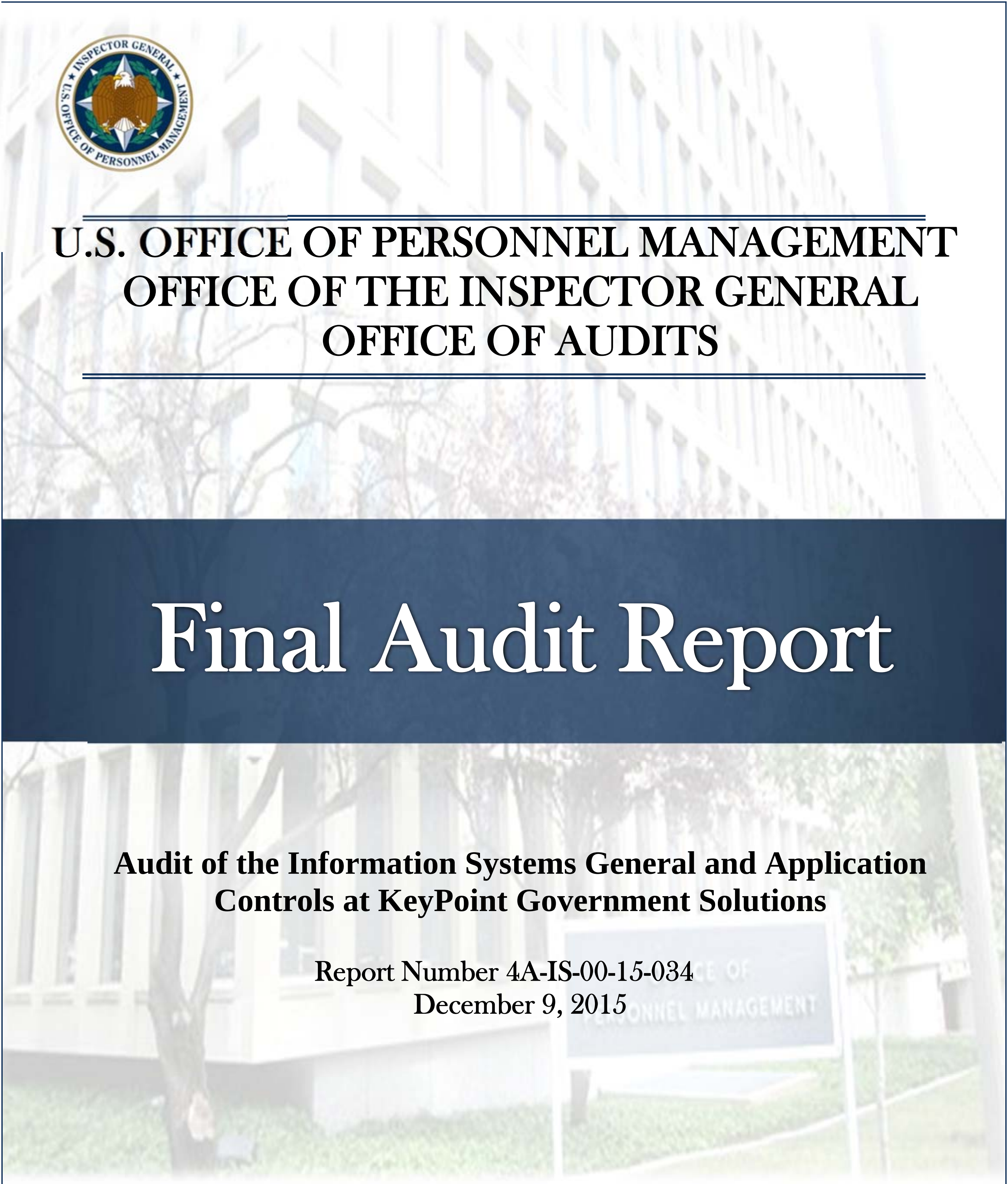


U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Audit of the Information Systems General and Application Controls at KeyPoint Government Solutions

Report Number 4A-IS-00-15-034
December 9, 2015

-- CAUTION --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at KeyPoint Government Solutions

Report No. 4A-IS-00-15-034 **December 9, 2015**

Why Did We Conduct the Audit?

KeyPoint Government Solutions (KeyPoint) is a service contractor for the U.S. Office of Personnel Management's (OPM) Federal Investigative Services (FIS), and operates the Secure Portal, one of the agency's critical Information Technology (IT) systems. As such, the Federal Information Security Management Act (FISMA) requires that the Office of the Inspector General (OIG) perform an audit of the IT security controls of this system, as well as all of the agency's systems, on a rotating basis. Additionally, in 2014 KeyPoint experienced an intrusion into their network, further increasing the need for OIG oversight.

What Did We Audit?

The OIG has completed a performance audit of KeyPoint and the Secure Portal to ensure that the system owner, FIS, in connection with KeyPoint, has managed the implementation of IT security policies and procedures in accordance with the standards established by FISMA, the National Institute of Standards and Technology, the Federal Information Security Controls Audit Manual and OPM's Office of the Chief Information Officer.

Michael R. Esser
Assistant Inspector General
for Audits

What Did We Find?

Our audit of the IT security controls of KeyPoint determined that:

- KeyPoint has established a security management program.
- KeyPoint has implemented controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information. However, we noted several opportunities for improvement related to KeyPoint's access controls:
  - Standardized access request forms are not utilized for managing information systems access;
  - There is no formal process for auditing logical and physical access privileges; and
  - There are no formal procedures for reviewing system logs.
- KeyPoint has implemented an incident response and network security program. However, we noted several areas of concern related to KeyPoint's network security controls:
  - A formal incident response procedure has not been established;
  - A firewall configuration standard has not been developed;
  - An outbound web proxy has not been implemented;
  - Controls are not in place to prevent unauthorized devices from connecting to the network and control the use of removable media;
  - Significant improvements are needed to the vulnerability management program;
  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized; and
  - Several vulnerabilities with known exploits were identified as a result of our independent vulnerability scans.
- KeyPoint has implemented a configuration management process to control changes made to its IT systems. However, there is no routine auditing of KeyPoint's server and workstation configuration.
- KeyPoint has documented contingency procedures that detail the recovery of servers in the event that normal service is disrupted. However, the contingency plan for workstations may not be feasible since it relies on a 3rd party without a service contract.
- KeyPoint has implemented multiple controls surrounding the input, processing, and output of sensitive data related to the background investigations it performs for OPM. However, KeyPoint is provided more sensitive data from OPM than it needs to perform its contractual obligations.

ABBREVIATIONS

FIPS	Federal Information Processing Standards
FIS	Federal Investigative Services
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
IT	Information Technology
KeyPoint	KeyPoint Government Solutions
NAC	Network Access Control
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	U.S. Office of Personnel Management
PII	Personally Identifiable Information
SIEM	Security Information Event Management
SP	Special Publication

TABLE OF CONTENTS

I. BACKGROUND

On December 18, 2014, President Obama signed into law the Federal Information Security Modernization Act of 2014 (P.L. 113.283), which amended the Federal Information Security Management Act (FISMA) of 2002. FISMA and the Modernization Act require an annual independent evaluation of each agency's information security program and practices to determine the effectiveness of such program and practices. For each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation shall be performed by the Inspector General.

