

**Information Technology
Management Letter for
the Federal Emergency
Management Agency
Component of the FY 2016
Department of Homeland
Security Financial
Statement Audit**





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2016 Department of Homeland Security Financial Statement Audit

June 8, 2017

Why We Did This Audit

Each year, our independent auditors identify component-level information technology (IT) control deficiencies as part of the DHS consolidated financial statement audit. This letter provides details that were not included in the fiscal year (FY) 2016 DHS Agency Financial Report.

What We Recommend

We recommend that FEMA, in coordination with the DHS Chief Information Officer and Acting Chief Financial Officer, make improvements to FEMA's financial management systems and associated IT security program.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

We contracted with the independent public accounting firm KPMG, LLP to perform the audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS) for the year ended September 30, 2016. KPMG evaluated selected general IT controls (GITC), IT entity-level controls, and business process application controls at the Federal Emergency Management Agency (FEMA). KPMG determined that FEMA took corrective action to address certain prior-year IT control deficiencies. For example, FEMA made improvements by implementing certain account and configuration management controls. However, KPMG continued to identify GITC deficiencies related to security management, access controls, configuration management, and contingency planning for FEMA's core financial and feeder systems.

The deficiencies collectively limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability. In addition, certain of these deficiencies adversely impacted internal controls over DHS' financial reporting and its operation and therefore are considered to collectively represent a material weakness reported in the FY 2016 DHS Agency Financial Report.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

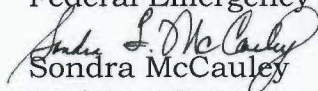
Washington, DC 20528 / www.oig.dhs.gov

June 8, 2017

MEMORANDUM FOR: Adrian R. Gardner
Chief Information Officer
Federal Emergency Management Agency

Thomas Lowry
Chief Financial Officer
Federal Emergency Management Agency

FROM:


Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Federal
Emergency Management Agency Component of the FY 2016
Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2016 Department of Homeland Security Financial Statement Audit*. This report contains comments and recommendations related to information technology internal control deficiencies. The observations did not meet the criteria to be reported in the *Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting*, dated November 14, 2016, which was included in the FY 2016 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2016 financial statements and is responsible for the attached information technology management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control, nor do we provide conclusions on compliance with laws and regulations. We will post the final report on our website.

Please call me with any questions, or your staff may contact Kevin Burke, Acting Director, Information Systems and Acquisitions Division, at (202) 254-5450.

Attachment

www.oig.dhs.gov

OIG-17-64



KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

December 15, 2016

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
Federal Emergency Management Agency,
Washington, DC

Ladies and Gentlemen:

We planned and performed our audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department), as of, and for the year ended, September 30, 2016, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*. We considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the consolidated financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

During our audit we noted certain matters involving internal control and other operational matters at the Federal Emergency Management Agency (FEMA), a component of DHS, which are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies.

We also noted certain internal control deficiencies at FEMA during our audit that, in aggregate and when combined with certain internal control deficiencies identified at certain other DHS components, contributed to a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. Specifically, with respect to financial systems at FEMA, we noted certain matters in the general IT control areas of security management, access controls, configuration management, and contingency planning. These matters are described in the *Findings and Recommendations* section of this letter.

Additionally, at the request of the DHS Office of Inspector General (OIG), we performed additional non-technical information security procedures to identify instances in which FEMA personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These matters are described in the *Observations Related to Non-Technical Information Security* section of this letter.

We have provided a description of key FEMA financial systems and IT infrastructure within the scope of the Fiscal Year (FY) FY 2016 DHS financial statement audit in Appendix A, and a listing of each FEMA IT Notice of Finding and Recommendation communicated to management during our audit in Appendix B.

During our audit we noted certain matters involving financial reporting internal controls (comments not related to IT) and other operational matters at FEMA, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and



U.S. Department of Homeland Security
Federal Emergency Management Agency
December 15, 2016
Page 2 of 2

those charged with governance in our *Independent Auditors' Report* and in a separate letter to the OIG and the FEMA Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form opinions on the FY 2016 DHS consolidated financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of FEMA's organization gained during our work to make comments and suggestions that we hope will be useful.

We would be pleased to discuss these comments and recommendations with you at any time.

