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 CACI International, Inc.

Report Number 6A-0A-00-16-004
July 21, 2016

-- CAUTION --

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at CACI International, Inc.

Report No. 6A-0A-00-16-004 **July 21, 2016**

Why Did We Conduct the Audit?

CACI International, Inc. (CACI) is a service contractor for the U.S. Office of Personnel Management's (OPM) Federal Investigative Services (FIS). The Investigation and Managements Service Division (IMSD) within CACI supports OPM's 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. The Federal Information Security Modernization Act (FISMA) requires that the Office of the Inspector General (OIG) perform an audit of the information technology (IT) systems supporting OPM, including those operated by a contractor such as CACI.

What Did We Audit?

The OIG has completed a performance audit of CACI to ensure that the CACI information systems supporting OPM's FIS are managed in compliance with security policies, procedures, and 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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of CACI and IMSD determined that:

- CACI and IMSD have established a security management program and have implemented a wide variety of security controls to protect sensitive data.
- IMSD has implemented controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information. However, we noted that the controls related to removing logical access for terminated employees could be improved. In addition IMSD could benefit from adding additional controls related to routinely auditing user access privileges to ensure they remain appropriate.
- IMSD could improve its network security program by routinely performing firewall configuration reviews.
- IMSD has implemented a configuration management process to control changes made to its IT systems, and leverages publically available configuration baseline standards as a guideline to securely configure its servers. However, IMSD has not formally documented deviations/exceptions to these public standards, and does not perform routine configuration audits to ensure that servers are actually in compliance with approved baseline standards.
- IMSD's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. IMSD has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.
- IMSD has implemented multiple controls surrounding the input, processing, and output of sensitive data related to the background investigations it performs for OPM. However, when making changes to applications, the person responsible for migrating changes into the production environment also has access to the development and test environments. This situation constitutes a segregation of duties violation.

ABBREVIATIONS

CACI	**CACI International, Inc.**
FIPS	**Federal Information Processing Standards**
FIS	**Federal Investigative Services**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Management Act**
IMSD	**Investigation and Managements Service Division**
IT	**Information Technology**
iTRAX	**Investigations, Tracking, Assigning and Expediting**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PII	**Personally Identifiable Information**
POA&M	**Plan of Action and Milestones**
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 CACI International, Inc. (CACI).

CACI is a contractor that conducts business with a variety of government agencies. The Investigation and Managements Service Division (IMSD) within CACI supports 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. This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over CACI and IMSD's information systems used to process background investigations on behalf of OPM.

This was our first audit of IMSD's organization-wide IT general and application controls. We performed an audit of the IT security controls specific to one of IMSD's applications in fiscal year 2014 (Report number 4A-IS-00-14-017). All recommendations from that audit are closed. We discussed the results of our audit with OPM and CACI representatives at an exit conference.

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 CACI's IT environment. We accomplished these objectives by reviewing the following areas:

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

Scope and Methodology

The scope of this audit centered on the information systems used by CACI's IMSD to process and/or store OPM data. IMSD's network environment is physically and logically segregated from the CACI corporate network. However, the CACI corporate network provides an additional layer of perimeter security and several additional IT security controls to the IMSD environment. The business processes reviewed are primarily located in Chantilly, Virginia.

The on-site portion of this audit was performed from September through December, 2015. We completed additional audit work before and after the on-site visit 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 CACI as of December 2015.

In conducting our audit, we relied to varying degrees on computer-generated data provided by CACI. 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.

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 CACI and IMSD'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 CACI and IMSD'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.

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed CACI and IMSD's business structure and environment;
- Performed a risk assessment of CACI'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 CACI's control structure. These criteria include, but are not limited to, the following publications:

- OPM Information Security and Privacy Policy Handbook;
- U.S. 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;
- FISCAM;
- 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 the Risk 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 CACI's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, CACI was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

CACI and IMSD maintain a series of thorough IT security policies and procedures.

The security management component of this audit involved the examination of the policies and procedures that are the foundation of CACI's overall IT security program.

As mentioned above, the IMSD unit within CACI is the organization's primary user of OPM data. CACI has implemented a security management program and has created IT security policies and procedures that apply specifically to IMSD. However, IMSD is also contractually obligated to adhere to all OPM policies and federal regulations that deviate from CACI's corporate policies or procedures.

We also analyzed CACI's enterprise and technical risk assessments as well as its security training program. Furthermore, we examined human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that CACI and IMSD do not have an adequate security management program.

B. Access Controls

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

We examined the physical access controls of IMSD's facilities and data center located in Chantilly, Virginia. We also examined the logical access controls protecting data in IMSD's network environment and applications.

The access controls observed during this audit include, but are not limited to:

- Procedures for appropriately granting physical access to facilities and data centers;
- Procedures for appropriately granting and adjusting logical access;
- Controls for monitoring user activity;
- Procedures for routinely auditing user facility access; and
- Adequate environmental controls over the data center.