FISMA compliance is mandated for contractor organizations processing federal data on behalf of a government agency. In accordance with FISMA, we audited the information technology (IT) security controls related to the U.S. Office of Personnel Management (OPM) contractor KeyPoint Government Solutions (KeyPoint).

KeyPoint provides contractor support to OPM's Federal Investigative Services (FIS), which is responsible for helping to ensure that the Federal Government has a workforce that is worthy of the public trust by providing both suitability and security clearance determinations. KeyPoint's primary role for OPM is to conduct background investigation fieldwork to collect data used in the clearance determination process.

This was our first audit of KeyPoint's IT general and application controls. We discussed the results of our audit with OPM and KeyPoint representatives at an exit conference.

All KeyPoint personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of Federal data processed and maintained in KeyPoint's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Contingency planning; and
- Application controls.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of KeyPoint's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of KeyPoint's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by KeyPoint to process and/or store Federal data that it maintains in an effort to perform its contractual obligations to OPM. The business processes reviewed are primarily located in [redacted].

The on-site portion of this audit was performed from April through June, 2015. We completed additional audit work before and after the on-site visits at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at KeyPoint as of July 2015.

In conducting our audit, we relied to varying degrees on computer-generated data provided by KeyPoint. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed KeyPoint's business structure and environment;
- Performed a risk assessment of KeyPoint's information systems environment and applications, and prepared an audit program based on the assessment and the Government Accountability Office's Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating KeyPoint's control structure. These criteria include, but are not limited to, the following publications:

- OPM Information Security Privacy and Policy Handbook;
- Office of Management and Budget (OMB) Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information";
- 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;
- The Federal Information System Controls Audit Manual;
- National Institute of Standards and Technology (NIST) Special Publication (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 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37 Revision 1, Guide for Applying Management Framework to Federal Information Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information systems and Organizations;
- NIST SP 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems; and
- Other criteria as appropriate.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether KeyPoint's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, KeyPoint was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

The security management component of this audit involved the examination of the policies and procedures that are the foundation of KeyPoint's overall IT security program. We evaluated KeyPoint's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

KeyPoint has implemented a series of formal policies and procedures that comprise its security management program. KeyPoint has developed an adequate risk management methodology, and has procedures to document, track, and mitigate or accept identified risk. We also reviewed KeyPoint's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that KeyPoint does not have an adequate security management program.

B. Access Controls

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized logical or physical access to sensitive resources.

The following sections document several opportunities for improvement related to KeyPoint's logical and physical access controls.

1. Logical Access – Access Request Forms

KeyPoint does not currently use standardized access request forms to help facilitate the process of granting logical access to its information systems. Currently, access is granted or adjusted by KeyPoint's IT Help Desk after it receives an informal email notification from human resources that an employee has been hired, transferred, or terminated. This informal process is not sufficient to ensure that the IT Help Desk is assigning access rights accurately, and makes it difficult to ensure that all access requests are appropriately achieved for later forensic or audit purposes.

FISCAM states that "access authorizations should be documented on standard forms and maintained on file."

Failure to utilize a standard access request form increases the risk that an employee's system access will be mishandled, altered, unsupported, or above the minimal privileges required for their job function.

Recommendation 1

We recommend that KeyPoint use a standard formal access request form to help facilitate the granting, changing and auditing of information system access.

Office of the Chief Information Officer (OCIO)/FIS Response:

"We concur. KeyPoint Government Solutions has implemented a new account management process utilizing formal access request forms for logical account creation, deletion, and modification."

Office of the Inspector General (OIG) Reply:

As part of the audit resolution process, we recommend OCIO/FIS provide OPM's Internal Oversight and Compliance (IOC) division with evidence that KeyPoint has implemented this recommendation. This statement applies to all subsequent recommendations in this audit report that OCIO/FIS agrees to implement.

2. Logical Access - Removing and Auditing Information System Accounts

KeyPoint policy requires that an individual's information system access be immediately disabled when employment is terminated. We tested the effectiveness of this policy by comparing a list of recently terminated employees to a current list of active network (Active Directory) user accounts. The test results indicated that several accounts had not been properly removed or disabled in a timely manner in accordance with KeyPoint policy.

In addition, KeyPoint does not currently have a standardized process to routinely audit active information system accounts for appropriateness. Such a process should not only include verifying that individuals are still actively employed by KeyPoint, but that their level of access allows the least amount of privilege required for their job function. The latter is dependent upon having a standard access request form to audit against, which as noted above, is not currently in place.

NIST SP 800-53, Revision 4, states that an organization should "review accounts for compliance with the account management requirements." FISCAM also states entities should "develop and implement a procedure that requires a complete user recertification on a periodic basis."

Failure to routinely audit logical access privileges to information systems increases the organization's risk of unauthorized access to sensitive information.

<u>Recommendation 2</u>
We recommend that KeyPoint implement a formal process to routinely audit information system accounts for appropriateness. This audit should include verification that individuals are still active employees and that their level of access is appropriate.

<u>OCIO/FIS Response:</u>
"We concur. KeyPoint Government Solutions [has] developed a system for the routine audit (weekly) of system account creations, deletions[,] and modifications. They have also created an audit task (annually) for the review of all system accounts."

3. **Logical Access – Operating System Logging and Monitoring**
KeyPoint monitors all user authentication activity for login successes and failures, but its procedures for monitoring other operating system activity could be improved.

KeyPoint's systems do log certain system transactions, and KeyPoint employees have reviewed these logs on an ad-hoc basis. However, KeyPoint has not documented a comprehensive list of operating system logs that its systems should store, nor formal procedures for routinely reviewing these logs.

NIST SP 800-53, Revision 4, states that organizations should "monitor the use of information system accounts," and monitor privileged role assignments and activities.

FISCAM states "appropriate entity officials should periodically review the use of privileged system software and utilities to ensure that access permissions correspond with position descriptions and job duties. Further, the use of sensitive/privileged accounts should be adequately monitored."

Monitoring activity and changes to an operating system is a critical component of an organization's IT security assurance program. The lack of a comprehensive procedure to address this issue increases the risk that malicious activity could remain undetected.

<u>Recommendation 3</u>
We recommend that KeyPoint develop a comprehensive list of logs that should be stored for each operating system it uses, and also develop procedures that ensure that these logs are routinely reviewed.

<u>OCIO/FIS Response:</u>
"We concur. KeyPoint Government Solutions has created a list of all audit events occurring on servers which is stored on the Security Information Event Management (SIEM) tool. They have also created a weekly audit task for review of all SIEM logs."

4. **Physical Access – Access Request Forms**

KeyPoint does not use standardized access request forms to manage the process of granting employees physical access to its facilities. Access is granted or adjusted by the security office after they receive email notification from human resources when an employee has been hired, transferred, or terminated. This informal process is not sufficient to ensure that security is assigning physical access accurately and appropriately, and also makes it difficult to ensure that access requests are achieved for audit purposes.

