OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the United States Coast Guard Component of the FY 2014 Department of Homeland Security Financial Statement Audit

Homeland Security

March 17, 2015
OIG-15-47

HIGHLIGHTS

Information Technology Management Letter For the United States Coast Guard Component of the FY 2014 Department of Homeland Security Financial Statement Audit

March 17, 2015

Why We Did This

Each year, our independent auditors identify component-level information technology control deficiencies as part of the Department of Homeland Security (DHS) consolidated financial statement audit. This letter provides details that were not included in the fiscal year (FY) 2014 DHS Agency Financial Report.

What We Recommend

We recommend that USCG, in coordination with the DHS Chief Information Officer and 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-IG.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, 2014. KPMG, LLP evaluated selected general information technology controls and business process application controls at the United States Coast Guard (USCG). KPMG, LLP determined that USCG took corrective action over designing and consistently implementing certain account management and configuration management controls.

However, KPMG, LLP continued to identify general information technology control deficiencies related to security management, logical access, configuration management, segregation of duties, and contingency planning for USCG's core financial and feeder systems. Such control deficiencies limited USCG's ability to ensure the confidentiality, integrity, and availability of its critical financial and operational data.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC

March 17, 2015

TO: Marshall B. Lytle III
Chief Information Officer
United States Coast Guard

Rear Admiral Stephen P. Metruck
Chief Financial Officer
United States Coast Guard

Sondra L. McCauley

FROM: Sond ra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the United States Coast Guard Component of the FY 2014 Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the United States Coast Guard Component of the FY 2014 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 2014 Financial Statements and Internal Control over Financial Reporting,* dated November 14, 2014, which was included in the FY 2014 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2014 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 Audit Division, at (202) 254-5451.

Attachment

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

December 19, 2014

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Coast Guard,
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, 2014 (hereinafter, referred to as the "fiscal year (FY) 2014 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. 14-02, *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 the U.S. Coast Guard (Coast Guard), 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 identified certain internal control deficiencies at Coast Guard 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 IT controls and financial system functionality at the DHS Department-wide level. Specifically, with respect to financial systems at Coast Guard, we noted certain matters in the general IT control areas of access controls and configuration management. These matters are described in the *Findings and Recommendations* section of this letter.

Additionally, at the request of the DHS Office of Inspector General (OIG), we performed additional non-technical information security procedures to identify instances where Coast Guard 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 key Coast Guard financial systems and IT infrastructure within the scope of the FY 2014 DHS financial statement audit in Appendix A, and a listing of each Coast Guard 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 Coast Guard, 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 Coast Guard Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form opinions on the FY 2014 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 Coast Guard's organization gained during our work to make comments and suggestions that we hope will be useful to you.

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

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

Very truly yours,

KPMG LLP

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, 2014 (hereinafter, referred to as the "fiscal year (FY) 2014 DHS consolidated financial statements"). In connection with our audit of the FY 2014 DHS consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and business process application controls (BPACs) at the U.S. Coast Guard (Coast Guard), 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 of our GITC evaluation procedures.

FISCAM was designed to inform financial statement auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial statement audit. FISCAM also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs and the IT environment of a Federal agency. FISCAM defines the following five control categories to be essential to the effective operation of GITCs and the IT environment:

1. *Security Management* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
2. *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
3. *Configuration Management* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.
4. *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
5. *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

While each of these five FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs for evaluation based on their relationship to the ongoing effectiveness of process-level automated controls or manual controls with one or more automated components. This includes those controls which depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2014 GITC procedures at Coast Guard 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 BPACs (process-level controls which 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 BPACs as the automated and/or manual controls applied to business transaction flows and relate 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 Coast Guard's financial systems' functionality may be inhibiting the agency's ability to implement and maintain internal controls, including effective GITCs and BPACs 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 2014, 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 Coast Guard facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to Coast Guard 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 2014 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG, DHS OIG, and DHS management.

Appendix A provides a description of the key Coast Guard financial systems and IT infrastructure within the scope of the FY 2014 DHS financial statement audit.

SUMMARY OF FINDINGS

During FY 2014, we noted that Coast Guard took corrective action to address one prior year IT control deficiency. Specifically, Coast Guard made improvements over implementing certain account management controls. However, we continued to identify GITC deficiencies related to access controls and configuration management of Coast Guard core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses over controls which were historically effective.

The conditions supporting our findings collectively limited Coast Guard's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, certain of these deficiencies at Coast Guard 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 14 IT Notices of Findings and Recommendations (NFRs) issued during our FY 2014 testing at Coast Guard, 7 were repeat findings, either partially or in whole from the prior year, and 7 were new findings. The 14 IT NFRs issued represent deficiencies and observations related to three of the five FISCAM GITC categories.

