

Department of Homeland Security **Office of Inspector General**

Information Technology Management Letter for the FY 2013 United States Customs and Border Protection Financial Statement Audit






OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 28, 2014

MEMORANDUM FOR: Charles Armstrong
Chief Information Officer
U.S. Customs and Border Protection

Deborah Schilling
Chief Financial Officer
U.S. Customs and Border Protection

FROM: 
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the FY
2013 United States Customs and Border Protection
Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the FY 2013 United States Customs and Border Protection Financial Statement Audit*. 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 19, 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 19, 2014

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

Chief Information Officer and Chief Financial Officer,
U.S. Customs and Border Protection

Ladies and Gentlemen:

In planning and performing our audit of the consolidated balance sheets of the U.S. Customs and Border Protection (CBP), a component of the U.S. Department of Homeland Security (DHS), and the related consolidated statements of net cost, changes in net position, and custodial activity, and the combined statements of budgetary resources as of and for the years ended September 30, 2013 and 2012 (hereinafter, referred to as "consolidated financial statements"), in accordance with auditing standards generally accepted in the United States of America, we considered CBP's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of CBP's internal control. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and the Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*. Accordingly, we do not express an opinion on the effectiveness of CBP's internal control.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated January 30, 2014, included internal control deficiencies identified during our audit that represented a significant deficiency in information technology (IT) controls at CBP. This letter represents the separate limited distribution report mentioned in that report.

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 CBP's financial systems' IT controls, we noted certain matters in the areas of security management, access controls, configuration management, contingency planning, and IT application controls. These matters are described in the *General IT Control Findings and Recommendations* and *IT Application Controls* sections of this letter.

The Table of Contents identifies each section of the letter. We have provided a description of key CBP financial systems and IT infrastructure within the scope of the FY 2013 CBP consolidated financial



statement audit engagement in Appendix A, and a list of each IT NFR communicated to management during our audit in Appendix B.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of CBP'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

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
September 30, 2013

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	4
General IT Control Findings and Recommendations	5
<i>Findings</i>	5
Security Management	5
Access Controls	5
Configuration Management	6
Contingency Planning	6
<i>Recommendations</i>	6
Security Management	6
Access Controls	6
Configuration Management	8
Contingency Planning	8
IT Application Controls	8

APPENDICES

Appendix	Subject	Page
A	Description of Key CBP Financial Systems and IT Infrastructure within the Scope of the FY 2013 CBP Financial Statement Audit	9
B	FY 2013 IT Notices of Findings and Recommendations at CBP	12

OBJECTIVE, SCOPE, AND APPROACH

Objective

We have audited the consolidated balance sheets of the U.S. Customs and Border Protection (CBP), a component of the U.S. Department of Homeland Security (DHS), as of September 30, 2013 and 2012, and the related consolidated statements of net cost, changes in net position, and custodial activity, and the combined statements of budgetary resources (referred to herein as the “fiscal year (FY) 2013 consolidated financial statements”). In connection with our engagement to audit CBP’s consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and IT application controls at CBP to assist in planning and performing our audit engagement.

Scope

The scope of our GITC and IT application control test work is described in Appendix A, which provides a description of the key CBP financial systems and IT infrastructure within the scope of the FY 2013 CBP consolidated financial statement audit engagement.

Approach

General Information Technology Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office, 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:

- *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.
 - In conjunction with our test work of security management GITCs, limited after-hours physical security testing at select CBP facilities was conducted to identify potential control deficiencies in non-technical aspects of IT security.
- *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 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.

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
September 30, 2013

- We performed technical information security testing for key CBP network and system devices. The technical security testing was performed from within select DHS facilities and focused on production devices that directly support CBP's financial processing and key general support systems.
- *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.

IT Application Controls

We performed testing over selected key IT application controls 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 application controls as the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS

During FY 2013, CBP took corrective action to address certain prior year IT control deficiencies. For example, CBP made improvements over designing and implementing certain configuration management and security management controls over CBP information systems, as well as strengthening and improving controls around physical and logical access (including enforcement of segregation of duties). However, during FY 2013, we continued to identify IT application control deficiencies related to financial system functionality, and GITC deficiencies related to controls over physical and logical access (including the generation and review of audit logs), configuration management, and contingency planning, for CBP core financial and feeder systems and associated General Support System (GSS) environments.

Collectively, the IT control deficiencies limited CBP'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 deficiencies negatively impacted CBP's internal controls over financial reporting and its operations. We consider certain deficiencies to represent a significant deficiency at CBP under standards established by the American Institute of Certified Public Accountants.

Of the 29 IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, 17 were repeat findings, either partially or in whole from the prior year, and 12 were new findings. The 29 IT NFRs issued represent deficiencies in four of the five FISCAM general IT control categories, as well as in the area of IT application controls.