FISCAM states that "access authorizations should be documented on standard forms and maintained on file."

Failure to utilize a standard access request form increases the risk that physical access privileges are not well managed and that employees can gain unauthorized access to secure areas.

Recommendation 4

We recommend that KeyPoint implement a formal access request form for physical access as a part of granting, modifying or removing physical access and that it maintain the forms for audit records.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions has implemented a formal access request form for physical access as part of granting, modifying[,] or removing physical access."

5. **Physical Access – Removing and Auditing Physical Access Privileges**

KeyPoint policy requires an individual's physical access privileges to be revoked when employment is terminated. We tested the effectiveness of this policy by comparing a list of recently terminated employees to a current list of active physical access cards. The test results indicated that several accounts had not been disabled in a timely manner in accordance with KeyPoint policy. In addition, KeyPoint does not have a process to routinely audit physical access privileges to ensure that access is revoked timely or to recertify that access to existing accounts remains at the appropriate level of access.

NIST SP 800-53, Revision 4, states that an organization should "routinely review the access list detailing authorized facility access by individuals." FISCAM also states that management should "conduct regular reviews of individuals with physical access to sensitive areas to ensure such access is appropriate."

Failure to audit physical access to facilities and recertify access to secure areas increases the organization’s risk of unauthorized individuals gaining access to the facilities and information systems.

Recommendation 5

We recommend that KeyPoint implement a formal process to routinely audit physical access accounts for appropriateness. This audit should include verification that individuals are still active employees and that their level of access is appropriate.

OCIO/FIS Response:

“We concur. KeyPoint Government Solutions has developed a system for the routine audit [redacted] ***of all physical access to KeyPoint facilities.”***

C. Network Security

Network security includes the policies and controls used to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

We evaluated KeyPoint’s network security program and reviewed the results of automated vulnerability scans that we performed during the audit. We noted the following opportunities for improvement related to KeyPoint’s network security controls:

1. Incident Response

KeyPoint has not implemented a formal incident response procedure that establishes a process for categorizing incidents based on risk and outlining the appropriate response for each type of incident.

FIPS 200-2, Incident Response, states an organization should “establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.”

NIST SP 800-53, Revision 4, states that the organization should develop and document “an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance,” in addition to, “procedures to facilitate the implementation of the incident response policy and associated incident response controls.”

Failure to standardize the incident response process decreases an organization’s ability to quickly detect, analyze, contain, report, and recover from incidents.

Recommendation 6

We recommend that KeyPoint implement a formal incident handling and response process that outlines detection, categorization, analysis, containment, recovery, tracking, and reporting requirements.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions has updated their incident response plan, trained and tested necessary individuals on the incident response plan."

2. Firewall Configuration Management

KeyPoint has implemented firewalls to help secure its network environment. Although we did not detect any specific weaknesses in the configuration of KeyPoint's firewalls at the time of the audit, KeyPoint has not developed a formal firewall configuration/hardening standard (i.e., approved firewall configuration settings). Without a firewall configuration standard, it is not possible for KeyPoint to routinely audit the current settings of the firewall for appropriateness.

NIST SP 800-41, Revision 1, states that "a firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies. The policy should also include specific guidance on how to address changes to the rule set."

Failure to implement a thorough firewall configuration policy and continuously manage the devices' settings increases the organization's exposure to insecure traffic and vulnerabilities.

Recommendation 7

We recommend that KeyPoint implement a formal firewall management policy that includes both a configuration standard/baseline and procedures for routinely auditing actual settings against the baseline.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions has developed a firewall baseline and modified their IT Security Management Policy to include the management of firewalls using the baseline configuration and the regular review of firewalls."

3. Outbound Web Proxy

KeyPoint currently utilizes web proxies for internal connections. However, it does not utilize outbound web proxies to control the flow of information to the public Internet.

NIST SP 800-53, Revision 4, states an information system should only connect "to external networks or information systems through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture."

NIST SP 800-53, Revision 4, also states that an information system should enforce approved authorizations for controlling the flow of information within the system and between interconnected systems.

Failure to implement an outbound web proxy allows for connections to websites and services which could result in the loss of protected data or 'man-in-the-middle' attacks.

Recommendation 8

We recommend that KeyPoint implement and configure a web proxy for all outbound traffic.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions has acquired and installed a next generation firewall that includes a web proxy. The web proxy is configured to limit outbound internet traffic."

4. Rogue Device Detection/Prevention

KeyPoint policies and procedures prohibit the use of personal software and hardware on the corporate network. However, KeyPoint does not have technical controls in place to enforce this policy that can prevent unauthorized devices from connecting to its internal network.

NIST SP 800-53, Revision 4, states an organization should focus on identifying and locating potential rogue devices.

Without technical controls that can detect rogue devices on the network, there is increased risk that unauthorized devices can be used to access the corporate domain and the sensitive information it contains.

Recommendation 9

We recommend that KeyPoint implement technical controls to detect or prevent rogue devices from connecting to its network.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions is in the process of designing and implementing a Network Access Control (NAC) solution. Their NAC solution is planned to be in place by [redacted]."

5. Removable Media Controls

KeyPoint has implemented policies and procedures to limit the use of removable media on corporate information systems. However, it has not implemented technical controls that can enforce these policies, such as removable media encryption or the disabling of USB ports.

FISCAM states that "media controls should be implemented to control unauthorized physical access to digital and printed media removed from the information system." FISCAM explains that these controls extend to "diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, [and] digital video disks."

A lack of technical controls protecting data leaving the network on removable media increases KeyPoint's risk for inadvertent disclosure of sensitive information.

Recommendation 10

We recommend that KeyPoint implement technical controls to protect sensitive data from leaving the network on removable media unencrypted.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions has implemented a group policy object … rule that eliminates the USB storage devices on corporate computers."

6. Vulnerability Scanning

KeyPoint has performed vulnerability scans against its technical environment, but it does not have a formal methodology to facilitate regular scanning activity, nor does it have a standardized process to analyze and remediate the results. In addition, the historical scans that were performed by KeyPoint included only a sample selection of servers and databases (as opposed to 100 percent of devices), and the scans did not include any user workstations or web applications.

NIST SP 800-53, Revision 4, states that the organization should employ "automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities."

Failure to conduct routine comprehensive vulnerability scans on the network environment greatly increases the risk that an organization has computers and network devices in its technical environment that contain vulnerabilities with known exploits.

Recommendation 11

We recommend KeyPoint implement a formal policy that requires routine vulnerability scanning on all computer servers, databases, web applications, and network devices. The policy should also address the process for analyzing the scan results, tracking remediation activity, and documenting accepted weaknesses.

OCIO/FIS Response:
"We concur. KeyPoint Government Solutions has created a vulnerability management process document. This document formalizes roles, types of scans performed, analysis of results[,] and timelines for mitigation activities[.]"