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	5
Findings and Recommendations	7
Findings	7
Recommendations	8
Observations Related to Non-Technical Information Security	10

APPENDICES

Appendix	Subject	Page
A	Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2016 DHS Financial Statement Audit	11
B	FY 2016 IT Notices of Findings and Recommendations at FEMA	17

OBJECTIVE, SCOPE, AND APPROACH

Objective

We audited the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2016, (referred to herein as the “fiscal year (FY) 2016 financial statements”). In connection with our audit of the FY 2016 DHS consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITC), IT entity-level controls (ELC), and IT application controls at the Federal Emergency Management Agency (FEMA), a component of DHS, to assist in planning and performing our audit engagement. At the request of the DHS Office of Inspector General (OIG), we also performed additional information security testing procedures to assess certain non-technical areas related to the protection of sensitive IT and financial information and assets.

Scope and Approach

General Information Technology Controls and IT Entity-Level Controls

The U.S. Government Accountability Office (GAO) issued the *Federal Information System Controls Audit Manual* (FISCAM), which formed the basis for our GITC and IT ELC evaluation procedures.

FISCAM was designed to inform financial statement auditors about IT controls and related audit concerns, to assist them in planning their audit work, and to integrate the work of auditors with other aspects of the financial statement audit. It also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs, IT ELCs, and the IT environment of a Federal agency. FISCAM defines the following five control categories to be essential to the effective operation of GITCs, IT ELCs, and the IT environment:

1. *Security Management* – controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
2. *Access Control* – controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
3. *Configuration Management* – controls that help prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.
4. *Segregation of Duties* – controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

5. *Contingency Planning* – controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

Although each of these FISCAM categories was considered during the planning and risk assessment phase of our audit, we selected GITCs and IT ELCs for evaluation based on their relationship to the ongoing effectiveness of process-level automated controls or manual controls with one or more automated components. This includes those controls that depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2016 GITC and IT ELC procedures at FEMA did not necessarily represent controls from each FISCAM category.

Business Process Application Controls

Where relevant GITCs were operating effectively, we tested selected IT application controls (process-level controls — fully automated or manual with an automated component) on financial systems and applications to assess internal controls over input, processing, and output of financial data and transactions.

FISCAM defines Business Process Application Controls (BPAC) as the automated and/or manual controls applied to business transaction flows, and related to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. BPACs typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes.

Financial System Functionality

In recent years, we have noted that limitations in FEMA's financial systems' functionality may be inhibiting the agency's ability to implement and maintain internal controls, including effective GITCs, IT ELCs, and IT application controls supporting financial data processing and reporting. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Therefore, in FY 2016, we continued to evaluate and consider the impact of financial systems functionality on internal control over financial reporting.

Non-Technical Information Security Testing

To complement our IT controls test work, we conducted limited after-hours physical security testing at selected FEMA facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to FEMA personnel awareness of policies, procedures, and other requirements governing the protection of sensitive IT and financial information and assets from unauthorized access or disclosure. This testing was performed in accordance with the FY 2016 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG LLP, DHS OIG, and DHS management.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

Appendix A provides a description of the key FEMA financial systems and IT infrastructure within the scope of the FY 2016 DHS financial statement audit.

SUMMARY OF FINDINGS

During our FY 2016 assessment of GITCs, IT ELCs, and IT application controls, we noted that FEMA took corrective action to address certain prior year IT control deficiencies. For example, FEMA made improvements over designing and consistently implementing certain account management and configuration management controls. However, we continued to identify GITC deficiencies related to controls over security management, access controls, configuration management, and contingency planning for FEMA core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses over new systems and new testing approaches in scope for FY 2016 that were remediated or historically effective in other system environments.

The conditions supporting our findings collectively limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability. In addition, certain of these deficiencies at FEMA adversely impacted the internal controls over DHS' financial reporting and its operation and we consider them to collectively contribute to a Department-wide material weakness regarding IT controls and financial system functionality for DHS, under standards established by the American Institute of Certified Public Accountants and the U.S. GAO.

Of the 16 IT Notices of Findings and Recommendations (NFR) issued during our FY 2016 testing at FEMA, 10 were repeat findings, either partially or in whole from the prior year, and 6 were new findings. The 16 IT NFRs issued represent deficiencies and observations related to three of the five FISCAM GITC categories.