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 DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, requirements and National Institute of Standards and Technology (NIST) guidance. Specifically, the findings stem from:

1. Inadequately designed and ineffective access control policies and procedures relating to the management of logical and physical access to financial applications, databases, and support systems;
2. Insufficient logging of system events and monitoring of audit logs;
3. Patch, configuration, and vulnerability management control deficiencies within systems;
4. Inconsistently implemented backup management controls; and
5. System functionality limitations preventing adequate implementation of automated preventative or detective controls to support management and implementation of custodial revenue and drawback processes.

These deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and CBP financial data could be exploited, thereby compromising the integrity of CBP financial data used by management and reported in the consolidated financial statements.

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

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2013 CBP consolidated financial statements, we identified the following GITC deficiencies. Certain deficiencies, in the aggregate, are considered a significant deficiency at CBP. For our assessment of the deficiencies, see Appendix B.

Security Management

- Separation clearance actions for separated or transferred Federal employees and contractors were not consistently or timely documented or implemented in accordance with DHS and CBP policy.

After-Hours Physical Security Testing

On June 26 and July 22, 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 a CBP employee's or contractor's work area or shared workspaces which could be used by others to gain unauthorized access to financial systems or other systems containing sensitive information. The testing was performed at various CBP locations in the Washington, DC, metropolitan area and Indianapolis, Indiana that process, maintain, and/or have access to financial data.

We observed 123 instances where passwords, sensitive IT information (such as server names or IP addresses), keys, unsecured or unlocked credentials, credit cards, laptops, remote access devices, and external media, and printed materials marked "For Official Use Only" or containing sensitive Personally Identifiable Information were accessible by individuals without a "need to know".

Access Controls

- Segregation of duties conflicts existed relative to administrator accounts on configuration management utilities used for CBP financial applications, and compensating controls to log and review administrator activity were not consistently implemented.
- DHS and CBP requirements for password complexity and lifetime were not fully implemented for accounts on the Systems, Applications, and Products (SAP) UNIX server, Automated Commercial Environment (ACE) Advanced Interactive eXecutive (AIX) operating system, and ACE Database 2 (DB2).
- Audit logs, including logs of emergency developer access to the production environment, for components of the SAP and Automated Commercial System (ACS) environments (including the application, database, and operating system/mainframe layers) were not consistently reviewed by management in accordance with DHS and CBP policy, and risk assessments were not performed to identify relevant security events subject to requirements for logging and periodic review.

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
September 30, 2013

- Developers were granted emergency access functions within the ACS production environment in violation of the principles of least privilege as referenced in NIST. The access granted was not commensurate with job responsibilities.
- Account management activities on CBP financial systems (including the application, database, and operating system/mainframe layers) and the District of Columbia (DC) Metropolitan (Metro) Local Area Network (LAN), including authorization of new access, periodic recertification of access, and revocation of access from separated or transferred Federal employees and contractors, were not consistently or timely documented or implemented in accordance with DHS and CBP policy.
- Logs of visitor access to the server room within the National Data Center were not consistently maintained.
- DHS and CBP requirements for the assignment of unique application account identifiers were not consistently implemented.

Configuration Management

- Security patch management and configuration deficiencies were identified during the vulnerability assessment on hosts supporting the SAP environment.
- Access to CBP application test and development environments was not consistently or timely documented or authorized in accordance with DHS and CBP policy.

Contingency Planning

- Backup parameters were not configured in accordance with CBP requirements.

Recommendations

We recommend that the CBP Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO) make the following improvements to CBP's financial management systems and associated IT security program (in accordance with CBP and DHS requirements, as applicable).

Security Management

- Continue to maintain and enforce existing security awareness campaigns, enhance focus on conducting periodic desktop reviews, and consider adding penalties for users with multiple recurring documented violations of security awareness policies and physical security requirements.

Access Controls

- Evaluate and enforce the configuration management Administrator access audit log process to ensure that configuration management Administrator access audit logs are being reviewed on a monthly basis, documented and audit log review evidence is maintained.

