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

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INVESTIGATIONS, TRACKING, ASSIGNING AND EXPEDITING SYSTEM FY 2014

Report No. 4A-IS-00-14-017

April 3, 2014

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INVESTIGATIONS, TRACKING, ASSIGNING AND EXPEDITING SYSTEM
FY 2014

WASHINGTON, D.C.

Report No. 4A-IS-00-14-017

Date: 04/03/14

Michael R. Esser
Assistant Inspector General for Audits

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INVESTIGATIONS, TRACKING, ASSIGNING AND EXPEDITING SYSTEM
FY 2014

WASHINGTON, D.C.

Report No. 4A-IS-00-14-017

Date: 04/03/14

This final audit report discusses the results of our audit of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Investigations, Tracking, Assigning and Expediting (iTRAX) System. Our conclusions are detailed in the "Results" section of this report.

Security Assessment and Authorization (SA&A)

An SA&A of iTRAX was completed in October 2013. We reviewed the authorization package for all required elements of an SA&A, and determined that the package contained all necessary documentation.

Federal Information Processing Standards (FIPS) 199 Analysis

The security categorization of iTRAX appears to be consistent with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 requirements, and we agree with the categorization of "high."

System Security Plan (SSP)

The iTRAX SSP contains the critical elements required by NIST SP 800-18 Revision 1.

Security Assessment Plan and Report

A security control assessment plan and report were completed in June and October 2013 for iTRAX as a part of the system's SA&A.

Security Control Self-Assessment

Federal Investigative Services ensures that annual security control self-assessments are conducted in accordance with OPM policy.

Contingency Planning and Contingency Plan Testing

A contingency plan was developed for iTRAX that is in compliance with NIST SP 800-34 Revision 1 and is tested annually.

Privacy Impact Assessment (PIA)

A privacy threshold analysis was conducted for iTRAX and indicated that a PIA was required. A PIA was conducted in June 2013.

Plan of Action and Milestones (POA&M) Process

The iTRAX POA&M follows the format of the OPM POA&M guide, and has been routinely submitted to the OCIO for evaluation.

NIST SP 800-53 Revision 3 Evaluation

We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 3 was implemented for iTRAX. We determined that several controls could be improved.

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 audited the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Investigations, Tracking, Assigning and Expediting (iTRAX) System.

Background

iTRAX is one of OPM's 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 critical systems, on a rotating basis.

The iTRAX web-based application is designed to support delivery of services to the Federal Investigative Service (FIS), which is responsible for delivery of investigative products and services that ensure federal agencies have the data needed on which to base determinations of eligibility for a security clearance or suitability for employment in sensitive positions. The system is operated and hosted by an OPM contractor, CACI, on behalf of FIS.

This was our first audit of the security controls surrounding iTRAX. We discussed the results of our audit with FIS representatives at an exit conference.

Objectives

Our objective was to perform an evaluation of the security controls for iTRAX to ensure that FIS officials have managed the implementation of IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

OPM's IT security policies require owners 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 audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for iTRAX, including:

- Security Assessment and Authorization;
- FIPS 199 Analysis;
- Risk Assessment;
- System Security Plan;
- Security Assessment Plan and Report;
- 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 Revision 3 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 FIS officials responsible for iTRAX, including IT security controls in place as of December 2013.

We considered the iTRAX 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 FIS and CACI employees with iTRAX 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 iTRAX 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 iTRAX system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Security Privacy and Policy Handbook;
- 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;
- 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 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 3, Recommended Security Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Volume II, 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 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 2013 through January 2014 in CACI's Chantilly, Virginia facility and OPM's Washington, D.C. office. This was our first audit of the security controls surrounding iTRAX.

Compliance with Laws and Regulations

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

Results

I. Security Assessment and Authorization

A Security Assessment and Authorization (SA&A) of iTRAX was completed in October 2013.

OPM's Chief Information Security Officer reviewed the iTRAX SA&A package and signed the system's authorization letter on October 28, 2013. The system's authorizing official signed the letter and authorized the continued operation of the system on October 30, 2013.

NIST SP 800-37 Revision 1 "Guide for Applying Management Framework to Federal Information Systems," provides guidance to federal agencies in meeting security accreditation requirements. The iTRAX SA&A appears to have been conducted in compliance with NIST requirements.

II. FIPS 199 Analysis

Federal Information Processing Standards (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 II, 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 iTRAX FIPS 199 Security Categorization Template analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. iTRAX is categorized with a high impact level for confidentiality, moderate for integrity, low for availability, and an overall categorization of "high."

The security categorization of iTRAX appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and we agree with the categorization of "high."