7. Vulnerabilities Identified in Automated Scans

As mentioned above, we believe that KeyPoint's vulnerability management program could be improved. As part of this audit, we also independently performed our own automated vulnerability scans on a sample of KeyPoint's servers, databases, web applications, and user workstations. The specific vulnerabilities that we identified will not be detailed in this report, but are summarized at a high level below. Copies of the full scan reports were provided directly to KeyPoint during the audit site visit, and were subsequently provided to OPM.

System Patching
KeyPoint appears to be generally compliant with its own patch management policies and procedures. However, our scans detected several instances where critical patches were missing; at the time of the test work these patches were older than the grace period allowed by KeyPoint's policy. The missing patches included both operating system and third-party software.

Noncurrent Software
The results of the vulnerability scans indicated that several servers and workstations contained noncurrent software applications that were no longer supported by the vendors and have known security vulnerabilities.

Server Configuration Vulnerabilities
The results of our scans determined that several isolated server configuration vulnerabilities that have known exploits exist in KeyPoint's technical environment.

Web Application Vulnerabilities
The results of the web application vulnerability scans also indicated that the KeyPoint portal has several vulnerabilities that are susceptible to common malicious attack methods.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53, Revision 4, states that the organization must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly. FISCAM also states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

The vulnerabilities identified in our test work increase the risk that a malicious attack on KeyPoint's technical environment would be successful. These vulnerabilities could have potentially been previously detected and remediated by KeyPoint if it had a more mature vulnerability management program in place (see section C.6, above.)

Recommendation 12
We recommend that KeyPoint make the appropriate changes to its servers, workstations, and web applications to address the specific vulnerabilities identified in our vulnerability scans.

OCIO/FIS Response:
"We partially concur. KeyPoint Government Solutions believes that they have remediated the findings identified by the OIG vulnerability scans. We would like to request a list from the OIG of what tools were used to scan the servers, workstations[,] and web applications along with the actual scan results, so new scans can be completed and compared against the prior results."

OIG Reply:
Per the Rules of Engagement document signed by both the OIG and KeyPoint, the OIG was not permitted to maintain a copy of the raw data vulnerability scan results after the audit site visits. If OPM's OCIO and/or FIS would like a copy of these reports, they must submit that request to KeyPoint. We have, however, provided OPM with a list of tools and targets involved in the scanning exercise along with our detailed notes of the test results. Once OPM has validated that the vulnerabilities have been addressed, it should provide OPM's IOC with relevant supporting evidence.

Recommendation 13
We recommend that KeyPoint implement a methodology to ensure that only current and supported versions of system software are installed on the production servers and workstations.

OCIO/FIS Response:
"We concur. KeyPoint Government Solutions has created a system lifecycle policy to ensure that current supported versions of software and operating systems are installed in the production environment."

D. Configuration Management

We evaluated KeyPoint's computer configuration management program as it relates to the operating platforms that support the processing of OPM information.

KeyPoint uses the United States Government Configuration Baseline for all servers and workstations, and its standard workstation is approved by OPM. However, KeyPoint does not currently have a process in place to routinely audit the current configuration settings of its workstations, servers, and databases against the established baseline security configurations.

FISCAM requires "current configuration information [to] be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected, creating a potential gateway for malicious virus and hacking activity.

Recommendation 14
We recommend that KeyPoint routinely audit all workstation, server, and database security configuration settings to ensure they are in compliance with the approved baselines.

OCIO/FIS Response:
"We concur. FIS will request KeyPoint Government Solutions update their vulnerability management process to audit for changes to approved baselines of workstations, servers[,] and databases."

E. Contingency Planning

We reviewed KeyPoint's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disrupting events occur.

We determined that KeyPoint's contingency planning documentation addressed the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." KeyPoint has identified and prioritized the information systems and resources that are critical to business operations, and has developed procedures to recover those systems and resources. Several opportunities for improvement related to KeyPoint's contingency planning program are outlined below.

1. Primary and Backup Data Center Proximities

KeyPoint uses data replication to establish a system of redundant servers in two data center locations for disaster recovery purposes. However, the close physical proximity of the primary and backup data centers increases the risk that both could be impacted by the same disrupting situation. In addition, the backup data center did not provide a comparable level of environmental and physical access controls to those at the primary data center.

KeyPoint indicated that it has completed a risk assessment and intends to change its alternate data center location. We agree that this change would be beneficial due to the close proximity of the current locations and the weaker environmental and physical access controls.

NIST SP 800-34, Revision 1, states that "the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site."

Failure to establish a refined disaster recovery methodology and location increases the organization's risk to large data losses and potential business outages.

Recommendation 15

We recommend that KeyPoint select an alternate data center with sufficient distance from the primary data center to mitigate the risks of a single disrupting event affecting both locations simultaneously. The new facility should contain physical access and environmental controls comparable to the primary data center.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions is in the process of procuring data center space in [redacted]; well over 1,000 miles from their primary data center.

They plan to have this facility operational by [redacted]."

2. Disaster Recovery Feasibility

KeyPoint's disaster recovery plan is dependent upon on the organization's ability to purchase, configure, and distribute new computer equipment to every affected employee. However, KeyPoint does not have a specific plan or agreement in place with a vendor to procure the equipment quickly. In addition, KeyPoint has not completed a feasibility study to confirm that it is possible to replace and build new hardware in a manner quick enough to ensure that the organization is able to meet its required contractual obligations to OPM.

NIST SP 800-34, Revision 1, provides three basic strategies for preparing for equipment replacement in the event of a disaster: maintaining vendor agreements with service level agreement response times, maintaining surplus equipment inventory, or maintaining existing compatible equipment housed in another location.

NIST SP 800-34, Revision 1, goes on to state that the organization "should consider that purchasing equipment when needed is cost-effective but can add significant overhead time to recovery while waiting for shipment and setup … [and that] based on impacts discovered through the [business impact analysis], consideration should be given to the possibility of a widespread disaster entailing mass equipment replacement and transportation delays that would extend the recovery period."

Failure to determine that the recovery objectives and goals are practical in a disaster recovery situation increases the risk that an organization cannot quickly resume business operations when disrupting events occur.

Recommendation 16

We recommend that KeyPoint conduct a feasibility study for replacing and imaging hardware in a disaster recovery situation.

OCIO/FIS Response:

"We concur. KeyPoint Government [Solutions] has conducted a feasibility study to review the operational plan of using their [redacted] operations office as a backup laptop imaging center. They determined that the facility and staff would be able to procure, image[,] and distribute machines in the case of a disaster recovery effort."

F. Application Controls

The following sections detail our review of the applications and business processes supporting KeyPoint's background investigation process. KeyPoint processes investigation data through applications owned and operated by OPM, and also uses its own Secure Portal for managing and distributing work to KeyPoint employees.

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control of KeyPoint's Secure Portal.

KeyPoint has implemented policies and procedures related to application configuration management, and has also adopted a system development life cycle methodology that IT personnel follow during routine software modifications. We observed the following controls related to testing and approvals of software modifications:

- KeyPoint has implemented practices that allow modifications to be tracked throughout the change process;
- Unit, system, and user acceptance testing are all conducted in accordance with a documented testing strategy; and

- KeyPoint uses a business unit independent from the software developers to move the code between development and production environments to ensure adequate segregation of duties.