The majority of findings resulted from the lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with the requirements of DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, National Institute of Standards and Technology guidance, and Coast Guard policies and procedures, as applicable. The most significant weaknesses from a financial statement audit perspective continued to include:

1. Excessive, unauthorized, or inadequately monitored access to, and activity within, system components for key Coast Guard financial applications; and
2. Configuration management controls that were not fully defined, followed, or effective.

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 Coast Guard's financial systems' functionality may be inhibiting Coast Guard'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 Coast Guard 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.*

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

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2014 DHS consolidated financial statements, we identified the following GITC deficiencies at Coast Guard, certain of which, in the aggregate, contribute to the IT material weakness at the Department level:

Access Controls

- Controls to notify Coast Guard system owners of separated or transferred military and civilian personnel and contractors and to generate reports of separated or transferred individuals to support periodic reviews of system access were not implemented.

- Reviews of financial application audit logs were not consistently performed in accordance with DHS policy.

- Programmers retained inappropriate or excessive access to financial application production environments in conflict with the principle of segregation of duties.

- Account management activities on Coast Guard financial systems were not consistently or timely documented or implemented. These activities included authorization of new access and periodic recertification of access.

- Account security controls, including invalid login attempt lockout parameters, were not fully implemented for accounts on one financial system.

- Strong password requirements were not consistently enforced on databases supporting financial applications.

Configuration Management

- Security patch management and configuration deficiencies were identified during vulnerability assessments of system components supporting multiple financial applications.

Recommendations

We recommend that the Coast Guard 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 Coast Guard’s financial management systems and associated IT security program (in accordance with Coast Guard and DHS requirements, as applicable):

Access Controls

- Complete efforts to document and implement enterprise-wide processes to ensure that system owners are notified and revoke access from separated or transferred military and civilian personnel and contractors timely in accordance with Coast Guard and DHS requirements.

- Implement monitoring controls over the account management process to ensure that financial application access is consistently authorized prior to being granted, and that all users of Coast Guard systems are periodically revalidated in accordance with Coast Guard and DHS requirements.

- Implement configurations to lock system accounts after three consecutive invalid login attempts for a duration not less than 20 minutes.

- Implement technical controls to ensure that passwords for financial databases accounts are configured in accordance with Coast Guard and DHS requirements.

- Implement monitoring controls over the audit log generation and review process for financial systems to ensure that evidence of audit log reviews is consistently retained.

Configuration Management

- Implement the specific vendor-recommended corrective actions detailed in the NFR that were issued for deficiencies identified during the vulnerability assessments.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2014 audit, we performed additional non-technical information security procedures at Coast Guard. These procedures included after-hours physical security walkthroughs and social engineering to identify instances where Coast Guard 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 2014 STAL, signed by DHS OIG management, KPMG management, and DHS management (Chief Information Officer [CIO], Chief Information Security Officer, Chief Financial Officer, Chief Privacy Officer, and Chief Security Officer) on June 3, 2014, and transmitted to the DHS CIO Council on June 12, 2014.

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 information gathering or obtaining computer system access. The objective of our social engineering tests was to identify the extent to which Coast Guard personnel were willing to divulge network or system passwords that, if exploited, could compromise Coast Guard sensitive information.

To conduct this testing, we made phone calls from various Coast Guard locations at various times throughout the audit. Posing as Coast Guard technical support personnel, we attempted to solicit access credentials from Coast Guard users. Attempts to login to Coast Guard 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 Coast Guard, we attempted to call a total of 51 employees and contractors and reached 29. Of those 29 individuals with whom we spoke, five divulged their 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 Coast Guard 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 (FOUO) Information*, mandate the physical safeguarding of certain materials and assets which, 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 Coast Guard 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 Coast Guard facilities that processed, maintained, and/or had access to financial data during FY 2014. 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 Coast Guard, DHS OIG and DHS OCIO.

During after-hours physical security walkthroughs performed at Coast Guard, we inspected a total of 270 workspaces. Of those, 84 were observed to have material – including, but not limited to, system passwords, information marked “FOUO”, documents containing sensitive PII, and government-issued laptops or storage media – 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 Coast Guard as a whole.

Appendix A

Description of Key Coast Guard Financial Systems and IT Infrastructure within the Scope of the FY 2014 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
U.S. Coast Guard
September 30, 2014

Below is a description of the significant Coast Guard financial management systems and supporting IT infrastructure included in the scope of the FY 2014 DHS financial statement audit.

Core Accounting System (CAS)

CAS is a web-based major application and the official accounting system of record for the Coast Guard. It is used to record all income and expenses and create income statements, balance sheets, and other financial reports to show financial condition. Accounting and financial management functions supported by CAS include accounts payable, accounts receivable, general and expense ledgers, and asset (including capital asset) management. It contains interfaces with the DHS Treasury Information Executive Repository (DHSTIER), internal Coast Guard feeder systems, and external service providers (including the Department of Treasury Bureau of the Fiscal Service).

