

**Information Technology
Management Letter for the
United States Immigration
and Customs Enforcement
Component of the FY 2016
Department of Homeland
Security Financial
Statement Audit**





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the Immigration and Customs Enforcement 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 ICE, in coordination with the DHS Chief Information Officer and Acting Chief Financial Officer, make improvements to ICE's financial management 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 (DHS) for the year ended September 30, 2016. KPMG evaluated selected general IT controls (GITC) and business process application controls at U.S. Immigration and Customs Enforcement (ICE). KPMG determined 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 and creating a configuration management plan. However, KPMG continued to identify GITC deficiencies related to access controls, configuration management, and segregation of duties of ICE's core financial and feeder systems.

The deficiencies collectively limited ICE'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

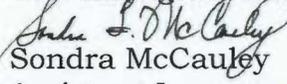
Department of Homeland Security

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

June 8, 2017

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

Stephen Roncone
Acting 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 2016 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 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



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,
U.S. Immigration and Customs Enforcement,
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 U.S. Immigration 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.

We also noted certain internal control deficiencies at ICE 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 ICE, we noted certain matters in the general IT control areas of access controls, segregation of duties, 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 in which 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 systems and IT infrastructure within the scope of the Fiscal Year (FY) 2016 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



U.S. Department of Homeland Security
U.S. Immigration and Customs Enforcement
December 15, 2016
Page 2 of 2

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 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 ICE'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
U.S. Immigration and Customs Enforcement
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 ICE Financial Systems and IT Infrastructure within the Scope of the FY 2016 DHS Financial Statement Audit	12
B	FY 2016 IT Notices of Findings and Recommendations at ICE	15

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, (hereinafter, referred to as the “fiscal year (FY) 2016 DHS consolidated 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) 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 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
U.S. Immigration and Customs Enforcement
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 procedures at ICE 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 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. Many key financial feeder systems are not fully integrated with the main financial system. Therefore, in FY 2016, 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 component facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to component 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
U.S. Immigration and Customs Enforcement
September 30, 2016

Appendix A provides a description of the key ICE 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 and IT application controls, we noted that ICE took corrective action to address certain prior-year IT control deficiencies. For example, ICE made improvements by implementing controls over the user account management process and creating a configuration management plan. However, we continued to identify GITC deficiencies related to access controls, configuration management, and segregation of duties of ICE's core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses over new controls in scope for FY 2016.

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 their confidentiality, integrity, and availability. In addition, certain of these deficiencies at ICE 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 24 IT Notices of Findings and Recommendations (NFR) issued during our FY 2016 testing at ICE, four were repeat findings, either partially or in whole from the prior year, and 20 were new findings. The 24 IT NFRs issued represent deficiencies and observations related to four 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 ICE 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 unauthorized or inadequately monitored access to, and activity within, system components for key ICE financial applications.

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 systems' functionality may be inhibiting ICE'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 inherited from legacy agencies several years ago. Many key ICE 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*.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2016

Although the recommendations made by us should be considered by ICE, it is ultimately the 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 2016 DHS consolidated financial statements, we identified the following GITC deficiencies at ICE:

Access Controls

- Strong password requirements were not consistently enforced on databases supporting financial applications.
- Account management policies and procedures were not completely developed and lacked detail regarding separated or terminated employees; account provisioning for privileged users, including end user database accounts and operating system accounts; and periodic account recertification of all users.
- Account management activities were not consistently or timely documented or implemented. These activities included individuals receiving elevated roles even though they were not in the Office of Human Capital, as required by policy; authorization documentation not corresponding to the date of account creation or modification; individuals receiving additional roles that were not authorized; no authorization documentation maintained; and individuals receiving roles that violated segregation of duties privileges.
- Requirements for generating audit logs with the detail required to perform reviews of auditable events were not implemented for two systems, and ICE had only partially implemented audit logging for the operating system of its core financial system.
- Documentary evidence that recertification of system users, including privileged users, was not maintained or was incomplete.
- All user accounts were not recertified as required by policy.
- Application users were not timely removed upon their separation from ICE.
- Authority to approve privileged access had not been formally delegated by the appropriate party in compliance with DHS policy.

Configuration Management

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

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2016

- Documentation of authorization and approval of configuration changes prior to implementation into the production environment was not maintained.

Segregation of Duties

- A developer had unmonitored access to production data and other sensitive systems software and data.

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

- Standardize password policy requirements by implementing DHS Hardening Guidelines.
- Develop and/or update account management policies and procedures.
- Develop and strengthen controls regarding access authorization, monitoring of system users, and document retention.
- Verify that audit logs provide adequate details to recreate events and have the Information System Security Officer (ISSO) review the logs on a scheduled basis.
- Implement a tool for monitoring and reviewing operating system auditable events.
- Update the current privileged user recertification process procedures so that accounts on the database and operating system are recertified semi-annually.
- Ensure that recertification documentation includes acknowledgement of review in accordance with ICE procedures.
- Update recertification procedural documentation to ensure all users accounts are included in the recertification activities.
- Update the existing process to research local area network deletion requests to ensure application access is removed upon time of user separation.
- Complete and ensure approval of the appropriate delegation letters.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2016

Configuration Management

- Create a process using enterprise tools to detect software that is not managed and ensure that this software is compliant with ICE policies and procedures.
- Create a configuration management plan, process, and procedure to address Data Center 1 service level support, and ensure that system procedures are aligned with department processes already in place.
- Identify and remediate vulnerability scan findings in a timely manner in order to fulfill internal ICE policy requirements.
- Review and update configuration management documentation retention guidelines.

