not affect the ability to recovery ESI services during a real disaster. The DR test infrastructure configuration is much more complex than an actual disaster recovery configuration because during a DR test both the live production environment *and* the DR testing environment must operate concurrently while physically and logically separated. Observations 18 and 19 are part of an ongoing process to improve preparation and deployment of the DR test environment without disruption to the live production environment. This process has no finite end point, instead it evolves as technology and the OPM infrastructure evolves.

Below is the "Areas for Further Review" list cited in the OIG draft audit. Comments (in bold) have been included below each item to add clarity.

Areas for Further Review – The overall testing was quite successful with only a few areas which need to be reviewed. A number of the areas could be considered major. These are in connectivity to the customer base. Having the IBM Enterprise Servers systems available is a prerequisite of the test but there also has to be connectivity to where the end user is located.

1. *There was no Disaster Recovery [redacted] available prior to the test. Network Management made the decision not to include the [redacted] because it was being phased out and not to include the [redacted] because it was too new. In the event of a disaster, [redacted] is now being hosted from both TRB and Macon, GA OPM locations. The impact of not having [redacted] available would be severe and mean there would be no remote access into general OPM applications which are not running on [redacted]. But many of the remote users rely on [redacted] for their access to [redacted] applications from home especially for all R&B applications. FIS PIPS users do not use [redacted] although CIS and FIS support personnel are dependent on it to maintain applications. DC has ways to access [redacted] applications, maintaining them remotely with only a VPN connection. In the event of a disaster, many users have been told to work at home. On the second day of the test, NM changed its position and assisted one MSA&C home user in San Francisco to gain access to new [redacted] which was successful.*

   [redacted] access was successfully tested on a small scale. This entry is intended to document that success and suggest expanding testing of [redacted] access during future DR exercises. More robust tests of the [redacted] DR will be conducted after the new [redacted] infrastructure is deployed in Macon, GA. NM manages [redacted] and decides the scope of the [redacted] test.

2. *There was no e-mail access during the test as requested by many users. There is a plan to recover some e-mail services in Boyers, PA as part of NM's Disaster Recovery Plan. OPM users who are at home and have their own Internet Service Provider, could use WebMail to access the recovered system provided the e-Mail servers are not hosted in TRB. Home users who rely on [redacted] will not be able to access e-mail.*

   This entry is intended to raise the possibility of testing eMail during future DR exercises. Tests of e-Mail DR have been successfully performed independent of the ESI DR exercise. NM manages e-Mail and related e-Mail DR tests.

3. *There is a continuing review underway to address the speed of the two communication lines; Sterling Forest, NY to Boyers, PA and Sterling Forest to Macon, GA. The Sterling Forest to Boyers connectivity consists of three T-1 circuits today and may need to be upgraded to DS-3 speeds in a real DR. DC needs to ensure the process is in place to exercise the option. The T-1 circuit from Sterling Forest to Macon, GA may need to upgraded in the event of a disaster since Macon would be the location of OPM's ISP. If*

NM would implement diverse routing. ISP traffic could flow from Macon to Boyers over DS-3 lines and then come into Sterling Forest on one of the three T-1 circuits.

A DS-3 communication circuit between Sterling Forest, NY and Boyers, PA has been installed and tested will be used in the 2011 ESI DR exercise.

4. *There are 40+ FIS Federal remote sites which are connected through Sprint MPLS connectivity into Washington DC's TRB. The plan is to failover from TRB to Boyers, PA in the event of a disaster. This was tested and was successful for the three locations tested.*

   FIS relies on work performed at FIS remotes sites. This entry documents the fact that Sprint MPLS connectivity, though not ESI hosted, was successfully tested during this year's DR exercise. This is positive; not negative.

5. *There are about 10+ FIS Federal remote sites connected using an Internet connection. A small VPN appliance was hosted out of OPM Macon, GA which serviced the testing from Miami, Fl.. The test was successful.*

   FIS relies on work performed at FIS remotes sites. This entry documents the fact that an Internet connection was successfully tested during this year's DR exercise. This is positive; not negative.

