

Department of Homeland Security **Office of Inspector General**

**Information Technology Management Letter for the
Immigration and Customs Enforcement Component of
the FY 2013 Department of Homeland Security's
Financial Statement Audit**





OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 29, 2014

MEMORANDUM FOR: Thomas P. Michelli
Chief Information Officer
U.S. Immigration and Customs Enforcement

Radha C. Sekar
Chief Financial Officer
U.S. Immigration and Customs Enforcement

FROM: 
Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the
Immigration and Customs Enforcement Component of the
FY 2013 Department of Homeland Security's Financial
Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2013 Department of Homeland Security's Financial Statement Audit*. This report contains comments and recommendations related to information technology internal control deficiencies that were not required to be reported in the Independent Auditors' Report.

We contracted with the independent public accounting firm KPMG LLP (KPMG) to conduct the audit of Department of Homeland Security fiscal year 2013 consolidated financial statements. The contract required that KPMG perform its audit according to generally accepted government auditing standards and guidance from the Office of Management and Budget and the Government Accountability Office. KPMG is responsible for the attached management letter dated March 11, 2014, and the conclusion expressed in it.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Audit Division, at (202) 254-5451.

Attachment



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

March 11, 2014

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement

Ladies and Gentlemen:

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the “fiscal year (FY) 2013 financial statements”), and have issued our report thereon dated December 11, 2013. In planning and performing our audit of the financial statements of DHS, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*, 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 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.

In accordance with *Government Auditing Standards*, our *Independent Auditors’ Report*, dated December 11, 2013, included internal control deficiencies identified during our audit that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. This letter represents the separate limited distribution report mentioned in that report, of matters related to U.S. Immigration and Customs Enforcement (ICE).

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management and communicated through Notices of Findings and Recommendations (NFRs), are intended to improve internal control or result in other operating efficiencies and are summarized as described below.

With respect to ICE’s financial systems’ IT controls, we noted certain matters in the areas of security management, access controls, configuration management, segregation of duties, and contingency planning. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The Table of Contents identifies each section of the letter. We have provided a description of key ICE financial systems and IT infrastructure within the scope of the FY 2013 DHS financial statement audit in Appendix A, and a listing of each IT NFR in Appendix B.



During our audit we noted certain matters involving financial reporting internal controls (comments not related to IT) and other operational matters, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form an opinion on the 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 DHS' organization gained during our work to make comments and suggestions that we hope will be useful to you.

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
U.S. Immigration and Customs Enforcement
September 30, 2013

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	4
General IT Control Findings and Recommendations	5
<i>Findings</i>	5
Security Management	5
Access Controls	5
Configuration Management	5
Segregation of Duties	5
Contingency Planning	6
<i>Recommendations</i>	6
Security Management	6
Access Controls	6
Configuration Management	6
Segregation of Duties	6
Contingency Planning	7
IT Application Controls	7

APPENDICES

Appendix	Subject	Page
A	Description of Key ICE Financial Systems and IT Infrastructure within the Scope of the FY 2013 DHS Financial Statement Audit	8
B	FY 2013 IT Notices of Findings and Recommendations at ICE	10

OBJECTIVE, SCOPE, AND APPROACH

Objective

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the “fiscal year (FY) 2013 financial statements”). In connection with our audit of the FY 2013 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and IT application controls at U.S. Immigration and Customs Enforcement (ICE) to assist in planning and performing our audit engagement.

Scope

The scope of our GITC and IT application control test work is described in Appendix A, which provides a description of the key ICE financial systems and IT infrastructure within the scope of the ICE component of the FY 2013 DHS consolidated financial statement audit.

Approach

General Information Technology Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office, formed the basis of our GITC 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. FISCAM also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs and the IT environment of a Federal agency. FISCAM defines the following five control categories to be essential to the effective operation of GITCs and the IT environment:

- *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.
 - In conjunction with our test work of security management GITCs, limited after-hours physical security testing at select ICE facilities was conducted to identify potential control deficiencies in non-technical aspects of IT security.
- *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
- *Configuration Management* – Controls that help to 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.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2013

- We performed technical information security testing for key ICE network and system devices. The technical security testing was performed from within select DHS facilities and focused on production devices that directly support DHS' and ICE's financial processing and key general support systems.
- *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
- *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

IT Application Controls

We performed testing over selected key IT application controls on financial systems and applications to assess the financial systems' internal controls over the input, processing, and output of financial data and transactions. FISCAM defines application controls as the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS

During FY 2012, ICE took corrective action to address certain prior year IT control deficiencies. For example, ICE made improvements over strengthening controls around logical access and patch and configuration management. However, during FY 2013, we continued to identify GITC deficiencies related to controls over security management (including deficiencies over physical security and security awareness), access controls, configuration management, segregation of duties, and contingency planning for the ICE core financial system and associated General Support System environments.

Collectively, the IT control deficiencies limited ICE's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted ICE's internal controls over financial reporting and its operations. We consider these deficiencies, in aggregate, to contribute to the IT material weakness at the Department level under standards established by the American Institute of Certified Public Accountants. In addition, based upon the results of our test work, we noted that ICE contributes to the Department's non-compliance with the relevant federal financial management systems requirements of the *Federal Financial Management Improvement Act of 1996*.

Of the nine IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, six were repeat findings, either partially or in whole from the prior year, and three were new findings. The nine IT NFRs issued represent deficiencies in all five FISCAM GITC categories.

The majority of findings resulted from the lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, requirements and National Institute of Standards and Technology guidance. Specifically, the findings stem from:

1. Inadequately designed and ineffective access control policies and procedures relating to the management of logical access to financial applications, databases, and support systems;
2. Patch, configuration, and vulnerability management control deficiencies within systems; and
3. Inconsistently documented backup management controls.

These deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and ICE financial data could be exploited, thereby compromising the integrity of ICE financial data used by management and reported in ICE's and DHS' financial statements.

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

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2013 DHS financial statements, we identified the following ICE GITC deficiencies that, in the aggregate, contribute to the IT material weakness at the Department level.

Security Management

After-Hours Physical Security Testing

On July 1, 2013, we performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to printed or electronic media, equipment, or credentials residing within an ICE employee's or contractor's work area or shared workspaces which could be used by others to gain unauthorized access to systems housing financial or other sensitive information. The testing was performed at various ICE locations in the Washington DC metropolitan area that process, maintain, and/or have access to financial data.

We observed 38 instances where passwords, unsecured or unlocked credit cards, laptops, and external media, and printed materials marked "For Official Use Only" or classified or containing sensitive Personally Identifiable Information were accessible by individuals without a "need to know".

Access Controls

- Account management activities for the National Protection and Programs Directorate instance of the Federal Financial Management System (FFMS), including authorization of new or modified application access, were not consistently or timely documented or implemented in accordance with DHS and ICE policy.
- DHS requirements for password complexity were not fully implemented for accounts on the ICE Network (ADEX).
- Exit clearance actions for separated or transferred ICE Federal employees and contractors were not consistently or timely documented or implemented in accordance with DHS and ICE policy.

Configuration Management

- Password, security patch management, and configuration deficiencies were identified during the vulnerability assessment on hosts supporting FFMS.

Segregation of Duties

- ICE personnel were granted access to the FFMS database that was inconsistent with the segregation of duties principles defined by DHS and ICE policy.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2013

Contingency Planning

- The FFMS contingency plan and security plan contained contradictory information regarding the design and implementation of FFMS backup controls.

Recommendations

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

Security Management

- Continue to deliver annual Information Assurance Awareness Training materials to include IT security policies and procedures related to properly securing sensitive DHS and ICE data within physical workspaces, conduct periodic after-reviews of ICE workspaces, and provide remedial individualized training, as appropriate.

Access Controls

- Implement monitoring controls over the FFMS account management process to ensure that all users are granted access to FFMS in accordance with ICE and DHS requirements and that documentation supporting access authorizations is properly retained.
- Implement technical controls to ensure that passwords for ADEX accounts are configured in accordance with DHS requirements. If necessary and justified by operational and business requirements, ensure that documented requests for exceptions from DHS password requirements identify all affected accounts subject to deviations from standard control requirements and follow established processes for DHS exceptions.
- Implement monitoring controls over the exit clearance process to ensure that all required actions related to verifying and documenting the return and/or safeguarding of Government-furnished equipment and systems from separating or transferring ICE Federal employees and contractors are consistently implemented in accordance with DHS and ICE policy.

Configuration Management

- Implement the specific vendor-recommended corrective actions detailed in the NFRs that were issued for deficiencies identified during our vulnerability assessment.

Segregation of Duties

- Conduct a risk assessment and, subject to a cost-benefit determination, implement additional monitoring controls over FFMS database access to ensure that segregation of duties principles are enforced in accordance with DHS and ICE policy.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2013

Contingency Planning

- Review and update the FFMS contingency plan and security plan to accurately reflect the current state of implemented backup controls.

IT APPLICATION CONTROLS

We conducted testing over certain FFMS application controls supporting in-scope processes during the ICE component of the FY 2013 DHS financial statement audit and did not identify any control deficiencies.

Appendix A

Description of Key ICE Financial Systems and IT Infrastructure within the Scope of the FY 2013 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2013

Below is a description of significant ICE financial management systems and supporting IT infrastructure included in the scope of the ICE component of the DHS FY 2013 financial statement audit.

Federal Financial Management System (FFMS)

FFMS is a CFO designated financial system and certified software application that conforms to Office of Management and Budget Circular A-127 and implements the use of a Standard General Ledger for the accounting of agency financial transactions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements. FFMS is a commercial off-the-shelf financial reporting system, which has an IBM z/OS operating system and an Oracle database. It includes the core system used by accountants, FFMS Desktop that is used by average users, and a National Finance Center payroll interface. The FFMS mainframe component and servers are hosted at the DHS Enterprise Data Center in Virginia (VA). The ICE OCIO is responsible for FFMS.

ICE Network (ADEX)

The ICE Network, also known as the ADEX E-mail System, is a major application for ICE. The ADEX servers and infrastructure for the headquarters and National Capital Area are located in Mississippi and VA. ADEX currently interfaces with the Diplomatic Telecommunications Service Program Office ICENet Infrastructure.

Appendix B
FY 2013 IT Notices of Findings and Recommendations at ICE

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
 September 30, 2013

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-JT-13-01	Weakness in FFMS Backup Documentation	Contingency Planning	X	
ICE-JT-13-02	Security Awareness Issues Identified during After-Hours Physical Security Testing at ICE	Security Management		X
ICE-JT-13-03	Weakness in FFMS Segregation of Duties Relating to IT Functions	Segregation of Duties	X	
ICE-JT-13-04	Weakness in implementation of procedures for transferred/terminated employee and contractor exit processing	Access Controls		X
ICE-JT-13-05	Inadequate FFMS User Access Request Forms	Access Controls		X
ICE-JT-13-06	FFMS network and servers were installed with default configuration settings and protocols	Configuration Management		X
ICE-JT-13-07	FFMS Mainframe Production databases were installed and configured without baseline security configurations	Configuration Management		X
ICE-JT-13-08	FFMS servers have inadequate patch management	Configuration Management		X
ICE-JT-13-09	Weakness in ADEX Password Complexity	Access Controls	X	



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy 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 Financial Officer
Chief Information Officer
Chief Information Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

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 (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

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

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.