Segregation of Duties

- Put in place proper requirements to restrict developer access to the production environment and verify system access during the annual account recertification.

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 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 2016 *Security Testing Authorization Letter* (STAL) signed by DHS OIG management, KPMG management, and DHS management.

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 12. Of those 12 individuals with whom we spoke, one individual 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 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 2016. We inspected workspaces to identify instances where materials designated by DHS policy as

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2016

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 104 workspaces. Of those, 18 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 2016 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2016

Below is a description of the significant ICE financial management systems and supporting IT infrastructure included in the scope of the FY 2016 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. FFMS 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 that ICE's OCFO and Office of Financial Management (OFM) use. FFMS also includes a desktop application that the broader ICE and USCIS user communities (including the Burlington Finance Center and the Dallas Finance Center) use. The ICE instance of FFMS interfaces with internal ICE feeder systems and systems of 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).

ICE OCIO hosts and supports the ICE instance of FFMS exclusively for the ICE user community.

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

Bond Management Information System (BMIS)

BMIS is an immigration bond management database that ICE's OFM primarily uses. 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 an Oracle database and Windows servers support it.

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 problems, and geospatial information.

The application is hosted at Datacenter 1 in Stennis, MS, and an Oracle database and Windows and UNIX-based servers support it.

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2016

PRISM

PRISM is a contract writing system that ICE acquisition personnel use to create contract awards. PRISM interfaces with the Federal Procurement Data System – Next Generation. ICE 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 supports PRISM, and the system resides in Datacenter 1 in Stennis, MS.

FileOnQ (FOQ)

FOQ is ICE's official invoice tracking system. Invoices are received at the various Service Centers and are scanned/uploaded into FOQ. The invoices are then routed through different individuals for review and approval via electronic signatures.

The application is hosted at Datacenter 2 in Clarksville, VA, and an SQL Server database and Windows servers support it.

ESP

ESP is a web-based application used for Standard Form (SF)-52 processing.

ICE OCIO hosts, operates, and maintains the ESP environment, and multiple components use it. An Oracle database and Windows servers support the application, and it resides in Datacenter 1 in Stennis, MS.

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. The ICE Office of the Human Capital Officer (OHC) uses NFC and WebTA to process front-end input and certification of ICE user community time and attendance entries to facilitate payroll processing.

Appendix B

FY 2016 IT Notices of Findings and Recommendations at ICE

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-16-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at ICE	Security Management		X
ICE-IT-16-02	Non-Compliance with DHS Policies Related to Oracle Database Password Configurations for the Federal Financial Management System (FFMS)	Access Controls	X	
ICE-IT-16-03	Insufficient Audit Log Controls for the Real Property Management System (RPMS)	Access Controls	X	
ICE-IT-16-04	Insufficient Audit Log Controls for the Bonds Information Management System (BMIS)	Access Controls	X	
ICE-IT-16-05	Non-Compliance with DHS Policies Related to Oracle Database Password Control Deficiencies for the RPMS	Access Controls	X	
ICE-IT-16-06	Non-Compliance with DHS Policies Related to Oracle Database Password Control Deficiencies for the BMIS	Access Controls	X	
ICE-IT-16-07	Inconsistent Account Management Controls of Privileged Access for Web Time and Attendance (WebTA)	Access Controls	X	
ICE-IT-16-08	Security Awareness Issues Identified during Social Engineering Testing at ICE	Security Management		X
ICE-IT-16-09	Weakness with BMIS Privileged User Semi-Annual Recertification Process	Access Controls	X	
ICE-IT-16-10	Weakness with RPMS Privileged User Semi-Annual Recertification Process	Access Controls	X	

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
 September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-16-11	Weakness in FileOnQ (FOQ) Configuration Management Controls	Configuration Management	X	
ICE-IT-16-12	Non-Compliance with Delegation of Authority for FFMS, BMIS and FOQ	Security Management	X	
ICE-IT-16-13	Lack of FFMS Account Management Policies and Procedures for Privileged User Access to the Operating System and Database	Access Controls	X	
ICE-IT-16-14	Weakness with FFMS Privileged User Semi-Annual Recertification Process	Access Controls	X	
ICE-IT-16-15	Insufficient Audit Log Controls for the FFMS Operating System	Access Controls	X	
ICE-IT-16-16	Deficiency in PRISM User Account Authorization Process	Access Controls	X	
ICE-IT-16-17	Deficiency in ICE FFMS User Account Authorization Process	Access Controls		X
ICE-IT-16-18	Weakness with Implementation of Separated User Access Control for FFMS	Access Controls	X	
ICE-IT-16-19	Deficiency in ICE WebTA User Account Authorization Process	Access Controls		X
ICE-IT-16-20	Weakness with ESP Account Management Controls	Access Controls	X	
ICE-IT-16-21	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted by ICE HQ, DC1 and DC2	Access Controls and Configuration Management	X	
ICE-IT-16-22	Weakness in FOQ Account Management Controls	Access Controls	X	
ICE-IT-16-23	Incomplete Documentation for FFMS Configuration Management Controls	Configuration Management	X	

Department of Homeland Security
Information Technology Management Letter
U.S. Immigration and Customs Enforcement
September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
ICE-IT-16-24	Weakness with PRISM Annual User Recertification Process	Access Controls	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