

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





# DHS OIG HIGHLIGHTS

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

May 10, 2016

### **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) 2015 DHS Agency Financial Report.

### **What We Recommend**

We recommend that USCIS, 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](mailto: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. Citizenship and Immigration Services (USCIS). KPMG, LLP determined that USCIS took corrective action to address certain prior-year IT control deficiencies.

However, KPMG continued to identify general IT control deficiencies related to access controls for USCIS' core financial and feeder systems. The conditions supporting our findings collectively limited USCIS' ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability.



## OFFICE OF INSPECTOR GENERAL

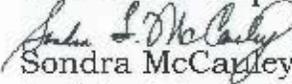
Department of Homeland Security

Washington, DC 20528 / [www.oig.dhs.gov](http://www.oig.dhs.gov)

May 10, 2016

MEMORANDUM FOR: Mark Schwartz  
Chief Information Officer  
U.S. Citizenship and Immigration Services

Joseph Moore  
Chief Financial Officer  
U.S. Citizenship and Immigration Services

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

SUBJECT: *Information Technology Management Letter for the U.S. Citizenship and Immigration Services 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. Citizenship and Immigration Services 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. Citizenship and Immigration Services,  
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. Citizenship and Immigration Services (USCIS), 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 USCIS, we noted certain internal control deficiencies in the general information technology (IT) control area of access controls. 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 USCIS 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 USCIS financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit in Appendix A, and a listing of each



USCIS 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 USCIS, 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 USCIS 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 USCIS' 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. Citizenship and Immigration Services*  
September 30, 2015

---

**TABLE OF CONTENTS**

	<b>Page</b>
Objective, Scope, and Approach	2
Summary of Findings	4
Findings and Recommendations	5
Findings	5
Recommendations	5
Observations Related to Non-Technical Information Security	6

**APPENDICES**

<b>Appendix</b>	<b>Subject</b>	<b>Page</b>
<b>A</b>	Description of Key USCIS Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit	8
<b>B</b>	FY 2015 IT Notices of Findings and Recommendations at USCIS	11

## 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. Citizenship and Immigration Services (USCIS), 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:

*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.

*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 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.

*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.

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. Citizenship and Immigration Services*  
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 USCIS 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 USCIS' 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 and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. 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 USCIS facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to USCIS 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 USCIS financial system and IT infrastructure within the scope of the FY 2015 DHS financial statement audit.

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Citizenship and Immigration Services*  
September 30, 2015

---

## SUMMARY OF FINDINGS

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

The conditions supporting our findings collectively limited USCIS' ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability. Of the five IT notices of findings and recommendations (NFRs) issued during our FY 2015 testing at USCIS, one was a repeat finding, either partially or in whole from the prior year, and four were new findings. The five IT NFRs issued represent deficiencies and observations related to two 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 USCIS policies and procedures, as applicable. The most significant weaknesses from a financial statement audit perspective included:

- Inadequate account management procedural documentation, and
- Not maintaining user access forms for key USCIS 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 USCIS' financial systems functionality may be inhibiting USCIS' ability to implement and maintain effective internal control and 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.

While the recommendations made by us should be considered by USCIS, it is the ultimate responsibility of USCIS 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 USCIS:

#### *Access Controls*

- Account management activities were not consistently or timely documented or implemented. These activities included not performing monthly recertification of user accounts, not maintaining account management documentation, and not having adequate system level procedural documentation that addressed account management, segregation of duties and audit logging.

### **Recommendations**

We recommend that the USCIS 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 USCIS' financial management systems and associated IT security program (in accordance with USCIS and DHS requirements, as applicable):

#### *Access Controls*

- Examine the management directive dealing with account management and the enterprise account management standard operating procedure (SOP) to ensure alignment with USCIS operational requirements.
- Perform monthly account access reviews as required by USCIS management directives.
- Identify and document a process to ensure accountability and control over user access request forms.

## **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 USCIS. These procedures included after-hours physical security walkthroughs and social engineering to identify instances where USCIS 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 USCIS personnel were willing to divulge network or system passwords that, if exploited, could compromise USCIS sensitive information.

To conduct this testing, we made phone calls from various USCIS locations at various times throughout the audit. Posing as USCIS technical support personnel, we attempted to solicit access credentials from USCIS users. Attempts to log into USCIS 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 USCIS, we attempted to call a total of 45 employees and contractors and reached 10. Of those 10 individuals with whom we spoke, none 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 USCIS 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 USCIS 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 USCIS 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. Citizenship and Immigration Services*  
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 USCIS, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at USCIS, we inspected a total of 64 workspaces. Of those, 19 were observed to have material – including, but not limited to, unsecured laptops, information marked “FOUO” or other sensitive information (per MD 11042.1), 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 USCIS as a whole.

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Citizenship and Immigration Services*  
September 30, 2015

---

## **Appendix A**

### **Description of Key USCIS 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. Citizenship and Immigration Services*  
September 30, 2015

---

Below is a description of the significant USCIS financial management systems 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 USCIS. 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 USCIS OCFO and the USCIS Financial Management Division. FFMS also includes a desktop application used by the broader USCIS user communities (including the Burlington Finance Center and the Dallas Finance Center). The USCIS instance of FFMS contains no known internal or external interfaces.

The USCIS instance is hosted and supported by the U.S. Immigration and Customs Enforcement (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.

Purchase Request Information System (PRISM)

PRISM is a contract writing system used by USCIS acquisition personnel to create contract awards. PRISM is interfaced with the Federal Procurement Data System – Next Generation. USCIS 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 United States Department of Agriculture (USDA) National Finance Center (NFC) and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The USCIS Office of Human Capital and Training (OHCT) utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the USCIS user community to facilitate payroll processing.

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Citizenship and Immigration Services*  
September 30, 2015

---

Electronic System for Personnel (ESP)

ESP is a web-based application used for Standard Form (SF)-52 processing. The ESP environment is hosted, operated, and maintained by ICE OCIO and used by multiple components.

Electronic Immigration System (ELIS2)

ELIS2 is a web-based application used by individuals to file their I-90 applications and make payments (such as filing fees, biometric services fees, and the USCIS Immigrant Fee) online. It also provides real-time case status updates to individuals seeking U.S. citizenship.

ELIS2 is supported by an Oracle database with Linux-based servers. The system resides on an Infrastructure as a Service (IaaS) private cloud at Amazon Web Services (AWS) Northern Virginia.

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Citizenship and Immigration Services*  
September 30, 2015

---

## **Appendix B**

### **FY 2015 IT Notices of Findings and Recommendations at USCIS**

Department of Homeland Security  
*Information Technology Management Letter*  
*U.S. Citizenship and Immigration Services*  
 September 30, 2015

<b>FY 2015 NFR #</b>	<b>NFR Title</b>	<b>FISCAM Control Area</b>	<b>New Issue</b>	<b>Repeat Issue</b>
CIS-IT-15-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCIS	Security Management		X
CIS-IT-15-02	Inadequate Account Management Procedural Documentation for the Electronic Immigration System (ELIS2) Environment	Access Controls	X	
CIS-IT-15-03	Inconsistent Implementation of Entity Level Account Recertification Management Directive for the Federal Financial Management System (FFMS)	Access Controls	X	
CIS-IT-15-04	Lack of ESP User Access Forms	Access Controls	X	
CIS-IT-14505	Lack of WebTA User Access Forms	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

**Citizenship and Immigration Services**

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](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto: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](http://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