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
September 30, 2013

- Implement technical controls, including a password value check, to ensure that passwords for CBP operating system and database accounts are configured in accordance with DHS and CBP requirements for complexity and lifetime.
- Perform and document a risk assessment to identify relevant security events on the SAP and ACS environments which should be subject to requirements for logging and periodic review.
- Conduct a cost-benefit analysis to determine the feasibility of implementing a tool or enhanced system functionality to automate the aggregation and review of system logs.
- Implement monitoring controls over the audit log review process in the SAP and ACS environments to ensure that audit logs, including logs of emergency developer access to the production environment, are being reviewed by management on a periodic basis, are documented, and audit log review evidence is maintained .
- Implement monitoring controls over the account management process within the ACS production environment, including relative to developer emergency access to production, to ensure that access granted is limited to necessary application functions commensurate with job responsibilities.
- Perform a root cause analysis to determine the source of instances of non-compliance with the annual account recertification process and, if appropriate, develop an enterprise-level solution to implement monitoring controls to ensure that all accounts are recertified annually.
- Implement monitoring controls over the account management process, including escalation to management for follow-up and enforcement as appropriate, to ensure that all users are granted access to CBP systems.
- Perform a root cause analysis to determine the source of instances of non-compliance with separation and transfer clearance and account revocation processes for Federal employees and contractors and implement monitoring controls to ensure that all access to CBP systems is revoked in a timely manner.
- Review and, if appropriate, update, disseminate and implement monitoring controls to enforce revised CBP directives to ensure that the process for tracking contractor employees is consistent.
- Review and, if appropriate, update, disseminate, and implement monitoring controls to enforce the physical security and visitor access management policies and procedures to ensure that visitor access to the server room is consistently logged.
- Implement monitoring controls over the account provisioning process to ensure that all users are assigned unique application account identifiers.

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
September 30, 2013

Configuration Management

- Implement the specific vendor-recommended corrective actions detailed in the NFRs that were issued for deficiencies identified during the vulnerability assessment.
- Document and implement a formal access management policy for granting access to CBP application test and environments to ensure that access is consistently and timely documented and authorized.

Contingency Planning

- Implement monitoring controls over backup processes and system configurations to ensure that backups continue to be performed daily.

IT APPLICATION CONTROLS

During the FY 2013 CBP financial statement audit, we identified the following IT application control and financial system functionality deficiency that, when aggregated with the GITC deficiencies, is considered a significant deficiency at CBP:

Finding

- ACS lacks the controls necessary to prevent, or detect and correct excessive drawback claims. Specifically, the programming logic for the system does not link drawback claims to imports at a detailed, line item level. This would potentially allow the importer to receive payment in excess of an allowable amount.

Recommendation

- We recommend that the CBP OCIO and OCFO continue to pursue alternative compensating or automated controls and measures that may ultimately remediate the risk of overpayment and identify the potential revenue loss exposure to CBP. These alternative internal controls over drawback claims may enhance CBP's ability to compare, verify, and track essential information on drawback claims and identify duplicate or excessive drawback claims.

Appendix A
Description of Key CBP Financial Systems and IT Infrastructure
within the Scope of the FY 2013 CBP Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
September 30, 2013

Below is a description of significant CBP financial management systems and supporting IT infrastructure included in the scope of the CBP FY 2013 financial statement audit.

Systems, Applications, and Products (SAP) Enterprise Central Component (ECC)

SAP is CBP's financial system of record. SAP is a major integrated client/server-based financial management system implemented by CBP to manage assets (e.g., budget, logistics, procurement, and related policy) and revenue (e.g., accounting and commercial operations: trade, tariff, and law enforcement), and to provide information for strategic decision making. The SAP instance includes several modules (including ECC 6.0, Intelligent Procurement, and Budget Tools) that provide system functionality for Funds Management, Budget Control, General Ledger, Real Estate, Property, Internal Orders, Sales and Distribution, Special Purpose Ledger, and Accounts Payable functionality, among others. The SAP ECC financial management system was included within the scope of the FY 2013 financial statement audit. The Border Enforcement and Management Systems (BEMS) Program Office and the Enterprise Data Management and Engineering (EDME) Program Office own the SAP application, UNIX and Windows operating systems and Oracle database located in Virginia (VA).

Automated Commercial Environment (ACE)

ACE is the commercial trade processing system being developed and implemented by CBP to replace the Automated Commercial System (ACS). The mission of ACE is to implement a secure, integrated, government-wide system for the electronic collection, use, and dissemination of international trade and transportation data essential to Federal agencies. ACE is a custom-developed, internet-facing, multi-tier system with high availability characteristics, and it processes sensitive data. ACE is being deployed in phases over several years. As a result, some financial modules will remain in the ACS operating environment until they can be developed and deployed in ACE. Since ACE was partially implemented during FY 2013, it was included within the scope of the FY 2013 financial statement audit. The Cargo Systems Program Office (CSPO), the Enterprise Networks and Technology Support (ENTS) Program Office and the EDME Program Office own the ACE application, AIX operating system and DB2 database located in VA.

Automated Commercial System (ACS)

ACS is a collection of seven mainframe-based sub-systems used by the CBP to track, control, and process commercial goods and conveyances entering the United States territory, for the purpose of collecting import duties, fees, and taxes owed to the Federal Government. ACS collects duties at ports, collaborates with financial institutions to process duty and tax payments, and provides automated duty filing for trade clients, and shares information with the Federal Trade Commission on trade violations, illegal imports and terrorist activities. The ACS system was included within the scope of the FY 2013 financial statement audit. The CSPO and the ENTS Program Office own the ACS application and mainframe located in VA.