The majority of the deficiencies that our audit identified were related to noncompliance with financial system controls. According to DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, National Institute of Standards and Technology guidance, and FEMA policies, financial system controls lacked proper documentation, were not fully designed and implemented, were inadequately detailed, and were inconsistently implemented. The most significant weaknesses from a financial statement audit perspective continued to include:

1. unauthorized or inadequately monitored access to, and activity within, system components for key FEMA financial applications; and
2. configuration management controls that were not adequately designed, fully implemented, or operating effectively.

During our IT audit procedures, we also evaluated and considered the impact of financial system functionality on financial reporting. In recent years, we have noted that limitations in FEMA's financial systems' functionality may be inhibiting FEMA's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data. Many key financial and feeder systems have not been substantially updated since being

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

inherited from legacy agencies several years ago. Many key FEMA financial systems were not compliant with Federal financial management system requirements as defined by the *Federal Financial Management Improvement Act of 1996* (FFMIA) and Office of Management and Budget Circular Number A-123 Appendix D, *Compliance with FFMIA*.

Although the recommendations made by us should be considered by FEMA, it is ultimately the responsibility of FEMA management to determine the most appropriate method(s) for addressing the deficiencies identified.

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2016 DHS consolidated financial statements, we identified the following GITC and IT ELC deficiencies at FEMA, certain of which, in the aggregate, contribute to the IT material weakness at the Department level:

Security Management

- Individuals with significant information security oversight and management responsibilities subject to role-based training did not complete their role-based training requirements as required by policy.
- Plans of Action and Milestones (POA&M) were non-compliant with DHS policy, including insufficient review by management, no planned and completed milestones, planned corrective actions that lacked detail, expected completion dates that were not achievable within the timeline provided, cancellation of POA&Ms despite remediation efforts that were still in progress, and POA&Ms that were not documented for known weaknesses.

Access Controls

- Policies and procedures for managing and monitoring FEMA personnel access to financial applications owned and operated on behalf of FEMA by third-party service organizations were not consistently or completely developed and formally documented. Furthermore, supporting authorization was not provided or was not properly documented.
- Requirements for generating audit logs with the detail required to review application-level auditable events had not been implemented for multiple financial systems.
- Documentation providing linkages between access permissions and each financial application environment was not developed.
- Strong password requirements were not consistently enforced on databases supporting financial applications.
- Privileged users on servers supporting key financial applications lacked documented supervisor approval, were not uniquely identified and shared user IDs, and utilized shared passwords.
- User access to applications was not timely removed upon user separation from FEMA.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

Configuration Management

- Certain configuration-related deficiencies identified on servers, workstations, and system software were not remediated timely or tracked appropriately for remediation within management's POA&M.

Contingency Planning

- Alternate processing sites for financial systems were not established. Consequently, testing of those systems' contingency plans, including restoration to an established alternate processing site, was not performed.

Recommendations

We recommend that the FEMA Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO), in coordination with the DHS OCIO and OCFO, make the following improvements to FEMA's financial management systems and associated IT security program (in accordance with FEMA and DHS requirements, as applicable).

Security Management

- Notify individuals with significant information security responsibilities that they must complete required training and ensure managers verify that training has been completed.
- Document, prepare, and review POA&Ms in accordance with DHS requirements and provide training to those individuals in charge of POA&Ms.

Access Controls

- Develop and fully implement policies and procedures to manage FEMA personnel access, including initial authorization and ongoing recertification of access, to financial applications owned and operated on behalf of FEMA by third-party service organizations.
- Create, update, and review access approval forms to ensure that system authorization is properly documented.
- Modernize key financial systems to ensure application-level auditable events are captured and review application, operating system, and database audit logs within an enterprise-wide audit logging solution.
- Modernize key financial systems to ensure application-level identity management controls are implemented in accordance with DHS policy.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

- Implement technical controls to ensure that passwords for financial databases accounts are configured in accordance with FEMA guidance, DHS requirements, and Defense Information Systems Agency (DISA) (Security Technical Implementation Guides (STIGs).
- Review and approve privileged accounts in accordance with FEMA policies and procedures, and ensure unique accounts are created.
- Formally document and approve a business justification if shared accounts must be used, and document and implement compensating controls to address the risk associated with these accounts.
- Review and develop compensating controls to ensure separated user access is removed in a timely manner.