The following sections document opportunities for improvement related to IMSD's access controls:

1) Removal of System Access

IMSD has a system access review process to ensure that former employees do not retain access after termination of their employment. To test the effectiveness of this process, we compared a list of employees with active access to IMSD systems to a list of employees that were terminated in the prior two years. We identified several terminated employees whose accounts remained active in IMSD systems.

NIST SP 800-53, Revision 4, requires that organizations create, enable, modify, disable, and remove information system accounts. NIST 800-53, Revision 4, also states that, "Conditions for disabling or deactivating accounts include … when individuals are transferred or terminated."

Failure to remove logical access from terminated employees in a timely fashion increases the risk that the information systems could be accessed by unauthorized users.

In response to our test work, IMSD created a new procedure document that outlines steps to routinely review logical access accounts for the IMSD domain, the Investigations, Tracking, Assigning and Expediting (iTRAX) system application, and non-system resources to ensure proper account removal. While the new procedure document appears adequate, we would like to see evidence that the process has been successfully implemented.

Recommendation 1

We recommend that FIS ensure that IMSD fully implements its new logical access review procedure.

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

"We concur. Following the OIG audit, CACI-IMSD has fully implemented auditing policies for access control which include the new logical access review procedure. CACI-IMSD has provided FIS with an audit report from January and February 2016 as evidence to support closure of this finding. FIS will provide OPM Internal Oversight and Compliance (IOC) a copy of the report to officially close the finding."

2) Review of User Accounts

iTRAX is the primary application used to support the IMSD management team in monitoring the status of background applications. The system contains multiple user groups each with specific access to different types of information. However, IMSD does not have a process in

place to routinely review each user's system privileges to ensure they are appropriate for a user's job function.

NIST SP 800-53, Revision 4, states that, "Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions." NIST SP 800-53, Revision 4, also requires the organization to identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs.

Failure to review the appropriateness of iTRAX user access privileges increases the risk that a user could access sensitive or unnecessary information.

Recommendation 2

We recommend that FIS require IMSD implement a routine access review process to ensure that iTRAX user access privileges are appropriate for the user's job function.

OCIO/FIS/IMSD Response:

"We concur. CACI-IMSD has an existing process in place where proposed user access privilege changes are reviewed and approved by a Functional Area Manager responsible for employee oversight. CACI-IMSD is planning to further formalize this process in coordination with both the iTRAX Development Team Lead and Functional Area Managers. Planned implementation will be a Functional Role Change Committee which will meet once per month to review all functional user access privilege changes proposed during the previous month across the entire program."

OIG Comment:

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

C. Network Security

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

We evaluated IMSD's network security program and reviewed the results of several automated vulnerability scans performed during this audit. The network security controls observed during this audit include, but are not limited to:

- Network monitoring and incident response procedures;
- Strong remote access controls; and
- Endpoint device controls over investigator laptops.

However, we noted one opportunity for improvement related to IMSD's network security controls.

IMSD has documented the approved communication requirements between all internal and external systems, and these requirements are used to design the firewall rules that control traffic at the network border. IMSD monitors its firewall logs for suspicious activity, such as attempts to make unauthorized changes to the device. Although these are good controls, IMSD could further improve its management of firewalls by performing a periodic review of the actual/current firewall rulesets and comparing them to the previously approved requirements.

NIST SP 800-53, Revision 4, states that an organization should monitor and control changes to configuration settings. NIST SP 800-41 states that policy rules "should also be reviewed periodically to ensure they remain in compliance with security policy."

Failure to review firewall security policy rules could allow an insecure configuration to go undetected, potentially exposing the network to unmanaged risk.

Recommendation 3

We recommend that FIS ensure that IMSD conduct a periodic review of the configuration rulesets for all firewalls and verify that they are in compliance with the approved requirements.

OCIO/FIS/IMSD Response:

"We concur. CACI-IMSD has delivered to FIS an updated policy for Firewall auditing to support closure of this finding. This policy includes the periodic review of configuration rulesets for all firewalls and verification of compliance with approved requirements. FIS will provide OPM-IOC a copy of this policy to officially close the finding."

D. Configuration Management

Configuration management consists of the policies and procedures used to ensure systems are configured according to approved, risk-based, configuration controls.

IMSD's server environment is composed of iTRAX and several other support applications that run on [redacted] operating systems. These systems are running in an isolated virtual server environment within IMSD's network. IMSD also utilizes [redacted] laptop computers for field investigators accessing resources remotely.

We reviewed IMSD's configuration management program and observed the following controls in place:

- Use of standard configuration baselines for [redacted] operating systems, and
- Thorough change management controls.