III. 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 and Organizations. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in a System Security Plan (SSP) for each system, and provides guidance for doing so.

The SSP for iTRAX was created using the template outlined in NIST SP 800-18 Revision 1. The template requires that the following elements be documented within the SSP:

- 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;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

We reviewed the iTRAX SSP and determined that it adequately addresses each of the elements required by NIST.

IV. Security Assessment Plan and Report

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for iTRAX in June and October 2013 as a part of the system's SA&A process. The SAP and SAR were completed by a contractor that was operating independently from FIS and CACI. We reviewed the documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a "high" security categorization according to NIST SP 800-53 Revision 3.

The SAP outlined the assessment approach and test methods. The SAR identified 25 control weaknesses; 18 of those weaknesses were immediately remediated, and the remaining weaknesses were added to the iTRAX Plan of Action & Milestones (POA&M). A risk rating was applied to each weakness to determine the potential impact of exploitation.

We also reviewed the Security Assessment results table that contained the detailed results of the NIST SP 800-53 Revision 3 controls testing. The table indicated that five controls were not fully satisfied. These controls were appropriately documented in the system POA&M for tracking.

Nothing came to our attention to indicate that the security controls of iTRAX have not been adequately tested by an independent source.

V. Security Control Self-Assessment

OPM requires that the IT security controls of each contractor-operated system be tested on an annual basis. In the years that an independent assessment is not being conducted on a system as part of an SA&A, the system's owner must ensure that annual controls testing is performed by a government employee or an independent third party (i.e., the contractor operating the system should not act as the assessor).

We reviewed the iTRAX security control tests for the past three years, and nothing came to our attention to indicate that the security controls of iTRAX have not been adequately tested.

A fourth revision to NIST SP 800-53 was published in April 2013, and agencies are allowed one year to implement any new or modified NIST guidance. We informed FIS that they must conduct an analysis to determine if testing modifications are necessary to comply with NIST SP 800-53 Revision 3 for the fiscal year 2014 security controls test.

VI. Contingency Planning and Contingency Plan Testing

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The iTRAX contingency plan documents the functions, operations, and resources necessary to restore and resume iTRAX operations when unexpected events or disasters occur. The iTRAX contingency plan adequately follows the format suggested by NIST SP 800-34 Revision 1 and contains the required elements.

Contingency Plan Test

NIST SP 800-34 Revision 1 provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A tabletop test of the iTRAX contingency plan was conducted by CACI officials in August 2013. The test involved documenting and discussing the recovery process for the iTRAX system. The testing documentation contained an analysis and review of the results. While the overall FIPS 199 security categorization of iTRAX is "high," the availability category is "low." NIST SP 800-34 Revision 1 states that tabletop exercises are sufficient testing for systems with a "low" availability categorization.

VII. Privacy Impact Assessment

FISMA 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.

FIS completed an initial privacy screening or Privacy Threshold Analysis of iTRAX and determined that a PIA was required for this system. A PIA was completed in June 2013 and approved by the system owner and CIO.

VIII. 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.

We evaluated the iTRAX POA&M and verified that it follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool, for evaluation. We determined that the weaknesses discovered during the SA&A security assessment were appropriately included in the POA&M. Nothing came to our attention to indicate that there are any current weaknesses in the management of the iTRAX POA&M.

IX. NIST SP 800-53 Revision 3 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we independently evaluated whether a subset of these controls had been implemented for the iTRAX. We tested approximately 55 security controls that were identified as being system-specific or a hybrid control. We tested one or more controls from each of the following control families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authorization
- Media Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communication Protection
- System and Information Integrity

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

We determined that all tested security controls appear to be in compliance with NIST SP 800-53 Revision 3 requirements with the following exceptions:

1. Control AC-5 – Separation of Duties

During interviews with subject matter experts we were informed that CACI application developers have access to the iTRAX production environment and have administrator privileges within the back-end software platform, Serena Business Manager. This situation constitutes a segregation of duties violation.

NIST SP 800-53 Revision 3 states that organizations should separate duties of individuals as necessary, to prevent malevolent activity without collusion, document separation of duties, and implement separation of duties through assigned information system access

authorizations. Failure to ensure separation of duties increases the risk that the application developers could make unauthorized or malicious modifications to the iTRAX application.

Recommendation 1

We recommend that FIS ensure that proper separation of duties is maintained within iTRAX and the back-end software platform.