Configuration Management

- Ensure vulnerabilities identified are reviewed and remediated in accordance with requirements specified in DHS and FEMA policy, and determine if waivers should be requested from DHS OCIO if vulnerabilities cannot be remediated due to existing system infrastructure and software versions.

Contingency Planning

- Allocate resources needed to fully design, develop, and implement management's planned approach to identify and implement an alternate processing site, and conduct and document the results of contingency planning tests and exercises.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2016 audit, we performed additional non-technical information security procedures at FEMA. These procedures included after-hours physical security walkthroughs to identify instances in which FEMA personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These procedures were performed in accordance with the FY 2016 *Security Testing Authorization Letter* (STAL) signed by DHS OIG management, KPMG management, and DHS management.

After-Hours Physical Security Walkthroughs

Multiple DHS policies, including the DHS Sensitive Systems Policy Directive 4300A, the DHS Privacy Office *Handbook for Safeguarding Sensitive Personally-Identifiable Information (PII)*, and DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive but Unclassified (SBU) (FOUO) Information*, mandate the physical safeguarding of certain materials and assets that, if compromised either due to external or insider threat, could result in unauthorized access, disclosure, or exploitation of sensitive IT or financial information.

We performed procedures to determine whether FEMA personnel consistently exercised responsibilities related to safeguarding sensitive materials as defined in these policies. Specifically, we performed escorted walkthroughs of workspaces – including cubicles, offices, shared workspaces, and/or common areas (e.g., areas where printers were hosted) – at FEMA facilities that processed, maintained, and/or had access to financial data during FY 2016. We inspected workspaces to identify instances where materials designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from FEMA, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at FEMA, we inspected a total of 251 workspaces. Of those, 33 were observed to have material – including, but not limited to, system passwords; information marked “FOUO” or otherwise meeting the criteria established by DHS MD 11042.1; documents containing sensitive PII; and government-issued laptops, mobile devices, or storage media – left unattended and unsecured after business hours in violation of DHS policy.

The selection of inspected areas was not statistically derived; therefore, the results described here should not be used to extrapolate to FEMA as a whole.

Appendix A

Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2016 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

Below is a description of the significant FEMA financial management systems and supporting IT infrastructure included in the scope of the FY 2016 DHS financial statement audit.

Federal Emergency Management Agency (FEMA)

Web Integrated Financial Management Information System (WebIFMIS)

WebIFMIS is a web-based major application and the official accounting system of record for FEMA. It maintains and is the source of all financial data for both internal and external financial reporting. It comprises five subsystems (Funding, Cost Posting, Disbursements, Accounts Receivable, and General Ledger) that budget, record, and track all financial transactions, manage vendor accounts, and process approved payments to grantees, FEMA employees, contractors, and other vendors.

WebIFMIS contains interfaces with internal FEMA feeder systems and external service providers, including the Department of Treasury's Bureau of the Fiscal Service, the U.S. Department of Agriculture's (USDA) National Finance Center (NFC), and the Department of Health and Human Services' (HHS) Grants Management System.

WebIFMIS is a commercial off-the-shelf (COTS) software package that Digital Systems Group, Inc. developed and maintains. FEMA's OCFO and OCIO host and support the application exclusively for the internal OCFO user community.

An Oracle database with Linux servers supports WebIFMIS, and the system resides in Mt. Weather, VA.

Payment and Reporting System (PARS)

PARS is a web-based major application that includes a public-facing component that collects quarterly Standard Form (SF) 425 (Federal Financial Report) submissions and payment requests from grantees. Through daily automated scheduled jobs, grant and obligation information is updated via an interface between PARS and WebIFMIS. An internal component (OCFO) provides FEMA staff with the ability to view SF 425 submissions, examine grantee payment history reports, and add or remove holds on grantee payments.

FEMA OCFO hosts and supports PARS externally for grantees and internally for the OCFO user community.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

An Oracle database with HP-UX servers supports PARS, and the system resides in Mt. Weather, VA.

Non-Disaster Grant Management System (NDGrants)

NDGrants is a web-based major application intended to provide FEMA and its stakeholders with a system that supports the grants management lifecycle. FEMA provides state and local governments with preparedness program funding in the form of Non-Disaster Grants to enhance the capacity of state and local emergency responders to prevent, respond to, and recover from weapons of mass destruction; terrorism incidents involving chemical, biological, radiological, nuclear, and explosive devices; and cyber-attacks.