CAS is hosted and supported by the Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO exclusively for internal use by the Coast Guard user community.

Finance Procurement Desktop (FPD)

FPD is a web-based major application that supports Coast Guard funds management processes by creating and managing simplified procurement documents and maintaining accurate accounting records agency wide. Functions performed by FPD include ledger management, budgeting and funds distribution, procurement requests and simplified acquisitions, receipt of goods/services (accruals), and program element status reporting. It is integrated with CAS and contains interfaces with DHSTIER, other internal Coast Guard feeder systems, including the Contract Management Information System, and external service providers (including the Department of Treasury Bureau of the Fiscal Service).

FPD is hosted and supported by the Office of the Director of Financial Operations/Comptroller and Coast Guard OCIO exclusively for internal use by the Coast Guard financial management and acquisitions user community.

Direct Access

Direct Access is a web-based major application and the system of record for all payroll events for the Coast Guard. Direct Access supports “self-service” capabilities for end-user updates and corrections to personal information, including beneficiary designations, and is used by the Coast Guard Pay & Personnel Center (PPC) to process payroll events and perform personnel actions, such as pay scales updates. It contains interfaces with other internal Coast Guard feeder systems, including the Joint Uniform Military Pay System (JUMPS), and external service providers (including the United States Public Health Service and the Department of Veterans Affairs). Global Pay, a module within Direct Access, provides retiree and annuitant support services.

Direct Access is developed, maintained, and hosted by Addx Corporation, and supported by Coast Guard OCIO for internal use by the Coast Guard user community and via external public (authenticated) access by Coast Guard retirees.

Joint Uniform Military Pay System (JUMPS)

JUMPS is a mainframe-based major application used for computations of all necessary information used to pay Active Duty and Reservist military members. It contains interfaces with other internal Coast Guard feeder systems, including Direct Access.

JUMPS is developed, maintained, and hosted by the Coast Guard Operations Systems Center (OSC) (a component of the Office of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology), and supported by Coast Guard PPC exclusively for internal use by the Coast Guard user community.

Naval and Electronics Supply Support System (NESSS)

NESSS is a web-based major application that provides integrated provisioning and cataloging, unit configuration, supply and inventory control, procurement, depot-level maintenance, property accountability, and financial ledger capabilities as part of the family of Coast Guard logistics systems.

NESSS is developed, maintained, and hosted by the Coast Guard OSC (a component of the Office of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology) and the Office of Logistics Program Management, and supported by Coast Guard OSC exclusively for internal use by the Coast Guard Yard and Surface Forces Logistics Center (SFLC) finance and logistics user communities.

Aviation Logistics Management Information System (ALMIS)

ALMIS is a hybrid web-based and client-server major application that provides Coast Guard Aviation logistics management support in the areas of operations, configuration management, maintenance, supply, procurement, financial management, and business intelligence. It integrates the forecasting capability of the Aviation Computerized Maintenance Systems subsystem with the inventory management and fiscal accounting functionality of the Aviation Maintenance Management System (AMMIS) subsystem to improve inventory purchase/repair decisions and provide total asset visibility.

ALMIS is developed, maintained, hosted, and supported by the Coast Guard Aviation Logistics Center exclusively for internal use by the Coast Guard financial management and aviation logistics user community.

Appendix B

FY 2014 IT Notices of Findings and Recommendations at Coast Guard

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-14-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems	Access Controls		X
CG-IT-14-02	JUMPS audit log review	Access Controls	X	
CG-IT-14-03	Inappropriate access to JUMPS Production Library Datasets	Access Controls	X	
CG-IT-14-04	Weakness in Direct Access Annual User Recertification	Access Controls		X
CG-IT-14-05	AMMIS System Administrator Account Lockouts for Invalid Login Attempts	Access Controls	X	
CG-IT-14-06	Security Awareness Issues Identified during Social Engineering Testing at Coast Guard Headquarters, SFLC/Coast Guard Yard; FINCEN	Security Management		X
CG-IT-14-07	Review of Direct Access Security Logs	Access Controls		X
CG-IT-14-08	Direct Access Database Profile Security Configurations	Access Controls	X	
CG-IT-14-09	Security Awareness Issues Identified during After-Hours Physical Security Testing at Coast Guard	Security Management		X
CG-IT-14-10	NESSS Database Profile Security Configurations	Access Controls	X	
CG-IT-14-11	NESSS System User Access	Access Controls	X	
CG-IT-14-12	FPD Audit Log Reviews	Access Controls	X	
CG-IT-14-13	Weakness in JUMPS Annual User Recertification	Access Controls		X
CG-IT-14-14	Security Management and Configuration Management Controls - Vulnerability Assessment	Configuration Management		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

United States Coast Guard

Commandant
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