Nothing came to our attention to indicate that KeyPoint has not implemented adequate controls related to the application configuration management process.

2. Background Investigation Data Flow

We evaluated the input, processing, and output controls associated with KeyPoint's Secure Portal application and the background investigation process. We have determined the following controls are in place:

- Data is synchronized between the KeyPoint system and OPM systems in a process called "Replication";
- The status of investigations is monitored as they are processed through both systems;
- There are multiple levels of review and verification of the investigator's work; and
- Investigators receive a variety of training on the job to cover both the investigative process and the protection of sensitive data.

As a part of our evaluation of the input controls for the KeyPoint Secure Portal, we reviewed KeyPoint's process of extracting data from OPM's investigative systems and the subsequent input into the KeyPoint Secure Portal. Our analysis of the process indicated that personally identifiable information (PII) is being extracted from OPM's systems that is not required for KeyPoint to perform its contractual obligation.

OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," instructs that Agencies must "review their current holdings of all personally identifiable information and . . . reduce them to the minimum necessary for the proper performance of a documented agency function."

By downloading PII that is not needed from OPM's systems, KeyPoint is creating an unnecessary point of failure for that data to be lost or misused.

Recommendation 17

We recommend that FIS and KeyPoint limit the information pulled in the 'Replication' process to the minimum necessary for use in KeyPoint's Secure Portal.

OCIO/FIS Response:

"We concur. KeyPoint Government Solutions has modified the 'Replication' process to not upload full Case Assignment Transmittals … in the process of parsing necessary information for background investigation item processing."

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

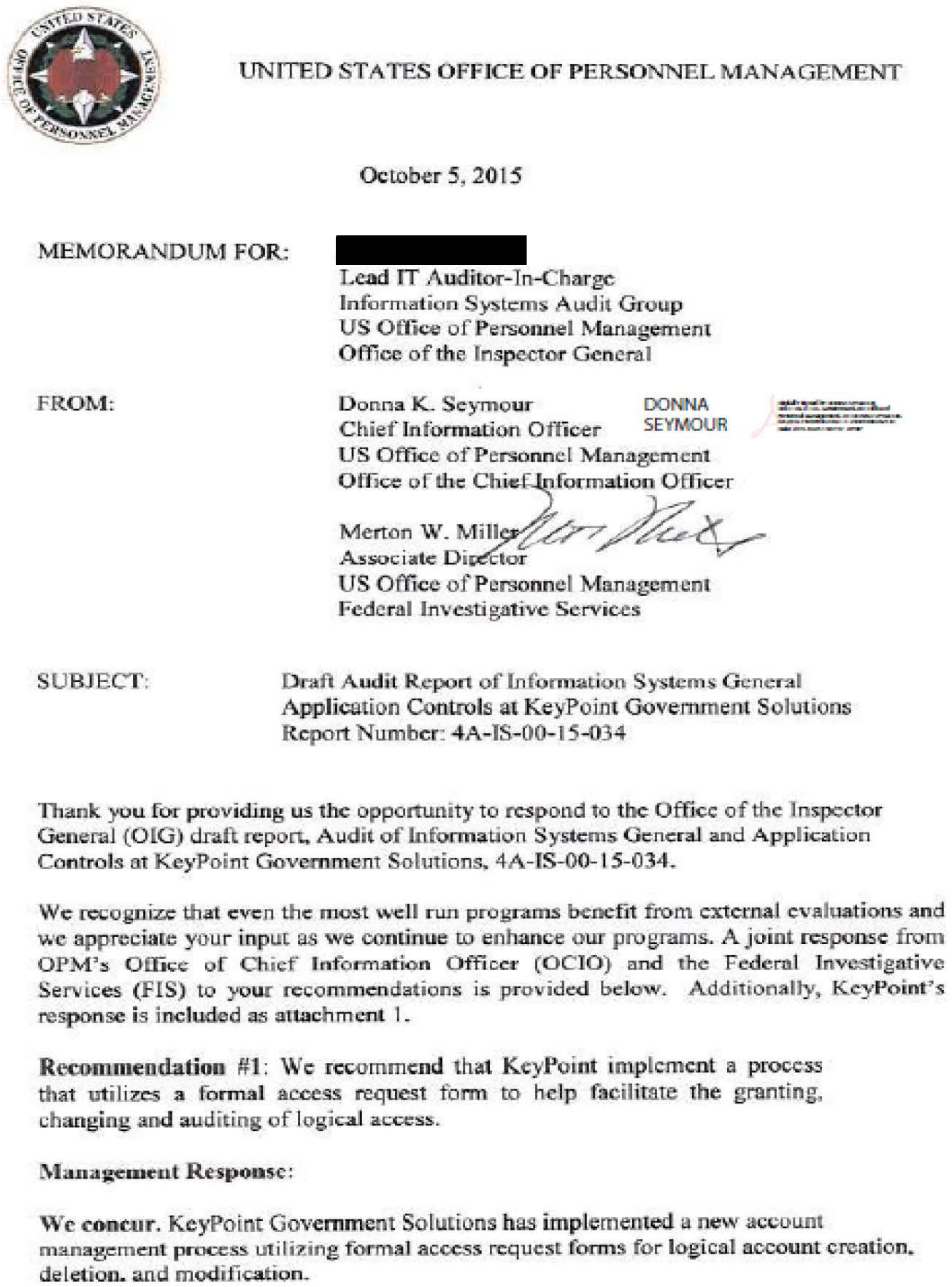
[redacted], Lead IT Auditor-In-Charge

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

V. APPENDIX



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

October 5, 2015

MEMORANDUM FOR: [redacted]
Lead IT Auditor-In-Charge
Information Systems Audit Group
US Office of Personnel Management
Office of the Inspector General

FROM: Donna K. Seymour
Chief Information Officer
US Office of Personnel Management
Office of the Chief Information Officer

DONNA SEYMOUR

Merton W. Miller
Associate Director
US Office of Personnel Management
Federal Investigative Services

SUBJECT: Draft Audit Report of Information Systems General
Application Controls at KeyPoint Government Solutions
Report Number: 4A-IS-00-15-034

Thank you for providing us the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of Information Systems General and Application Controls at KeyPoint Government Solutions, 4A-IS-00-15-034.

We recognize that even the most well run programs benefit from external evaluations and we appreciate your input as we continue to enhance our programs. A joint response from OPM's Office of Chief Information Officer (OCIO) and the Federal Investigative Services (FIS) to your recommendations is provided below. Additionally, KeyPoint's response is included as attachment 1.

Recommendation #1: We recommend that KeyPoint implement a process that utilizes a formal access request form to help facilitate the granting, changing and auditing of logical access.

Management Response:

We concur. KeyPoint Government Solutions has implemented a new account management process utilizing formal access request forms for logical account creation, deletion, and modification.

Recommendation #2: We recommend that KeyPoint implement a formal process to routinely audit information system accounts for appropriateness. This audit should include verification that individuals are still active employees and that their level of access is appropriate.