However, we did identify the following opportunities for improvement:

1) Configuration Baselines

IMSD uses the United States Government Configuration Baseline and Defense Information Systems Agency Security Technical Implementation Guide standards to create security configuration baselines for its operating systems. As is typical with many organizations, IMSD has business needs that require specific settings to deviate from these standards. However, IMSD has not formally documented these exceptions to the standards.

NIST SP 800-53, Revision 4, states that organizations must identify, document, and approve any deviations from established configuration settings based on operational requirements.

Failure to adequately document configuration settings could lead to inconsistently applied security configurations.

Recommendation 4

We recommend that FIS ensure that IMSD document all approved exceptions to the published standards used for system configuration.

OCIO/FIS/IMSD Response:

"We concur. CACI-IMSD will add DISA STIG compliance monitoring to the CACI-IMSD group of server assets. Following the OIG audit, CACI-IMSD has obtained an SCAP tool suite and has completed an initial compliance assessment of their servers. CACI-IMSD is now in the process of configuring the servers to STIG standards and formally documenting any deviations that may be required. CACI-IMSD will complete this process by May 31, 2016 at which time they will deliver the list of any requested deviations to FIS for review and or approval."

2) Configuration Monitoring

The servers in IMSD's environment are monitored for configuration changes through log and event management software. However, the servers are not audited on a routine basis to ensure that they are in compliance with formally approved baseline standards.

IMSD does not routinely audit its servers to ensure they are in compliance with approved baselines.

NIST SP 800-53, Revision 4, states that an organization should monitor and control changes to configuration settings.

NIST SP 800-128 states that security configuration monitoring may be supported by numerous means, including "Scanning to identify disparities between the approved baseline configuration and the actual configuration for an information system." NIST SP 800-128 also states that "If an information system is inconsistent with approved configurations as defined by the organization's baseline configurations … the organization may be unaware of potential vulnerabilities and not take actions that would otherwise limit those vulnerabilities and protect it from attacks."

Failure to identify unknown vulnerabilities could lead to system compromise and the loss of sensitive data.

Recommendation 5

We recommend that FIS ensure that IMSD implements a process to audit systems for compliance with approved baseline configuration settings.

OCIO/FIS/IMSD Response:

"We concur. CACI-IMSD will add the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance component to its existing United States Government Configuration Baseline (USGCB) compliance auditing policy, leveraging the Security content Automation Protocol (SCAP) tool suite they have recently acquired."

3) Patch Management

We performed several automated vulnerability scans and configuration compliance audits as part of our test work. Our vulnerability scans identified several systems with out of date software. We provided scan results to IMSD and they informed us that they were already

aware of the issue and are implementing a new tool to more effectively manage the patch management process for system and third-party software. We believe that IMSD's solution will address the issues we identified in our scans, but we had initial concerns that there was not a formal Plan of Action and Milestones (POA&M) to track this weakness and the associated remediation efforts. At the conclusion of our field work, IMSD provided evidence that a POA&M has been created; no further action is required.

E. Contingency Planning

We reviewed the following elements of IMSD's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disastrous events occur:

- Disaster recovery plan
- Business continuity plan
- Disaster recovery plan tests
- Emergency response procedures

IMSD has documented contingency plans that are tested regularly.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1. IMSD has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that IMSD has not implemented adequate controls related to contingency planning.

F. Application Controls

1) Investigative Case Management Process

We reviewed the applications and business processes supporting CACI's efforts to perform background investigations on behalf of OPM. IMSD performs basic work assignment and scheduling tasks through the iTRAX system. IMSD has designed its entire investigative case management process in a manner that does not require it to extract or store personally identifiable information (PII) related to background investigations from OPM systems. We evaluated the input, processing, and output controls associated with IMSD's case management process. We determined that IMSD has implemented policies and procedures to help ensure that:

- Case tracking data contains minimal PII and is handled securely;
- Sensitive case information is transmitted only through secure connections; and

- Case material is tracked and disposed of in a secure manner.

Nothing came to our attention to indicate that IMSD has not implemented adequate controls over its case processing systems.

2) Application Change Control

We evaluated the policies and procedures governing application development and change control of IMSD's case processing systems.

IMSD has documented system development life cycle procedures for software modifications. All changes require formal approval and undergo testing prior to migration to the production environment. However, the person responsible for migrating changes into the production environment also has access to the development and test environments. This situation constitutes a segregation of duties violation.

NIST SP 800-53, Revision 4, states that the organization should document the separation of duties of individuals, and define information system access authorizations to support separation of duties. NIST SP 800-53, Revision 4, also states that "Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion."

Failure to ensure proper separation of duties between development, test, and production environments increases the risk that unauthorized changes could be made to the system.

Recommendation 6

We recommend that FIS ensure that IMSD implements proper segregation of duties within the application change control process.