NDGrants includes a public-facing component that permits external grantees and stakeholders to apply for grants, monitor the progress of grant applications and payments, and view related reports. NDGrants also has an internal component that the FEMA Grants Program Directorate (GPD), Program Support Division (PSD) uses to review, approve, and process grant awards. NDGrants interfaces with the HHS Grants.gov system to facilitate upload and integration of information submitted via SF 424 (Application for Federal Assistance).

FEMA's GPD and OCIO host and support NDGrants externally for grantees and stakeholders, and internally for the GPD user community.

An Oracle database with Linux servers supports NDGrants, and the system resides in Mt. Weather, VA.

Assistance to Firefighters Grants (AFG)

AFG is a web-based major application developed to assist the United States Fire Administration (USFA) division of FEMA in managing the AFG program. The primary goal of AFG is to meet the firefighting and emergency response needs of fire departments, first responders, and nonaffiliated emergency medical service organizations to obtain equipment, protective gear, emergency vehicles, training, and other resources to protect the public and emergency personnel from fire and related hazards.

AFG includes a public-facing component that permits external grantees and stakeholders to apply for grants and submit payments and reports, and an internal component used by the GPD PSD and the AFG Program Office to review, approve, and process grant awards.

FEMA GPD and FEMA OCIO host and support AFG externally for grantees and stakeholders, and internally for the GPD user community.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

An Oracle database with Linux servers supports AFG, and the system resides in Mt. Weather, VA.

Emergency Management Mission Integrated Environment (EMMIE)

EMMIE is a web-based major application used by FEMA program offices and user communities directly involved in the grant lifecycles associated with the Public Assistance grant program. These include Fire Management Assistance grants to State, Tribal, and local governments, and certain types of private nonprofit organizations so that communities can quickly respond to and recover from major disasters or emergencies declared by the President.

EMMIE includes a public-facing component that permits external grantees and stakeholders to apply for grants, and an internal component that different communities use when processing grants from solicitation to closeout, and assisting with coordination between the respective program and grants management offices and the Office of Legislative Affairs. The system also contains an interface with the Environmental and Historic Preservation Management Information System (EMIS) to automate the process of reviewing and documenting FEMA-funded projects for environmental and historic preservation (EHP) compliance.

FEMA's Public Assistance Division (PAD) and OCIO host and support EMMIE externally for grantees and stakeholders, and internally for the FEMA user community.

An Oracle database with Linux servers supports EMMIE, and the system resides in Mt. Weather, VA.

Emergency Support (ES)

ES is a web-based major application that performs front-end financial management for disaster processing, and controls and monitors FEMA's funds and external financial interfaces. As a module of the National Emergency Management Information System (NEMIS), ES pre-processes financial transactions, including allocation, commitment, obligation, mission assignment, and payment requests from other NEMIS modules and other external systems and serves as the primary interface to WebIFMIS. ES supports the Enterprise Coordination and Approvals Processing System (eCAPS), which helps initiate, track, and expedite the process of providing direct aid and technical assistance. This includes electronic coordination and approval of internal requisitions for services, supplies, and mission assignments to other Federal agencies and states in response to Presidentially-declared disasters.

ES includes a public-facing component that authorizes access to applicants for grants or disaster assistance, and to other state, local, and non-governmental organization (NGO) representatives and members of the public. It also includes an internal component that FEMA OCFO uses to process disaster housing payments, perform payment recoupment, and conduct other administrative tasks associated with disaster payments.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

In addition to WebIFMIS and eCAPS, ES contains interfaces with other internal FEMA feeder systems, including EMMIE and AFG.

FEMA's OCFO and OCIO host and support ES externally for grantees and stakeholders, and internally for the OCFO user community.

An Oracle database with Linux servers support ES, and the system resides in Mt. Weather, VA.

Transaction Recording and Reporting Processing (TRRP)

TRRP is a mainframe-based application and a subsystem of the National Flood Insurance Program (NFIP) Information Technology System (ITS) general support system. It collects, maintains, and reports on all data and activity that the Write Your Own (WYO) companies and the Direct Servicing Agent (DSA) for NFIP submit. Additionally, TRRP creates and updates policies, claims, and community master files that are maintained on the NFIP ITS mainframe.

Computer Sciences Corporation (CSC), Inc. hosts and supports TRRP, on behalf of the Federal Insurance & Mitigation Administration, exclusively for the NFIP user community.