Management Response:

We concur. KeyPoint Government Solutions have developed a system for the routine audit (weekly) of system account creations, deletions and modifications. They have also created an audit task (annually) for the review of all system accounts.

Recommendation #3: We recommend that KeyPoint develop a comprehensive list of logs that should be stored by each operating system it uses, and also develop procedures that ensure that these logs are routinely reviewed.

Management Response:

We concur. KeyPoint Government Solutions has created a list of all audit events occurring on servers which is stored on the Security Information Event Management (SIEM) tool. They have also created a weekly audit task for the review of all SIEM logs.

Recommendation #4: We recommend that KeyPoint implement a formal access request form for physical access as a part of granting, modifying or removing physical access and that it maintain the forms for audit records.

Management Response:

We concur. KeyPoint Government Solutions has implemented a formal access request form for physical access as part of granting, modifying or removing physical access.

Recommendation #5: We recommend that KeyPoint implement a formal process to routinely audit physical access accounts for appropriateness. This audit should include verification that individuals are still active employees and that their level of access is appropriate.

Management Response:

We concur. KeyPoint Government Solutions has developed a system for the routine audit [redacted] of all physical access to KeyPoint facilities.

Recommendation #6: We recommend that KeyPoint implement a formal incident handling and response process that outlines detection, categorization, analysis, containment, recovery, tracking, and reporting requirements.

We concur. KeyPoint Government Solutions has updated their incident response plan, trained and tested necessary individuals on the incident response plan.

Recommendation #7: We recommend that KeyPoint implement a formal firewall management policy that includes both a configuration standard/baseline and procedures for routinely auditing actual settings against the baseline.

Management Response:

We concur. KeyPoint Government Solutions has developed a firewall baseline and modified their IT Security Management Policy to include the management of firewalls using the baseline configuration and the regular review of firewalls.

Recommendation #8: We recommend that KeyPoint implement and configure a web proxy for all outbound traffic.

Management Response:

We concur. KeyPoint Government Solutions has acquired and installed a next generation firewall that includes a web proxy. The web proxy is configured to limit outbound internet traffic.

Recommendation #9: We recommend that KeyPoint implement technical controls to detect or prevent rogue devices from connecting to its network.

Management Response:

We concur. KeyPoint Government Solutions is in the process of designing and implementing a Network Access Control (NAC) solution. Their NAC solution is planned to be in place by [redacted].

Recommendation #10: We recommend that KeyPoint implement technical controls to protect sensitive data from leaving the network on removable media unencrypted.

Management Response:

We concur. KeyPoint Government Solutions has implemented a group policy object (GPO) rule that eliminates the USB storage devices on corporate computers.

Recommendation #11: We recommend KeyPoint implement a formalized policy to facilitate routine vulnerability scanning on all computer servers, databases, web applications, and network devices. The policy should also address the process for analyzing the scan results, tracking remediation activity, and documenting accepted weaknesses.

We concur. KeyPoint Government Solutions has created a vulnerability management process document. This document formalizes roles, types of scans performed, analysis of results and timelines for mitigation activities

Recommendation #12: We recommend that KeyPoint make the appropriate changes to its servers, workstations, and web applications to address the specific vulnerabilities identified in our vulnerability scans.

Management Response:

We partially concur. KeyPoint Government Solutions believes that they have remediated the findings identified by the OIG vulnerability scans. We would like to request a list from the OIG of what tools were used to scan the servers, workstations and web applications along with the actual scan results, so new scans can be completed and compared against the prior results.

Recommendation #13: We recommend that KeyPoint implement a methodology to ensure that only current and supported versions of system software are installed on the production servers and workstations.

Management Response:

We concur. KeyPoint Government Solutions has created a system lifecycle policy to ensure that current supported versions of software and operating systems are installed in the production environment.

Recommendation #14: We recommend that KeyPoint routinely audit all workstation, server and database security configuration settings to ensure they are in compliance with approved baselines.

Management Response:

We concur. FIS will request KeyPoint Government Solutions update their vulnerability management process to audit for changes to approved baselines of workstations, servers and databases.

Recommendation #15: We recommend that KeyPoint select an alternate data center with sufficient distance from the primary data center to mitigate the risks of a single disrupting event affecting both locations simultaneously. The new facility should contain physical access and environmental controls comparable to the primary data center.

Management Response:

We concur. KeyPoint Government Solutions is in the process of procuring data center space in [redacted]; well over 1,000 miles from their primary data center.

They plan to have this facility operational by [redacted].

Recommendation #16: We recommend that KeyPoint conduct a feasibility study for replacing and imaging hardware in a disaster recovery situation.

Management Response:

We concur. KeyPoint Government Services has conducted a feasibility study to review the operational plan of using their [redacted] operations office as a backup laptop imaging center. They determined that the facility and staff would be able to procure, image and distribute machines in the case of a disaster recovery effort.

Recommendation #17: We recommend that FIS and KeyPoint limit the information pulled in the 'Replication' process to the minimum necessary for use in KeyPoint's Secure Portal.

Management Response:

We concur. KeyPoint Government Solutions has modified the 'Replication' process to not upload full Case Assignment Transmittals (CATs) in the process of parsing necessary information for background investigation item processing.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact [redacted], [redacted], [redacted]@opm.gov OR [redacted], [redacted], [redacted]@opm.gov.

cc: Angela Bailey
Chief Operating Officer
US Office of Personnel Management

Janet Barnes
Director, Internal Oversight and Compliance
US Office of Personnel Management

[redacted]
Senior Procurement Executive
US Office of Personnel Management

KeyPoint Government Solutions ("KeyPoint" or "KGS") welcomes the opportunity to comment upon the Office of Inspector General's ("OIG's") recommendations following its audit of KGS's systems.

Providing a secure environment for our clients' data is, and always will be a top priority for KeyPoint, and as such, KeyPoint concurs with the OIG's recommendations. Below, we provide more detailed comments regarding enhancements to our already robust systems and processes.

OIG Recommendation 1

We recommend that KeyPoint implement a process that utilizes a formal access request form to help facilitate the granting, changing and auditing of logical access.

KeyPoint Comment to Recommendation 1

While KeyPoint employed a process that utilized a ticketing system to grant and change user logical access prior to the OIG visit, KeyPoint agrees that a standardized form will assist with consistency and audit of process.

KeyPoint has developed standardized forms for the process of logical and physical account management and a process to routinely audit these accounts. The new standardized forms create an artifact for each of the account transitions that occur during an employee's/contractor's engagement with KeyPoint. The new forms include:

- KGS New Hire Physical and Logical Access Request – Form for all new engagements with KeyPoint.
- KGS Logical Access Change Request Form – Form for all changes of account privileges at KeyPoint.
- KGS Account Conversion Request Form – Form for the specific change in role between an employee and contractor.
- KGS Physical and Logical Access Termination Request Form - Form for the termination of an employee and contractor engagement at KeyPoint.

These forms augment the existing KeyPoint account management process. These forms are used as part of the account audit process as described in Recommendation 2.

