

**Information Technology
Management Letter for the
U. S. Immigration and Customs
Enforcement Component of
the FY 2015 Department of
Homeland Security Financial
Statement Audit**





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the U. S. Immigration and Customs Enforcement Component of the FY 2015 Department of Homeland Security Financial Statement Audit

April 22, 2016

Why We Did This

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 2015 DHS Agency Financial Report.

What We Recommend

We recommend that ICE, in coordination with the DHS Chief Information Officer and Chief Financial Officer, make improvements to its financial systems and associated information technology 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 for the year ended September 30, 2015. KPMG, LLP evaluated selected general IT controls and business process application controls at U.S. Immigration and Customs Enforcement (ICE). KPMG, LLP determined that ICE took corrective action to address certain prior year IT control deficiencies.

However, KPMG continued to identify general IT control deficiencies related to access controls and configuration management of ICE's core financial system. The conditions supporting our findings collectively limited ICE's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability.



OFFICE OF INSPECTOR GENERAL


Department of Homeland Security

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

April 22, 2016

MEMORANDUM FOR: Michael Brown
Chief Information Officer
U.S. Immigration and Customs Enforcement

Jonathan Carver
Chief Financial Officer
U.S. Immigration and Customs Enforcement

FROM: 
Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the U.S. Immigration and Customs Enforcement Component of the FY 2015 Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the U.S. Immigration and Customs Enforcement Component of the FY 2015 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 2015 Financial Statements and Internal Control over Financial Reporting*, dated November 13, 2015, which was included in the FY 2015 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2015 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 Sharon Huiswoud, Director, Information Systems and Acquisitions Division, at (202) 254-5451.

Attachment



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

December 20, 2015

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

Ladies and Gentlemen:

In planning and performing 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, 2015 (hereinafter, referred to as the “fiscal year (FY) 2015 DHS consolidated financial statements”), 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 U.S. Immigrations and Customs Enforcement (ICE), a component of DHS that 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.

With respect to financial systems at ICE, we noted certain internal control deficiencies in the general information technology (IT) control areas of access controls and configuration management. 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 where ICE 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 the key ICE financial system and IT infrastructure within the scope of the FY 2015 DHS financial statement audit in Appendix A, and a listing of each ICE 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 ICE, including certain deficiencies in internal control that we consider to be 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 OIG and the ICE Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form opinions on the FY 2015 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 ICE's 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, 2015

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	4
Findings and Recommendations	5
Findings	5
Recommendations	5
Observations Related to Non-Technical Information Security	7

APPENDICES

Appendix	Subject	Page
A	Description of Key ICE Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit	9
B	FY 2015 IT Notices of Findings and Recommendations at ICE	12

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, 2015 (hereinafter, referred to as the “fiscal year (FY) 2015 DHS consolidated financial statements”). In connection with our audit of the FY 2015 DHS consolidated 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), 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

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office (GAO), formed the basis for 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:

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

While each of these five FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs for evaluation based on their relationship to the ongoing

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2015

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 2015 GITC procedures at ICE did not necessarily represent controls from each FISCAM category.

Business Process Application Controls

Where relevant GITCs were determined to be operating effectively, we performed testing over selected IT application controls (process-level controls that were either fully automated or manual with an automated component) 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 Business Process Application Controls 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. They 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 ICE's financial systems' functionality may be inhibiting the agency's ability to implement and maintain internal controls, including effective GITCs and IT application controls supporting financial data processing and reporting. Some key financial feeder systems are not fully integrated with the main financial system. Therefore, in FY 2015, we continued to evaluate and consider the impact of financial system 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 and social engineering at selected ICE facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to ICE 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 2015 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG, DHS OIG, and DHS management. Appendix A provides a description of the key ICE financial system and IT infrastructure within the scope of the FY 2015 DHS financial statement audit.

SUMMARY OF FINDINGS

During FY 2015, we noted that ICE took corrective action to address certain prior-year IT control deficiencies. For example, ICE made improvements by implementing controls over user account management. However, we continued to identify GITC deficiencies related to access controls and configuration management of ICE's core financial system. In many cases, new control deficiencies reflected weaknesses over new systems in scope for FY 2015 that were remediated or historically effective in other system environments.

The conditions supporting our findings collectively limited ICE's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability. Of the seven IT Notices of Findings and Recommendations (NFRs) issued during our FY 2015 testing at ICE, two were repeat findings, either partially or in whole from the prior year, and five were new findings. The seven IT NFRs issued represent deficiencies and observations related to three of the 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 the requirements of DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*; National Institute of Standards and Technology guidance; and ICE policies and procedures, as applicable. The most significant weakness from a financial statement audit perspective continued to include missing user authorization documentation and improper approvals of access.

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 ICE's financial system's functionality may be inhibiting ICE's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data.

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.

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2015 DHS consolidated financial statements, we identified the following GITC deficiencies at ICE:

Access Controls

- Account management activities on ICE's property system were not consistently or timely documented or implemented. These activities included no authorization documentation, individuals approving their own access, access being approved by individuals other than their supervisor, and no documentation of the review and recertification of users.
- User account authorization documentation was not maintained for users of ICE's core financial system.
- User account authorization documentation was not maintained for ICE's time and attendance system.

Configuration Management

- A configuration management procedure or plan had not been formally documented even though management had a consistent process for implementing changes.

IT Application Controls

- The primary financial system allowed obligations to be posted to future dates, which allowed receipts to be processed in excess of available funding, and payments to be processed against these obligations where there was no available funding.

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 system and associated IT security program (in accordance with ICE and DHS requirements, as applicable):

Access Controls

- Update the User Account Management Plan to be in line with current processes, ensure that all user access controls are in compliance with the Plan, and maintain documentation.
- Review and update the User Management Plan and implement changes to ensure that authorization documentation is maintained.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2015

- Continue to develop and strengthen controls around access authorization, annual recertification of users, and document retention.

