Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit – National Protection and Programs Directorate

OIG-14-98

May 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 28, 2014

MEMORANDUM FOR: David Epperson
Chief Information Officer

Nicole Windham
Director, Budget and Financial Administration

FROM:

Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the FY 2013 Department of Homeland Security's Financial Statement Audit – National Protection and Programs Directorate*

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

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

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

Attachment

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

March 11, 2014

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

Ladies and Gentlemen:

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"), and have issued our report thereon dated December 11, 2013. In planning and performing our audit of the financial statements of DHS, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated December 11, 2013, included internal control deficiencies identified during our audit that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. This letter represents the separate limited distribution report mentioned in that report, of matters related to the Office of Financial Management (OFM) and the Office of the Chief Information Officer (OCIO).

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

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

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

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of DHS' organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Department of Homeland Security
Information Technology Management Letter
National Protection and Programs Directorate
September 30, 2013

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	**2**
General IT Control Findings and Recommendations	**2**
FY 2013 IT Notices of Findings and Recommendations at NPPD	**3**

OBJECTIVE, SCOPE, AND APPROACH

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"). In connection with our audit of the FY 2013 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) at the National Protection and Programs Directorate (NPPD) to assist in planning and performing our audit engagement. Specifically, limited after-hours physical security testing and social engineering at select NPPD facilities was conducted to identify potential control deficiencies in non-technical aspects of IT security.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Summary

During FY 2013, we continued to identify GITC weaknesses that could potentially impact NPPD's financial data related to controls over security management.

Collectively, the IT control weaknesses limited NPPD's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over NPPD's financial reporting and its operations.

The two IT Notices of Findings and Recommendation (NFRs) issued during our FY 2013 testing were repeat findings from the prior year and represent weaknesses in the category of security management as defined by the *Federal Information System Controls Audit Manual*, issued by the U.S. Government Accountability Office, which formed the basis of our GITC evaluation procedures.

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

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

Findings

During our audit of the FY 2013 DHS financial statements, we identified the following NPPD GITC control deficiencies.

After-Hours Physical Security Testing

On August 20, 2013, we performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to printed or electronic media, equipment, or credentials residing within an NPPD employee's or contractor's work area or shared workspaces which could be used by others to gain unauthorized access to systems housing financial or other sensitive information. The testing was performed at an NPPD facility in Arlington, Virginia, that processes, maintains, and has access to financial data.

At this location, we observed 14 instances where unsecured or unlocked laptops and printed materials marked "For Official Use Only" or containing sensitive personally identifiable information were accessible by individuals without a "need to know".

Social Engineering

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing/enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or gaining computer system access.

On July 22, 2013, we performed social engineering testing from a DHS facility to identify risks related to NPPD personnel awareness of responsibilities for protecting sensitive IT information, including personal system access credentials, from disclosure to unauthorized personnel. We noted four instances where individuals divulged their FFMS application account password to KPMG auditors.

Recommendation

We recommend that the NPPD 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, develop a stronger compliance process to ensure employees are complying with information, physical, and privacy security policies.

FY 2013 IT NOTICES OF FINDINGS AND RECOMMENDATIONS AT NPPD

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
NPPD-IT-13-01	Security Awareness Issues Identified During Social Engineering Testing at NPPD	Security Management		X
NPPD-IT-13-02	Security Awareness Issues Identified during After-Hours Physical Security Testing at NPPD	Security Management		X

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

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

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

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

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

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