KeyPoint considers Recommendation 1 fully implemented.

OIG Recommendation 2

We recommend that KeyPoint implement a formal process to routinely audit information system accounts for appropriateness. This audit should include verification that individuals are still active employees and that their level of access is appropriate.

KeyPoint Comment to Recommendation 2

While KeyPoint routinely audited accounts prior to the OIG audit, KeyPoint has further reviewed the company's information system account audits processes and has developed an information system to manage audit tasks.

To manage audits, KeyPoint created the KeyPoint Audit Reporting Tool (KART). The KART system was designed to manage the process of routine audits of KeyPoint control compliance. The KART system was designed to meet five major goals. (1) A mechanism to record the numerous KeyPoint audit tasks each on its own reporting schedule. (2) To provide an assigned owner or group to an audit task. (3) To provide a timely reminder to the auditor of an audit task. (4) To provide for the collection and indexing of audit artifacts. (5) A system of record to record and provide reporting that audit tasks are being performed per KeyPoint policies and procedures. To complete these goals, the KART tool consists of two major components. The first component of KART is an automated message which is programmed to be sent to a person or group of people instructing them to perform an audit or review of a control item. This system allows for the assignment of an individual or group to perform the audit task. KART also defines the instruction to be provided to the auditor which comes in the form of an email. Each KART task is also assigned a schedule for this audit task to be performed, commonly daily, weekly, monthly quarterly or annually. The second component of KART is a response and artifact storage system. Once the audit or review is completed, the user replies to the original message indicating that the assigned task has been complete. This message may include any output or artifacts that may be required as part of the audit task. The message reply with the attached documents is then stored in the KART system. The responses in KART are secure and searchable for later review for potential audits of the KeyPoint audit process.

KeyPoint has created a number of audit tasks that verify that user accounts are accurately assigned to only active employees and contractors and that permission levels are compliant and appropriate. To perform this account verification audit, KeyPoint has created the following audit tasks in the KART system:

- KART [redacted] Privilege Account Audit
- KART [redacted] New Domain Accounts Audit
- KART [redacted] Deleted Domain Accounts Audit
- KART [redacted] Review of All Accounts Audit

KeyPoint considers Recommendation 2 fully implemented.

OIG Recommendation 3

We recommend that KeyPoint develop a comprehensive list of logs that should be stored by each operating system it uses, and also develop procedures that ensure that these logs are routinely reviewed.

KeyPoint Comment to Recommendation 3

Prior to the OIG audit, KeyPoint maintained numerous logs in our Security Information and Event Management (SIEM) device.

KeyPoint conducted a review of our system logs and related policies and developed a comprehensive list of server logs for all systems on our network. The list is available for review. The log files are moved from their originating servers and are stored for analysis on the KeyPoint Security SIEM device. On the SIEM these log files are maintained for an organizationally defined period of time as described by the KeyPoint System Security Plan (SSP). KeyPoint developed a routine audit task in the KeyPoint KART system to review all audit records weekly by the KeyPoint Security System Administrator.

KeyPoint considers Recommendation 3 fully implemented.

OIG Recommendation 4

We recommend that KeyPoint implement a formal access request form for physical access as a part of granting, modifying or removing physical access and that it maintain the forms for audit records.

KeyPoint Comment to Recommendation 4

While KeyPoint had a process for the granting, modifying and removing of physical access accounts prior to the OIG audit, KeyPoint agrees that a standardized form will enhance consistency and audit of process

KeyPoint has developed standardized forms for the process of logical and physical account management and a process to routinely audit these accounts. The standardized forms create an artifact for each of the account transitions that occur during an employee's/contractor's engagement with KeyPoint and what physical access they will need, down to the office, secure area and time of entry allowed. The forms include:

- KGS New Hire Physical and Logical Access Request Form
- KGS Physical and Logical Access Termination

Request Form KeyPoint considers Recommendation 4

fully implemented.

OIG Recommendation 5

We recommend that KeyPoint implement a formal process to routinely audit physical access accounts for appropriateness. This audit should include verification that individuals are still active employees and that their level of access is appropriate.

KeyPoint Comment to Recommendation 5
Prior to the OIG audit, KeyPoint audited physical access accounts. In an effort to enhance our processes, KeyPoint has reviewed our physical access account audit processes and developed two periodic account reviews to verify that only proper access is provided to KeyPoint employees and contractors. These physical account tasks are managed in the KeyPoint KART system. KeyPoint has developed the following periodic audit tasks:

- KART [redacted] Physical Security Access Review Audit
- KART [redacted] Review of ALL Physical Access Audit

KeyPoint considers Recommendation 5 fully implemented.

OIG Recommendation 6

We recommend that KeyPoint implement a formal incident handling and response process that outlines detection, categorization, analysis, containment, recovery, tracking, and reporting requirements.

KeyPoint Comment to Recommendation 6

Prior to the OIG audit, KeyPoint did have an incident response plan that had been reviewed and approved by the Office of Personnel Management (OPM) with our December 2012 Authorization To Operate (ATO) submission; KeyPoint agrees that the plan should be reviewed and potentially enhanced.

KeyPoint has reviewed its Incident Response Plan in order to verify that it properly outlines guidance on the detection, categorization, analysis, containment, recovery, tracking and reporting requirements of each incident. A number of enhancements to the plan have been developed, including a process for the categorization of incidents. .

KeyPoint considers Recommendation 6 fully implemented.

OIG Recommendation 7

We recommend that KeyPoint implement a formal firewall management policy that includes both a configuration standard/baseline and procedures for routinely auditing actual settings against the baseline

KeyPoint Comment to Recommendation 7

Prior to the OIG audit KeyPoint did maintain our firewall and other network border devices using a set of procedures but did not maintain a formal policy.

KeyPoint has documented a firewall baseline configuration and created a Firewall Management Policy. The Firewall Management Policy, which resides in the KeyPoint IT Security Management Policy 2015, details that Firewalls are to be managed against a baseline configuration and are to be audited monthly. KeyPoint also reviewed the baseline configuration of the firewalls verifying that they are consistent with corporate policy and goals. This baseline is now documented as our baseline configuration.

KeyPoint considers Recommendation 7 fully implemented.

OIG Recommendation 8

We recommend that KeyPoint implement and configure a web proxy for all outbound traffic.

KeyPoint Comment to Recommendation 8

Prior to the OIG audit, KeyPoint managed outbound traffic to the internet from users using management controls.

KeyPoint has acquired a next generation firewall that includes a web proxy for all outbound traffic to the public Internet. KeyPoint acquired the equipment from a leading provider of this technology and worked with the vendor to implement the equipment in the KeyPoint environment.

KeyPoint considers Recommendation 8 fully implemented.

OIG Recommendation 9

We recommend that KeyPoint implement technical controls to detect or prevent rogue devices from connecting to its network.

KeyPoint Comment to Recommendation 9

While prior to the OIG audit KeyPoint had numerous physical controls to limit direct access to the network and all border devices required multi-factor authentication to limit remote access to the network, KeyPoint agrees that a Network Access Control (NAC) solutions would further enhance our security posture.