Configuration Management

- Complete and document the configuration management plan.

IT Application Controls

- Update system configurations to ensure obligations cannot be entered with future dates and to restrict expenses from being recorded that exceed available funding.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2015 audit, we performed additional non-technical information security procedures at ICE. These procedures included after-hours physical security walkthroughs and social engineering to identify instances where ICE 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 2015 STAL, signed by DHS OIG management, KPMG management, and DHS management on May 20, 2015, and transmitted to the DHS CIO Council on May 27, 2015.

Social Engineering

Social engineering is defined as the act of manipulating people into performing actions or divulging sensitive information. The term typically applies to trickery or deception for the purpose of gathering information or obtaining computer system access. The objective of our social engineering tests was to identify the extent to which ICE personnel were willing to divulge network or system passwords that, if exploited, could compromise ICE sensitive information.

To conduct this testing, we made phone calls from various ICE locations at various times throughout the audit. Posing as ICE technical support personnel, we attempted to solicit access credentials from ICE users. Attempts to log into ICE systems were not performed; however, we assumed that disclosed passwords that met the minimum password standards established by DHS policy were valid exceptions. During social engineering performed at ICE, we attempted to call a total of 45 employees and contractors and reached 10. Of those 10 individuals with whom we spoke, two individuals divulged passwords in violation of DHS policy.

The selection of attempted or connected calls was not statistically derived, and, therefore, the results described here should not be used to extrapolate to ICE as a whole.

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 ICE 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 ICE facilities that processed, maintained, and/or had access to financial data during FY 2015. We inspected workspaces to identify instances where materials

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2015

designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from ICE, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at ICE, we inspected a total of 84 workspaces. Of those, 36 were observed to have material – including, but not limited to, unsecured laptops and external media, system passwords and access credentials, information marked “FOUO”, and documents containing sensitive PII – left unattended and unsecured after business hours in violation of DHS policy.

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

Appendix A

Description of Key ICE Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2015

Below is a description of the significant ICE financial management system and supporting IT infrastructure included in the scope of the FY 2015 DHS financial statement audit.

Federal Financial Management System (FFMS)

FFMS is a mainframe-based major application and the official accounting system of record for ICE. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

FFMS includes a back-office component used by the ICE OCFO and the ICE Office of Financial Management. FFMS also includes a desktop application used by the broader ICE and U.S. Citizenship and Immigration Services (USCIS) user communities (including the Burlington Finance Center and the Dallas Finance Center). The ICE instance of FFMS contains interfaces with internal ICE feeder systems and external service providers, including the Department of Treasury's Bureau of the Fiscal Service and the U.S. Department of Agriculture's (USDA) National Finance Center (NFC).

The ICE instance of FFMS is hosted and supported by the ICE OCIO, exclusively for internal use by the ICE user community. The USCIS instance is hosted and supported by the ICE OCIO on behalf of USCIS (under the terms established through a Memorandum of Understanding between the two components), exclusively for internal use by the USCIS user community and, on a limited basis, ICE OCIO and finance center personnel performing support services for USCIS.

The application is hosted at Datacenter 2 in Clarksville, VA and is supported by the IBM z/OS mainframe and Oracle databases.

Bond Management Information System (BMIS)

BMIS is an immigration bond management database used primarily by the Office of Financial Management (OFM) at ICE. The basic function of BMIS is to record and maintain for financial management purposes the immigration bonds that are posted for aliens involved in removal proceedings.

The application is hosted at Datacenter 1 in Stennis, MS, and is supported by an Oracle database and Windows servers.

Real Property Management System (RPMS)

RPMS is an enterprise real estate system for tracking ICE's property portfolio. This includes capturing and generating data in order to create reports on projects, space and move management, leases and contracts, facilities operations and maintenance, energy and environmental, and geospatial information.

The application is hosted at Datacenter 1 in Stennis, MS, and is supported by an Oracle database and Windows servers.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2015

Purchase Request Information System (PRISM)

PRISM is a contract-writing system used by ICE acquisition personnel to create contract awards. PRISM is interfaced with the Federal Procurement Data System – Next Generation. ICE utilizes an instance of the application while the DHS Office of the Chief Procurement Officer (OCPO) owns and manages the system. OCPO is responsible for application configuration and operating system and database administration.

PRISM is supported by an Oracle database with UNIX-based servers. The system resides in Datacenter 1 in Stennis, Mississippi.

Web Time and Attendance (WebTA)

WebTA is a commercial off-the-shelf (COTS) web-based major application hosted by the USDA NFC, and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The ICE Office of the Human Capital Officer (OHC) utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the ICE user community to facilitate payroll processing.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2015

Appendix B

FY 2015 IT Notices of Findings and Recommendations at ICE

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
 September 30, 2015

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-15-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at ICE	Security Management		X
ICE-IT-15-02	Security Awareness Issues Identified during Social Engineering Testing at ICE	Security Management	X	
ICE-IT-15-03	Real Property Management System (RPMS) Account Management Weakness	Access Controls	X	
ICE-IT-15-04	Lack of Bond Management Information System (BMIS) Configuration Management Plan	Configuration Management	X	
ICE-IT-15-05	Deficiency in ICE Federal Financial Management System (FFMS) User Account Authorization Process	Access Controls		X
ICE-IT-15-06	FFMS Application Control Failures	Business Process	X	
ICE-IT-15-07	Deficiency in ICE Web Time and Attendance (WebTA) User Account Authorization Process	Access Controls	X	



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix E
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

Immigration Customs and Enforcement

Director
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