OCIO/FIS/IMSD Response:

"We concur. CACI-IMSD is in the process of restructuring its system development team and creating a new 'Release Manager' position which will have no access to change any Development/Test system code, and will only have authorization to update production system code. As part of this transition, CACI-IMSD is creating a new policy which will document the user role control processes and how separation of duties will be achieved."

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], IT Auditor
[redacted], IT Auditor
[redacted], IT Auditor

[redacted], Senior Team Leader
[redacted], Group Chief

V. APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

April 21, 2016

MEMORANDUM FOR NORBERT E. VINT
Acting Inspector General
Office of the Inspector General

THRU: [redacted]
Lead IT Auditor-in-Charge
Office of the Inspector General

FROM: LISA SCHLOSSER
Acting Chief Information Officer
Office of the Chief Information Officer

MERTON W. MILLER
Associate Director
Federal Investigative Services

SUBJECT: Draft Audit Report of Information Systems General Application Controls at CACI International, Inc. Report Number: 6A-0A-00-16-004

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 CACI International, Inc. 6A-0A-00-16-004.

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. The Federal Investigative Services (FIS), Office of the Chief Information Officer (OCIO) and the CACI Investigations and Management Service Division (IMSD) collective responses to your recommendations follow.

OIG Recommendation #1: "We recommend that FIS ensure that IMSD fully implements its new logical access review procedure."

FIS/OCIO/IMSD Response:

We concur. Following the OIG audit, CACI-IMSD has fully implemented auditing policies for access control which include the new logical access review procedure. CACI-IMSD has provided FIS with an audit report from January and February 2016 as evidence to support closure of this finding. FIS will provide OPM Internal Oversight and Compliance (IOC) a copy of the report to officially close the finding.

OIG Recommendation #2: "We recommend that FIS ensure that IMSD implement a routine access review process to ensure that iTRAX user access privileges are appropriate for the user's job function."

FIS/OCIO/IMSD Response:

We concur. CACI-IMSD has an existing process in place where proposed user access privilege changes are reviewed and approved by a Functional Area Manager responsible for employee oversight. CACI-IMSD is planning to further formalize this process in coordination with both the iTRAX Development Team Lead and Functional Area Managers. Planned implementation will be a Functional Role Change Committee which will meet once per month to review all functional user access privilege changes proposed during the previous month across the entire program.

OIG Recommendation #3: "We recommend that FIS ensure that IMSD conduct a periodic review of the configuration rulesets for all firewalls and verify that they are in compliance with the approved requirements."

FIS/OCIO/IMSD Response:

We concur. CACI-IMSD has delivered to FIS an updated policy for Firewall auditing to support closure of this finding. This policy includes the periodic review of configuration rulesets for all firewalls and verification of compliance with approved requirements. FIS will provide OPM-IOC a copy of this policy to officially close the finding.

OIG Recommendation #4: "We recommend that FIS ensure that IMSD document all approved exceptions to the published standards used for system configuration."

FIS/OCIO/IMSD Response:

We concur. CACI-IMSD will add DISA STIG compliance monitoring to the CACI-IMSD group of server assets. Following the OIG audit, CACI-IMSD has obtained an SCAP tool suite and has completed an initial compliance assessment of their servers. CACI-IMSD is now in the process of configuring the servers to STIG standards and formally documenting any deviations that may be required. CACI-IMSD will complete this process by May 31, 2016 at which time they will deliver the list of any requested deviations to FIS for review and or approval.

OIG Recommendation #5: "We recommend that FIS ensure that IMSD implements a process to audit systems for compliance with approved baseline configuration settings."

FIS/OCIO/ISMD Response:

We concur. CACI-IMSD will add the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance component to its existing United States Government Configuration Baseline (USGCB) compliance auditing policy, leveraging the Security content Automation Protocol (SCAP) tool suite they have recently acquired.

Recommendation #6: "We recommend that FIS ensure that IMSD implements proper segregation of duties within the application change control process."

FIS/OCIO/ISMD Response:

We concur. CACI-IMSD is in the process of restructuring its system development team and creating a new "Release Manager" position which will have no access to change any Development/Test system code, and will only have authorization to update production system code. As part of this transition, CACI-IMSD is creating a new policy which will document the user role control processes and how separation of duties will be achieved.

We appreciate the opportunity to respond to this draft report. We believe all recommendations to be requirements within scope of the existing contract between OPM and CACI-IMSD. We will solicit support from the OPM Office of Procurement Operations (OPO) as necessary. If you have any questions regarding our response, please contact [redacted], [redacted], [redacted]@opm.gov OR [redacted], [redacted], [redacted]@opm.gov.

cc: Kathy McGettigan
Chief Management Officer

[redacted]
Chief Information Security Officer

Janet Barnes
Director, Internal Oversight and Compliance

Nina Ferraro
Senior Procurement Executive

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