District of Columbia Metropolitan Local Area Network (DC Metro LAN)

The DC Metro LAN provides CBP's DC area employees and contractors user access to enterprise-wide applications and systems. The mission of the DC Metro LAN is to support the mission of CBP

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
September 30, 2013

operational elements in the DC Metro LAN region of the organization. The boundary of the DC Metro LAN includes tools such as personal computers, laptop computers, printers and file/print servers which enable CBP officers and agents to interact with all other applications and systems in the CBP environment. The DC Metro LAN supports ACE, ACS, and SAP and provides authentication mechanisms that are used by SAP for single sign on capability; as a result, the DC Metro LAN was included within the scope of the FY 2013 financial statement audit. The Field Support Program Office and the EDME Program Office own the DC Metro LAN located in VA.

Appendix B
FY 2013 IT Notices of Findings and Recommendations at CBP

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
 September 30, 2013

FY 2013 NFR # ¹	NFR Title	FISCAM Control Area	New Issue	Repeat Issue	More Significant ²
CBP-IT-13-01	Inappropriately Configured Password Parameters for SAP UNIX Operating System (OS)	Access Controls	X		
CBP-IT-13-02	Audit Activity Logs Not Reviewed for SAP Oracle Database (DB)	Access Controls		X	X
CBP-IT-13-03	Lack of Review of SAP Windows OS Accounts	Access Controls		X	X
CBP-IT-13-04	Incomplete SAP UNIX OS Backups	Contingency Planning	X		
CBP-IT-13-05	Lack of Evidence of Review of SAP UNIX OS Audit Logs	Access Controls	X		X
CBP-IT-13-06	Lack of Review of ACS Application Audit Logs	Access Controls		X	X
CBP-IT-13-07	Security Awareness Issues Identified during After-Hours Physical Security Testing at CBP	Security Management		X	
CBP-IT-13-08	Lack of Review of Developer Access to the ACS Production Application Data	Access Controls		X	X
CBP-IT-13-09	Inappropriately Configured ACE AIX OS Password Parameters	Access Controls	X		
CBP-IT-13-10	Inappropriately Configured ACE DB2 Database Password Parameters	Access Controls	X		
CBP-IT-13-11	Lack of Functionality in the ACS	Business Process Controls		X	X
CBP-IT-13-12	Lack of Review of ACE DB2 Database Accounts	Access Controls	X		X
CBP-IT-13-13	Lack of Annual Recertification of Mainframe Privileged Users	Access Controls		X	
CBP-IT-13-14	Incomplete Raised Floor Visitors Logs	Access Controls	X		

¹ NFR numbers CBP-IT-13-15, CBP-IT-13-21, CBP-IT-13-26, CBP-IT-13-27 and CBP-IT-13-32 were intentionally omitted from sequence.

² NFRs designated as "More Significant" represent control deficiencies that we determined to pose an increased risk to the integrity of CBP financial data.

Department of Homeland Security
Information Technology Management Letter
Customs and Border Protection
 September 30, 2013

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue	More Significant
CBP-IT-13-16	Weaknesses in Creating New DC Metro LAN Accounts	Access Controls		X	
CBP-IT-13-17	Separated Personnel on SAP Application User Listing	Access Controls		X	X
CBP-IT-13-18	Weaknesses in Creating New ACE Accounts	Access Controls		X	X
CBP-IT-13-19	Weaknesses in Creating New ACS Accounts	Access Controls		X	X
CBP-IT-13-20	SAP Configuration Baseline Weaknesses	Configuration Management	X		X
CBP-IT-13-22	Separated Personnel on Mainframe User Listing	Access Controls		X	X
CBP-IT-13-23	Weaknesses in Documenting New ACE User Accounts in the Development and Testing Environments	Configuration Management	X		
CBP-IT-13-24	ACS Segregation of Duties Weaknesses over the Production Environment	Access Controls		X	X
CBP-IT-13-25	Lack of Unique Account Identifiers for ACS	Access Controls	X		
CBP-IT-13-28	ACS Application Recertification Weaknesses	Access Controls	X		X
CBP-IT-13-29	Audit Activity Logs Not Generated or Reviewed for SAP Windows OS	Access Controls	X		X
CBP-IT-13-30	Separated Personnel on DC Metro LAN User Listing	Access Controls		X	
CBP-IT-13-31	Separated Personnel on ACE Application User Listing	Access Controls		X	X
CBP-IT-13-33	Contractor Separation Process Weaknesses	Security Management		X	
CBP-IT-13-34	Weaknesses over the Employee Separation Process	Security Management		X	



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy 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 Financial Officer
Chief Information Officer
Chief Information Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

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](https://twitter.com/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.