FIS Response:

"FIS agrees with the recommendation and has taken action to resolve the issue prior to the report's finalization. The iTRAX Development Team has been segregated into two groups to meet separation of duties requirements. Administrative privileges have been removed for all Developers except the Serena Development Team Lead (normally not involved in actual code development). The Serena Development Team Lead will be added to the Configuration Control Board (CCB) and will coordinate with approval procedures, internally review all code created on the development environment prior to production approval, and orchestrate periodic and planned iTRAX software updates to the production server. The supporting evidence has been supplied in the Post-Exit Brief Submission package."

OIG Reply:

The evidence provided by FIS in response to the draft audit report indicates that adequate segregation of duties has been implemented; no further action is required.

2. Control AC-7 – Unsuccessful Login Attempts

iTRAX servers and user workstations are not configured in accordance with OPM security guidelines. User accounts are appropriately configured to automatically lock after an incorrect password has been entered three times. However, the accounts automatically unlock after a predefined period of time; 15 minutes for workstations and 30 minutes for servers.

The OPM Security and Privacy Policy Handbook requires that "the information system automatically locks the account until released by an administrator when the maximum number of unsuccessful attempts is exceeded." Failure to enforce these guidelines increases the risk of unauthorized access to the system through a brute force attack.

Recommendation 2

We recommend that FIS ensure that iTRAX server and workstation account lockout settings are modified to comply with OPM policy.

FIS Response:

"FIS agrees with the recommendation. These requirements are appropriately met in regards to logging into the OPM CISCO VPN and at the iTRAX application interface thru PIV logon. However, the local machine login continues to use user id and password. As a result, the account unlock setting is currently 15 minutes. The iTRAX users are a remote

workforce across the country and sending the laptop to a central location for an Administrator to unlock the account (per the OPM policy) is not a feasible option based on investigation timelines dictated by federal law.

FIS and the iTRAX technical teams have been pursuing internal conversations with OPM and other parties to find a proper resolution for PIV authentication on the local endpoints. POA&Ms (POA&Ms # FYI4-QI-ITRAX-03, FY14-QI-ITRAX-04 and FY14-QI-ITRAX-05) are already in place regarding the need for PIV authentication of these devices. FIS will provide more detail in the POA&Ms and will accurately reflect the condition in Trusted Agent FISMA (TAF)."

OIG Reply:

As part of the audit resolution process, we recommend that FIS provide OPM's Internal Oversight and Compliance (IOC) division with evidence that server and workstation account lockout settings are configured in compliance with OPM guidelines.

Control AU-6 – Audit Review, Analysis, and Reporting

iTRAX servers are configured to record the activity of privileged users (i.e., system administrators). However, the event logs generated by these servers are only reviewed retroactively if a problem has been reported or detected, and there is no process in place to routinely review privileged user activity logs. Furthermore, there is no policy or procedure documenting the process for reviewing audit logs or reporting anomalies.

NIST SP 800-53 Revision 3 requires that an organization "Reviews and analyzes information system audit records . . . for indications of inappropriate or unusual activity, and reports findings to designated organizational officials. . . ."

Failure to routinely review elevated user activity increases the risk that malicious activity could go undetected and sensitive information could be compromised.

Recommendation 3

We recommend that FIS ensure that a documented process is in place to routinely review iTRAX privileged user (administrator) activity.

FIS Response:

"FIS agrees with the recommendation and has taken action to resolve the issue prior to the report's finalization. iTRAX did not have a documented procedure to satisfy this requirement. Logs were monitored on an as needed basis, but no official audit procedure existed for Administrator activity and no official reporting mechanisms were identified or utilized. This situation has been resolved with newly introduced policy, procedure and reporting documentation. The supporting evidence has been supplied in the Post-Exit Brief Submission package."

OIG Reply:

The evidence provided by FIS in response to the draft audit report indicates that a policy, procedures, and an event tracking template related to reviewing privileged user activity have been created. As part of the audit resolution process we recommend that FIS provide IOC with evidence that the template is being utilized in accordance with the new policy and procedures.

Control PE-1 – Physical and Environmental Protection Policy and Procedures

Although the current employees at CACI facilities have an informal understanding of their roles and responsibilities when responding to an emergency, the organization has not formally documented emergency response procedures. We were told that CACI is in the process of collecting and documenting procedures in one centralized repository, but they have not done so at this time.

NIST SP 800-53 Revision 3 requires that an organization have "A formal, documented physical and environmental protection policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance" and "Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls."

Failure to establish documented emergency response procedures increases the likelihood that personnel will not know how to respond in emergency situations within the computer room.

Recommendation 4

We recommend that FIS ensure that emergency response procedures are formally documented for CACI facilities.