KeyPoint has initiated engineering processes to implement rogue device detection on the KeyPoint network. This project is currently progressing and plans to be fully implemented by [redacted] [redacted].

KeyPoint considers Recommendation 9 on plan for a [redacted] full implementation.

Recommendation 10

We recommend that KeyPoint implement technical controls to protect sensitive data from leaving the network on removable media unencrypted.

KeyPoint Comment to Recommendation 10

While prior to the OIG audit KeyPoint had management controls that controlled the removal of sensitive data from the network, KeyPoint agrees that a technical control to enforce potential data removal would enhance our data management posture.

KeyPoint has implemented a technical control to disable computer USB data ports on nearly all corporate machines. Exceptions were made for specific roles such as IT technical support who utilize USB devices as part of machine maintenance activities.

KeyPoint considers Recommendation 10 fully implemented.

OIG Recommendation 11

We recommend KeyPoint implement a formalized policy to facilitate routine vulnerability scanning on all computer servers, databases, web applications, and network devices. The policy should also address the process for analyzing the scan results, tracking remediation activity, and documenting accepted weaknesses.

KeyPoint Comment to Recommendation 11

While prior to the OIG audit KeyPoint did routinely scan systems on the network to identify potential vulnerabilities, we agree that a formalized policy would facilitate these reviews.

KeyPoint has reviewed its system scanning activities, including how we analyze and categorize the results from vulnerability scans and our process for remediating any issues found. The results of this review assisted in the development of the KeyPoint Vulnerability Management Process. The goal of the KeyPoint Vulnerability Management Process is to detect and remediate vulnerabilities in a timely fashion. This is done by: defining roles in the vulnerability scanning process; defining the scope and types of scans to be performed; the frequency of scanning activities, how vulnerabilities are categorized, mitigation timelines for each risk categorization; a re-scanning process to determine the successful implementation of mitigation efforts and the technical control to verify that this process is executed by plan. This KeyPoint Vulnerability Management Process has been successfully applied to the KeyPoint environment.

KeyPoint considers Recommendation 11 fully implemented.

OIG Recommendation 12

We recommend that KeyPoint make the appropriate changes to its servers, workstations, and web applications to address the specific vulnerabilities identified in our vulnerability scans.

KeyPoint Comment to Recommendation 12

Prior to the OIG audit, KeyPoint patched its servers as updates became available from system vendors.

KeyPoint has taken steps to mitigate known vulnerabilities found from scanning activities pursuant to the KeyPoint Vulnerability Management Process. KeyPoint has also configured existing scanning software and acquired scanning software to mirror the scanning processes that were performed by the OIG to confirm closure on vulnerability items.

KeyPoint considers Recommendation 12 fully implemented.

OIG Recommendation 13

We recommend that KeyPoint implement a methodology to ensure that only current and supported versions of system software are installed on the production servers and workstations.

KeyPoint Comment to Recommendation 13

Prior to the OIG audit KeyPoint kept its systems up-to-date with current supported versions of systems.

KeyPoint has drafted and implemented the KeyPoint System Lifecycle and Management Policy, which states that only current manufacturer-supported versions of system software be allowed in our environment. After implementation of the policy, KeyPoint engaged in a comprehensive review of all system software to verify its compliance with the new policy. This review and necessary remediation activities have been completed.

KeyPoint considers Recommendation 13 fully implemented.

OIG Recommendation 14

We recommend that KeyPoint routinely audit all workstation, server and database security configuration settings to ensure they are in compliance with approved baselines.

KeyPoint Comment to Recommendation 14

While prior to the OIG audit KeyPoint did maintain servers, workstations and databases to specific configuration standards, KeyPoint agrees that routine audits of these equipment and databases will facilitate compliance with approved standards.

KeyPoint has reviewed its routine audit activities for workstations, servers and database configurations. As a result of this review, KeyPoint added configuration management of workstations, servers and databases as part of the KeyPoint Vulnerability Management Process, which is detailed in our comment to Recommendation 11. This document formalizes roles in the compliance scanning process, scope of scans, frequency of scans and timelines to mitigate found results.

KeyPoint considers Recommendation 14 fully implemented.

OIG Recommendation 15

We recommend that KeyPoint select an alternate data center with sufficient distance from the primary data center to mitigate the risks of a single disrupting event affecting both locations simultaneously. The new facility should contain physical access and environmental controls comparable to the primary data center.

KeyPoint Comment to Recommendation 15

While prior to the OIG audit KeyPoint felt that our primary and secondary data centers being nearly 50 miles apart in the relatively low-risk [redacted] area provided sufficient mitigating distance for nearly all disaster events, KeyPoint agrees that additional distance, if logistically possible, can improve disaster recovery posture.

Prior to the OIG out-briefing from the onsite inspection portion of the audit, KeyPoint had begun looking for potential secondary data center sites in the [redacted] area near our [redacted] office. KeyPoint also started engineering a telecommunication solution that would allow for the same high level of readiness in the case of a disaster currently available through our data center configuration. As part of the procurement effort, KeyPoint is only considering data center locations with physical access controls as strong as, or stronger than, our primary data center. KeyPoint is currently near a contract execution point and plans to have our new secondary data center operational by [redacted].

KeyPoint considers Recommendation 16 on plan for an [redacted] full implementation.

OIG Recommendation 16

We recommend that KeyPoint conduct a feasibility study for replacing and imaging hardware in a disaster recovery situation.

KeyPoint Comment to Recommendation 16

Prior to the OIG audit, KeyPoint felt that we had a high level of readiness to move laptop imaging operations to our secondary [redacted] office but had not yet undertaken an actual feasibility study.

KeyPoint has conducted a feasibility study for the replacing and imaging of hardware from our [redacted] office. The feasibly study considered if KeyPoint could successfully execute from the [redacted] office the equipment procurement, imaging, distribution and support of laptops in the case of a disaster affecting our primary [redacted] [redacted] office. The study found that the [redacted] office has the capabilities to perform all necessary activities to reconstitute laptops in our primary [redacted] office within [redacted] of a disaster being declared.

KeyPoint considers Recommendation 16 fully implemented.

OIG Recommendation 17

We recommend that FIS and KeyPoint limit the information pulled in the 'Replication' process to the minimum necessary for use in KeyPoint's Secure Portal.

KeyPoint Comment to Recommendation 17

Prior to the OIG audit, KeyPoint had performed a review of all PII stored in the KeyPoint portal database to verify that it stored only data that was required to perform the work of the contract. KeyPoint agrees with the OIG that in the process of accessing the necessary PII records during the 'replication' process unnecessary PII details would be exposed as they were on the same OPM provided electronic document, the Case Assignment Transmittals (CATs). While these details were not stored on the KeyPoint database during the investigative process, they were temporarily accessed during the replication process.

KeyPoint has reviewed how its systems review records on the PIPS mainframe. KeyPoint has since modified the Replication process to not access the entire CAT file on the KeyPoint portal but to parse the non-PII data locally and save the non-PII data on the KeyPoint Portal.

KeyPoint considers Recommendation 17 fully implemented.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100