6. *FIS has field investigators who carry laptops and access the PIPS system remotely. The remote test coming through the Internet was successful even though there is no ISP provider for Boyers, PA. OPM has links to the Internet through TRB and Macon, GA. ISP access into PIPS is very new and expanding. A portion of remote access is through dial circuits into VPN concentrators. A growing population of remote FIS users are coming through the Internet which would imply remote connectivity using the Internet would have to come through OPM's Macon, GA ISP. Macon was provisioned with a small VPN appliance for the test and it was successful. The location is not hosted with significant sized VPN appliances to host the entire FIS workload. There are no VPN concentrators hosted in Sterling Forest as part of the* [redacted]*t. Therefore in the event of disaster, FIS Federal Investigators would have to visit their many remote sites to enter data.*

   FIS relies on the investigators being able to upload their data from their laptops via the Internet. This entry documents the successful test of this functionality but raises the potential capacity limitation of the Macon, GA VPN concentrator in providing access for large numbers of FIS investigators during a disaster. NM manages the VPN concentrators and related DR tests.

7. *There was no capability for the fixed FIS remote sites (numbering 50+) to be able to print reports during the disaster. The LAN printing methodology implemented has yet to provide redundant LAN print queues in other than the TRB location. Print from PIPS*

travels from the [redacted] to the remote location PIPS terminal and then is handed off to the [redacted]. The local high speed network printer is only accessible using Washington DC TRB hosted [redacted].

This DR printing capability issue is understood by NM and FIS. DC worked with others to develop a detailed set of instructions on how to utilize "Named Printer" capability that mitigates the problem by bypassing the [redacted]. These instructions were distributed to about half of the remote FIS locations. In order to exploit this capability the staff in each location must make changes to bypass the [redacted]. Some of the field offices deployed the changes and found they work well; other offices did not attempt to make the changes. The "Named Printer" change mitigates this problem, but the change must be performed in the field by FIS staff.

8. *Merit Systems Accountability & Compliance personnel are located in external OPM sites around the country. Their offices are connected to OPM into Washington DC's TRB. There are no NM provisions for these circuits to be replaced by comparable ones in Boyers, PA or Macon, GA. Testers from the and San Francisco, CA and Philadelphia, PA offices were successful accessing their [redacted] application called [redacted] from their homes using specially provisioned means of access called [redacted] Using this home access they have no facility to print. Printing is one of their requirements. The implication is all Human Capital Leadership and Merit Accountability offices who are connected using dedicated T-1 circuits into Washington DC's TRB must work from home using [redacted] There was a very limited test from San Francisco using the new [redacted] system. The [redacted] has not been implemented to attempt to do [redacted] printing. It is being recommended to MSA&C they request to be moved to NM's MPLS or Internet connections using a VPN. If this is completed, then the will have access to the Disaster Recovery system in Sterling Forest, NY.*

   Merit Systems Accountability & Compliance personnel do not have access to [redacted] applications during a disaster because they are still using dedicated T-1 circuits. These circuits should be replaced with modern communications capability. This is a NM engineering issue.

9. *In the 2009 test, the Service Credit application was never successfully recovered. In the 2010 test, the MEF R&B Retirement application called Service Credit was not attempted because of problems in the application unrelated to Disaster Recovery.*

   The ESI hosts the bulk of the Retirement System applications. A number of years ago a key part of the system, Service Credit, was moved outside the ESI to the distributed platform. The Data Center recommends that Service Credit be included in the annual ESI DR exercise as it is an integral part of the retirement system. Recovering and testing it is outside the purview of the DC.

10. *In the 2009 test, the [redacted] was successfully recovered but only able to be tested in Boyers. In the 2010 test, the MEF R&B Retirement application called [redacted]*

was successfully recovered on the replacement [redacted] in Boyers, PA. Testing of the system was successfully completed by personnel in Boyers, PA and able to be tested successfully by personnel in the Gaithersburg, MD testing location.

This entry documents the fact that [redacted], though not ESI hosted, was successful recovered and tested during this year's ESI DR exercise. This is positive; not negative.

