OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the U.S. Citizenship and Immigration Services Component of the FY 2016 Department of Homeland Security Financial Statement Audit

Homeland Security

June 26, 2017
OIG-17-76

DHS OIG HIGHLIGHTS

Information Technology Management Letter for the U.S. Citizenship and Immigration Services Component of the FY 2016 Department of Homeland Security Financial Statement Audit

June 26, 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 USCIS, in coordination with the DHS Chief Information Officer and Acting Chief Financial Officer, make improvements to its 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. Citizenship and Immigration Services (USCIS). KPMG determined 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 controls related to user access forms. However, KPMG continued to identify GITC deficiencies related to access controls for USCIS' core financial and feeder systems.

The deficiencies collectively limited USCIS' 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 identified in the FY 2016 DHS Agency Financial Report.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 26, 2017

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

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

Sondra L. McCauley

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 2016 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 2016 Department of Homeland Security Financial Statement Audit.* This report contains comments and recommendations related to information technology internal control deficiencies. The deficiencies 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. Citizenship and Immigration Services,
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. 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.

We also noted certain internal control deficiencies at USCIS 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 USCIS, we noted certain matters in the general IT control areas of security management, 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 in which 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 Fiscal Year (FY) 2016 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, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the OIG and the USCIS 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 USCIS' 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. Citizenship and Immigration Services
September 30, 2016

TABLE OF CONTENTS

APPENDICES

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. 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 U.S. Government Accountability Office (GAO) issued the *Federal Information System Controls Audit Manual* (FISCAM), which 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. It 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, 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.
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 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 evaluated at USCIS 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 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 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 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 2016 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG LLP, DHS OIG, and DHS management.

Appendix A provides a description of the key USCIS 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 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 controls related to user access forms. However, we continued to identify GITC deficiencies related to access controls for USCIS' core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses over systems in scope for FY 2016 that were remediated or historically effective in other system environments.

USCIS' main financial application is owned and operated by U.S. Immigration and Customs Enforcement (ICE). As a service provider, ICE provides support to USCIS. The GITC deficiencies we identified at ICE could potentially impact USCIS' financial data, and as such, we issued a finding to USCIS.

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 their confidentiality, integrity, and availability. In addition, certain of these deficiencies at USCIS 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 seven IT notices of findings and recommendations (NFR) issued during our FY 2016 testing at USCIS, three were repeat findings, either wholly or in part from the prior year, and four were new findings. The seven IT NFRs issued represent deficiencies and observations related to three of the five FISCAM GITC categories.

The majority of the deficiencies that our audit identified were related to noncompliance with financial system controls. According to DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, National Institute of Standards and Technology guidance, and USCIS 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 inadequate account management controls.

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 USCIS financial systems were not compliant with Federal financial management system requirements as defined by the *Federal Financial Management Improvement Act of 1996* (FFMIA) and Office of Management and Budget Circular Number A-123 Appendix D, *Compliance with FFMIA*.

Although the recommendations made by us should be considered by USCIS, it is ultimately the 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 2016 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. Activities included a lack of user signatures, maintenance of account management documentation, timely signatures, and formal authorization and business justification for shared/generic user accounts.

- Quarterly recertification of system accounts was incomplete for one quarter and was not completed for another quarter.

- Controls related to user account recertification, removal of inactive and/or terminated individuals, and audit logging of account management activity to include account creation date were not in place or were ineffective.

Configuration Management

- A configuration management plan was not developed, documented, approved, or disseminated for one system.

Access Controls and Configuration Management

- Deficiencies exist regarding non-compliance with DHS policy for database password configurations, non-compliance with delegation of authority requirements, a lack of account management policies and procedures for privileged user access to operating systems and databases, an inadequate privileged user semi-annual recertification process, insufficient audit log controls for the operating system, incomplete documentation for configuration management controls, and weaknesses in vulnerability scanning activities.

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

- Revise the access request form signature blocks.
- Conduct a review over access controls of users who transfer to USCIS from other DHS offices and update account management procedures as appropriate.
- Complete appropriate documentation to address the use of generic/shared accounts.
- Review and update the current recertification process to ensure recertification of users is performed per policy.
- Update procedures for account recertification and removal of inactive and/or terminated individuals, and complete and provide artifacts around account creation dates.

Configuration Management

- Develop an enterprise configuration management plan.

Access Controls and Configuration Management

- Monitor ICE OCIO/OCFO remediation efforts on a monthly basis, and request corrective action plans and documents validating the remediation of deficiencies.

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 USCIS. These procedures included after-hours physical security walkthroughs and social engineering to identify instances in which 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 2016 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 USCIS personnel were willing to divulge network or system passwords that, if exploited, could compromise sensitive USCIS 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 18. Of those 18 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 2016. We inspected workspaces to identify instances where materials designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from USCIS, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at USCIS, we inspected a total of 70 workspaces. Of those, 8 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.

Appendix A

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

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

ICE OCIO on behalf of USCIS (under the terms of a Memorandum of Understanding established between the two components) hosts and supports the USCIS instance of FFMS. This is done exclusively for the internal USCIS user community and, on a limited basis, for ICE OCIO and finance center personnel performing support services for USCIS.

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

Procurement Request Information System Management (PRISM)

PRISM is a contract writing system that USCIS acquisition personnel use to create contract awards. PRISM interfaces with the Federal Procurement Data System – Next Generation. USCIS uses an instance of the application, and 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.

An Oracle database with UNIX-based servers supports PRISM. The system resides in Datacenter 1 in Stennis, MS.

Electronic System for Personnel (ESP)

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

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

Electronic Immigration System (ELIS2)

ELIS2 is a web-based application that individuals use 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.

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

Web Time and Attendance (WebTA)

WebTA is a commercial off-the-shelf (COTS) web-based major application that the U.S. Department of Agriculture's National Finance Center (NFC) hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. The USCIS Office of Human Capital and Training (OHCT) uses WebTA to process front-end input and certification of USCIS user community time and attendance entries to facilitate payroll processing.

Appendix B

FY 2016 IT Notices of Findings and Recommendations at USCIS

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CIS-IT-16-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at USCIS	Security Management		X
CIS-IT-16-02	Lack of Configuration Management Plan for the Electronic Immigration System (ELIS2)	Configuration Management	X	
CIS-IT-16-03	Unsigned ESP User Access Forms	Access Controls	X	
CIS-IT-16-04	Weakness in ESP Quarterly Account Recertification	Access Controls	X	
CIS-IT-16-05	Inadequate Audit Logging and Account Management and Recertification for the Electronic Immigration System (ELIS2) Environment	Access Controls		X
CIS-IT-16-06	Lack of WebTA User Access Forms	Access Controls		X
CIS-IT-16-07	FFMS Deficiencies at ICE that Impact USCIS	Access Controls	X	

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

Acting Chief Financial Officer
Chief Information Officer
Audit Liaison

U.S. Citizenship and Immigration Services

Acting 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