FIS Response:

"FIS agrees with the recommendation and has taken action to resolve the issue prior to the report's finalization. FIS would like to specify the CACI facilities in question are specifically those housing the IT infrastructure for the iTRAX system located at the Park East Data Center in Chantilly, Virginia. Emergency response procedures have been formally documented and will be attached to the System Security Plan. The supporting evidence has been supplied in the Post-Exit Brief Submission package."

OIG Reply:

The evidence provided by FIS in response to the draft audit report indicates that emergency response procedures have been formally documented; no further action is required.

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], Auditor-In-Charge
- [redacted], IT Auditor

Appendix

United States Office of Personnel Management

TO: [redacted]
Chief, Information Systems Audits Group

FROM: [redacted]
iTRAX System Owner
Chief, IT System Security & Access
Federal Investigative Services

[redacted] 2/19/2014

SUBJECT: **Response to "Draft" Report No. 4A-IS-00-14-017 – Dated - January 28, 2014**

OIG Recommendation 1:
We recommend that FIS ensure that the iTRAX system is subject to a functional disaster recovery test and that the system can be fully recovered at the backup location.

FIS Response:
FIS respectfully disagrees with the OIG recommendation and requests an opportunity for further discussion on this finding. In August 2013, a full interrupt test and server rebuild was completed for the iTRAX system as identified in the System Security Plan (SSP) dated October 2013. In addition to the actual contingency situation declaration in August, a table top exercise was also completed and with successful results reported.

FIS would also request and opportunity to discuss the OPM policy on security control scoping guidance. Although the overall system categorization of the iTRAX system is "High", the FIPS 199 indicates a "Low" categorization for "Availability". Based on our understanding of OPM policy and the requirements identified in NIST 800-34 Rev1, we believe tape back-up and plans for relocation to a cold site should fully satisfy the requirement.

OIG Recommendation 2:
We recommend that FIS ensure that proper separation of duties is maintained within iTRAX and the back-end software platform.

FIS Response:
FIS agrees with the recommendation and has taken action to resolve the issue prior to the report's finalization. The iTRAX Development Team has been segregated into two groups to meet separation of duties requirements. Administrative privileges have been removed for all Developers except the Serena Development Team Lead (normally not involved in actual code development). The Serena Development Team Lead will be added to the Configuration Control Board (CCB) and will coordinate with approval procedures, internally review all code created on the development environment prior to production approval, and orchestrate periodic and planned iTRAX software updates to the production server. The supporting evidence has been supplied in the Post-Exit Brief Submission package.

OIG Recommendation 3:
We recommend that FIS ensure that iTRAX server and workstation account lockout settings are modified to comply with OPM policy.

FIS Response:
FIS agrees with the recommendation. These requirements are appropriately met in regards to logging into the OPM CISCO VPN and at the iTRAX application interface thru PIV logon. However, the local machine login continues to use user id and password. As a result, the account unlock setting is currently 15 minutes. The iTRAX users are a remote workforce across the country and sending the laptop to a central location for an Administrator to unlock the account (per the OPM policy) is not a feasible option based on investigation timelines dictated by federal law.

FIS and the iTRAX technical teams have been pursuing internal conversations with OPM and other parties to find a proper resolution for PIV authentication on the local endpoints. POA&Ms (POA&Ms # FY14-Q1-ITRAX-03, FY14-Q1-ITRAX-04 and FY14-Q1-ITRAX-05) are already in place regarding the need for PIV authentication of these devices. FIS will provide more detail in the POA&Ms and will accurately reflect the condition in Trusted Agent FISMA (TAF).

OIG Recommendation 4:
We recommend that FIS ensure that a documented process is in place to routinely review iTRAX privileged user (administrator) activity.

FIS Response:
FIS agrees with the recommendation and has taken action to resolve the issue prior to the report's finalization. iTRAX did not have a documented procedure to satisfy this requirement. Logs were monitored on an as needed basis, but no official audit procedure existed for Administrator activity and no official reporting mechanisms were identified or utilized. This situation has been resolved with newly introduced policy, procedure and reporting documentation. The supporting evidence has been supplied in the Post-Exit Brief Submission package.

OIG Recommendation 5:
We recommend that FIS ensure that emergency response procedures are formally documented for CACI facilities.

FIS Response:
FIS agrees with the recommendation and has taken action to resolve the issue prior to the report's finalization. FIS would like to specify the CACI facilities in question are specifically those housing the IT infrastructure for the iTRAX system located at the Park East Data Center in Chantilly, Virginia. Emergency response procedures have been formally documented and will be attached to the System Security Plan. The supporting evidence has been supplied in the Post-Exit Brief Submission package.