11. *The Chief Financial Officer's (CFO) system called PFIS was never successfully recovered on the replacement [redacted] in Boyers, PA. In the 2009 test, the test was never successfully recovered. The new implementation of CBIS at an out sourced location has a dependency on PFIS within OPM to process financial data and invoices for FIS. The CFO chose to exclude PFIS from the 2010 DR test.*

    The PFIS application runs on a server outside the ESI. Recovery of PFIS was not attempted during the ESI DR exercise. This is mentioned for the sake of completeness as PFIS is a financial component that interfaces with the FIS application suite. Recovering and testing it is outside the purview of the DC.

12. *The R&B Insurance Services application called FEHB2000 was successfully recovered on a replacement [redacted] located in Boyers, PA. The system was thoroughly tested and is the second time in a row it has been successfully recovered and used in a DR test.*

    This entry documents the fact that FEHB2000, though not ESI hosted, was successful recovered and tested during this year's ESI DR exercise. This is positive; not negative.

13. *The FIS[redacted] e-QIP server did not participate. The e-QIP operational plan has it being hosted in Boyers, PA for six (6) months and then hosted in Washington DC's TRB for six (6) months. The server was located in Boyers already during this test. Fail-over is demonstrated every six (6) months. This is sufficient evidence that e-QIP is recoverable in the event of a disaster.*

    The ESI hosts FIS's Personnel Information Processing System (PIPS) application. E-QIP, an integral part of the PIPS system, is hosted on a [redacted] outside the ESI. For the sake of completeness, the independent e-QIP test was reported in the ESI exercise summary. This is positive; not negative.

14. *There was still no connection available for DR to the FIS contractor hosted [redacted] for outside agency access using the Agency Menu. In the event of a disaster, this would exclude outside agency access, numbering 2K+ users from accessing PIPS. In the event of a disaster, this critical requirement would not be available with the 12 hour window required.*

The ESI hosts FIS's PIPS application. A key PIPS remote user access facility is hosted at [redacted] (a contractor site). FIS contracted for these services and did not to include them in the ESI DR exercise. Remote access has always been part of each ESI DR exercise, and the non-participation of [redacted] has been reported to FIS each year. They have taken no action to correct this deficiency. Since the contract is owned and managed by FIS correcting this deficiency is outside the purview of the DC.

15. *There was no FIS Department of Defense (DOD) JPAS connection available for DR where inquiries are passed from DOD to OPM. In the event of a disaster, this critical requirement would not be available with the 12 hour window required.*

The ESI hosts FIS's PIPS application. A key PIPS remote DOD user access facility, JPAS, is hosted through a connection from the [redacted] FIS requested the connection originally through the Pentagon and now has the connection to [redacted] directly. Remote access has always been part of each ESI DR exercise, and the lack of a JPAS DR connection has been reported to FIS each year. They have taken no action to correct this deficiency. Since the connection agreement is between FIS and DOD, correcting this deficiency is outside the purview of the DC.

16. *A number of [redacted] File transfers were included in the Plan supporting various Lines of Business:*

    a. *FIS – [redacted] for credit information (future)*
    b. *FIS – [redacted] for credit information (future)*
    c. *FIS – US Census (future)*
    d. *FIS – FBI (future)*
    e. *FIS – Agency Delivery (future)*
    f. *FIS – IRS (future)*
    g. *E-HRI – Human Resources data from e-HRI's contractor was successful because of IP addressing issues on NM's part along with e-HRI's need to cut short the time allocated to the exercise.*
    h. *R&B – Annuity Payroll data completed to FMS's Kansas City, MO location (successful)*
    i. *Human Resources Solutions – Data exchanges (successful)*
    j. *R&B – Social Security Administration (future)*

The ESI provides the bulk of OPM's electronic data exchange services. As part of the disaster preparedness services provided by the DC, recommendations are provided to Lines of Business and CIO's application support areas. The above list describes those data exchanges the DC believes to be key and should be considered for testing by the Lines of Business. Since each Line of Business determines what is important for them to test the DC only offers its recommendations. For the sake of completeness, this observation documents the advice and results. Of the 10 tests recommended 3 were successfully tested and 7 were deferred by the Lines of

Business. The Lines of Business may wish to consider testing these data exchanges in the 2011 ESI DR exercise.