A FOCUS database with an IBM z/OS mainframe supports TRRP, and the system resides in Norwich, CT.

Quick Claims

Quick Claims is a web-based application that a Windows operating system and MySQL database support. WYOs use the application to self-report claims data prior to officially submitting that data through TRRP. The NFIP Actuary incorporates September claims data per Quick Claims into its actuarial calculation, as September claims data is not available from TRRP until after financial reporting deadlines for year-end. The system resides in Norwich, CT.

Payment Management System (PMS)

PMS, commonly referred to as Smartlink, is a web-based major application that the HHS National Institutes of Health's (NIH) Center for Information Technology (CIT) Information Systems Branch (ISB) developed, hosts, operates, and maintains. FEMA OCFO's Finance Center user community uses Smartlink to disburse grant funds to grantees, track and maintain grantee payment and expenditure data, and manage cash advances to recipients. An Oracle database with HP-UX servers supports PMS, and the system resides in Bethesda, MD.

Procurement Information System for Management (PRISM)

PRISM is a contract writing system that FEMA acquisition personnel use to create contract awards. PRISM interfaces with the Federal Procurement Data System – Next Generation.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2016

FEMA uses an instance of PRISM, and DHS OCPO owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

An Oracle database with UNIX-based servers support PRISM, and the system resides in Datacenter 1 in Stennis, MS.

Concur Government Edition (CGE)

CGE is a third party application developed by Systems, Applications, and Products (SAP) that supports FEMA in managing travel authorizations and processing travel vouchers in compliance with government travel regulations.

Hazard Mitigation Grant Program (HMGP)

HMGP is the Mitigation module within the National Emergency Management Information System (NEMIS) Access Control System (NACS) that supports FEMA in administering grants to state and local governments to implement long-term hazard mitigation measures after a major disaster declaration. Section 404 of the Stafford Act authorizes the program and FEMA administers it. HMGP was created to reduce the loss of life and property due to natural disasters. The system resides in Mt. Weather, VA.

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application that USDA NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. FEMA's Office of the Chief Component Human Capital Officer (OCCHCO) utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the FEMA user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application that NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. DHS components use NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

Appendix B
FY 2016 IT Notices of Findings and Recommendations at
FEMA

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-16-01	Non-Compliance with Alternate Processing Site Requirements for Key Financial Systems	Contingency Planning		X
FEMA-IT-16-02	Insufficient Audit Log Controls for Key Financial Systems	Access Controls		X
FEMA-IT-16-03	Network Access Control Systems (NACS) Account Management Weakness	Access Controls		X
FEMA-IT-16-04	Non-Compliance with Baseline Configuration Guidance for Oracle Database User Account Passwords	Access Controls		X
FEMA-IT-16-05	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management		X
FEMA-IT-16-06	Weaknesses within Web Time and Attendance (WebTA) Account Management Policies and Procedures	Access Controls		X
FEMA-IT-16-07	Inconsistent Implementation of EmpowHR Account Management Controls	Access Controls		X
FEMA-IT-16-08	Weaknesses with CGE Account Management Controls	Access Controls	X	
FEMA-IT-16-09	Non-Compliance with DHS Policy for Elevated Privileged (EP) Server Access	Access Controls and Configuration Management	X	
FEMA-IT-16-10	Inconsistent Authorization of Privileged Access for Systems Managed by OCIO IT Operations	Access Controls	X	
FEMA-IT-16-11	Weaknesses with Monitoring and Enforcing Role-Based Training for Individuals with Significant Information Security Responsibilities	Security Management		X

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-16-12	Non-Compliant Plan of Action and Milestone (POA&M) Reporting for Key Financial Systems	Access Controls		X
FEMA-IT-16-13	Weaknesses with Implementation of Separated User Access Controls for Key Financial Systems	Access Controls	X	
FEMA-IT-16-14	Weaknesses with PRISM Account Management Policy and Procedures	Access Controls	X	
FEMA-IT-16-15	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted at the Mount Weather Emergency Operations Center (MWEOC)	Access Controls and Configuration Management		X
FEMA-IT-16-16	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted by NFIP ITS	Access Controls and Configuration Management	X	



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Chief Privacy Officer

Management Directorate

Deputy Under Secretary
Acting Chief Financial Officer
Chief Information Officer
Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.



OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305