17. *No discussions were conducted by FIS of testing DR connectivity for its USIS, Kroll, and CACI contractors. This should be considered for the DR 2010 test. These contractors are an essential part of FIS operations and would be needed in the event of a disaster.*

    The ESI hosts FIS's PIPS application. As part of the disaster preparedness services provided by the DC, recommendations are provided to Lines of Business and CIO's application support areas. The above observation lists contractors the DC believes FIS should consider including in the ESI DR test. Since each Line of Business determines what is important for them to test, the DC is only in a position to offer its recommendations. FIS may wish to consider including the above contractors in future tests, but doing so is a FIS decision.

18. *There were DNS problems throughout the test. TCP/IP addressing is the responsibility of NM. One of the major problems was the lack of documentation created by NM and in the coordination of DC and NM about what IP addressing will be used during the test. NM personnel are rotated into the test new each year which does not provide time to complete the experience of one test and carry it forward into the next year. DC and NM staffs needs to work closer prior to the test to ensure sufficient knowledge of relevant network topology and settings are is in place in order to debug network issues in a timely manner. A bright spot in this years test for NM is the work* [redacted] *who preformed the duties of NM's DR Project Manager. His organizational skills greatly assisted in coordinating the work of the NM participants. Unlike DC staff who are located in Sterling Forest and Gaithersburg, NM has staff located in Sterling Forest, Gaithersburg, Boyers, Macon, and Ft Meade.*

    The structure of the network topology during a real disaster would have few if any changes. However, during an ESI DR exercise the production systems in TRB must continue to operate but be blocked from [redacted] **Sterling Forest and Gaithersburg recovery site access. The complexity associated with reconfiguring the network and rerouting applications for the ESI DR exercise is significant. Each year the coordination between the various organizations has improved. The ultimate goal is to have the overall test be executed precisely and have all parts work the first time. This observation is intended as a reminder to ensure all ESI DR exercise participants strive to improve DR test documentation prior to the annual exercise to achieve this goal. This does not impact the recovery of the ESI during an actual disaster.**

19. *The continued refinement of the documentation provided by DC of the DR URLs needs to be continued. There were a few cases where the URL in the Test Plans did not match with what eventually worked. Work needs to be focused on how these URLs are made available through the DNS Servers maintained by NM.*

This issue relates to Observation 18 (above). Along with refining the DR exercise documentation the method of accurately determining and deploying URLs should be improved to avoid errors. This must be a joint effort between NM and DC. This does not impact the recovery of the ESI during an actual disaster.

The 2010 OIG Audit report recommends:
"Recommendation 2

We recommend that OCIO develop and implement a plan to remediate weaknesses identified during ESI disaster recovery tests; remediation activities should be tracked on the ESI POA&M."

CIO Comment:
We disagree in part with the recommendation. Clearly there are not 19 weaknesses. However, the list of observations should be reviewed to determine which, if any, of the items are actual weaknesses. The Data Center agrees that any items found to be actual weaknesses need to be documented in a POA&M and a plan developed to remediate them. However, the Data Center does not control infrastructures outside the ESI, nor does it determine which tests will be conducted by the Lines of Business or other organizations. During the ESI DR exercise the Data Center recovers the ESI environment and executes tests to ensure the platform is wholly recovered. While the Data Center can make test recommendations, decisions regarding the testing of infrastructure external to the ESI and customer applications are outside the control of the Data Center. Any weaknesses found during the review of the list should be documented and tracked in the POA&M of the organization responsible for taking corrective actions; not necessarily the ESI POAM. Likewise, plans to remediate any weaknesses should be developed by the parties responsible for taking corrective actions.

X. NIST SP 800-53 Evaluation

The 2010 OIG Audit report states:
"Although the OCIO's Security and Privacy Group is currently developing a list of common controls that ESI shares with other systems, this information has not been formally documented and shared with other OPM program offices. Without a well defined list of common controls, the owners of other systems must use their own judgment to determine which security controls are inherited from ESI, increasing the risk that these systems have controls that are not adequately implemented or tested."

CIO Comment:
We concur.

The 2010 OIG Audit report recommends:
"Recommendation 3

We recommend that OCIO formally document common controls provided by ESI and implement a process to share this information to the owners of other applications relying on this support system."

CIO Comment:
We concur. This work is in progress.