Department of Homeland Security

Office of Inspector General

Evaluation of DHS' Information Security Program for Fiscal Year 2013

OIG-14-09

November 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

November 21, 2013

MEMORANDUM FOR: Jeffrey Eisensmith
Chief Information Security Officer

FROM: Frank W. Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2013*

Attached for your information is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2013*. We incorporated the formal comments from the Director, Departmental GAO OIG Liaison Office, in the final report.

The report contains five recommendations aimed at improving the Department's information security program. The Department concurred with all recommendations. Based on information provided in the Department's response to the draft report, we consider recommendations #1 through #5 open and resolved. After the Department has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed upon corrective actions. Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Attachment

Table of Contents

Appendixes

Abbreviations

AO	authorization official
ATO	authority to operate
CBP	United States Customs and Border Protection
CCR	critical control review
CCV	cybersecurity capability validation
CDM	Continuous Diagnostics & Mitigation

CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FNR	Federal Network Resilience
FY	fiscal year
HQ	Headquarters
HSPD-12	Homeland Security Presidential Directorate 12
ICAM PMO	Identity, Credential, and Access Management Program Management Office
ICE	Immigration and Customs Enforcement
ISO	Information Security Office
IT	information technology
MES	mission essential systems
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OA	ongoing authorization
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	plan of action and milestones
RMS	risk management system
SA	security authorization
S&T	Science and Technology Directorate
SOC	Security Operations Center
SP	Special Publication
SPM	Security Process Metrics
TIC	Trusted Internet Connections
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USGCB	United States Government Configuration Baseline
USSS	United States Secret Service

Executive Summary

We conducted an independent evaluation of the Department of Homeland Security (DHS) information security program and practices to comply with the requirements of the *Federal Information Security Management Act*. In evaluating DHS' progress in implementing its agency-wide information security program, we specifically assessed the Department's plans of action and milestones, security authorization processes, and continuous monitoring programs.

DHS continues to improve and strengthen its information security program. During the past year, DHS drafted an ongoing authorization methodology to help improve the security of the Department's information systems through a new risk management approach. This revised approach transitions the Department from a static, paperwork-driven, security authorization process to a dynamic framework that can provide security-related information on demand to make risk-based decisions based on frequent updates to security plans, security assessment reports, and hardware and software inventories.

Additionally, DHS developed and implemented the *Fiscal Year 2013 Information Security Performance Plan* which defines the performance requirements, priorities, and overall goals for the Department throughout the year. DHS has also taken actions to address the Administration's cybersecurity priorities, which include the implementation of trusted internet connections, continuous monitoring, and strong authentication.

While these efforts have resulted in some improvements, components are still not executing all of the Department's policies, procedures, and practices. Our review identified the following more significant exceptions to a strong and effective information security program: (1) systems are being operated without authority to operate; (2) plans of action and milestones are not being created for all known information security weaknesses or mitigated in a timely manner; and (3) baseline security configuration settings are not being implemented for all systems. Additional information security program areas that need improvement include incident detection and analysis, specialized training, account and identity management, and contingency planning. Finally, the Department still needs to consolidate all of its external connections, and complete the implementation of personal identity verification compliant logical access on its information systems and networks.

We are making five recommendations to the Chief Information Security Officer. The Department concurred with all recommendations and has begun to take actions to implement them. The Department's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

Background

Recognizing the importance of information security to the economic and national security interests of the United States, the Congress enacted Title III of the *E-Government Act of 2002* (Public Law 107-347, Sections 301-305) to improve security within the Federal Government. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Title III of the *E-Government Act*, entitled *Federal Information Security Management Act* (FISMA), provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets.

FISMA focuses on the program management, implementation, and evaluation of the security of unclassified and national security systems. As required by FISMA, each Federal agency must develop, document, and implement an agency-wide security program. The security program should protect the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As specified in FISMA, agency heads are charged with conducting an annual evaluation of information programs and systems under their purview, as well as an assessment of related security policies and procedures. Offices of Inspector General (OIG) must independently evaluate the effectiveness of an agency's information security program and practices on an annual basis.

The Office of Management and Budget (OMB) issues updated instructions annually for agency and OIG reporting under FISMA. Our annual FISMA evaluation summarizes the results of our review of DHS' information security program and practices based on the reporting guidance, dated November 30, 2012.

In March 2012, the Cybersecurity Coordinator and Special Assistant to the President identified three Administration priorities and recommended that Federal agencies focus their resources on the most effective controls to improve cybersecurity and the security of Federal information systems.[1] The priority areas include:

- Trusted Internet Connections (TIC) - consolidate external telecommunication connections and ensure a set of baseline security capabilities for situational awareness and enhanced monitoring.
- Continuous Monitoring of Federal information systems - transforms the otherwise static security control assessment and authorization process into a

[1] *Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*, March 7, 2012.

dynamic risk mitigation program that provides essential, near real-time security status and remediation, increasing visibility into systems operations and helping security personnel make risk-management decisions based on increased situational awareness.

- Strong Authentication - passwords alone provide little security. Federal smartcard credentials, such as personal identity verification (PIV) and common access cards provide multi-factor authentication and digital signature and encryption capabilities, authorizing users to access Federal information systems with a higher level of assurance.

By fiscal year (FY) 2013, agencies are required to implement and/or adopt 86 percent of the Administration's government-wide priority cybersecurity capabilities. Specifically, the Administration has identified cross-agency cybersecurity goals for each priority for the entire government. Figure 1 depicts the Administration's government-wide and DHS' implementation goals for each priority for FY 2013.

Figure 1: FY 2013 Administration's Government-wide and DHS Cross-Agency Priority Goals

	TIC Consolidation	TIC Capabilities	Continuous Monitoring	Strong Authentication
Government-wide	**88%**	**92%**	**87%**	**74%**
DHS	**95%**	**95%**	**90%**	**50%**

The Chief Information Security Officer (CISO), who leads the Information Security Office (ISO), is responsible for managing DHS' information security program. To aid in managing its security program, the CISO developed the *Fiscal Year 2013 DHS Information Security Performance Plan* to enhance the Department's information security program and to improve existing processes, such as continuous monitoring. In its FY 2013 performance plan, the CISO defines the information security performance requirements and overall goals for the Department and focuses on five key information security areas, including inventory of systems and assets, information security continuous monitoring, security management, security operations center (SOC) effectiveness, and enterprise initiatives.

DHS uses enterprise management tools to collect and monitor data related to all unclassified and classified ("Secret") plan of action and milestones (POA&M) activities, including weaknesses identified during the security authorization (SA) process and annual self assessments.[2] DHS' enterprise management tools also collect data on other

[2] The National Institute of Standards and Technology (NIST) defines "security authorization" as the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.

FISMA metrics, such as the number of employees who have received information technology (IT) security training. DHS is currently migrating to a new enterprise-wide management system with the goal of streamlining the risk management process by reducing the number of systems used to generate and maintain SA documentation. The transition is expected to be completed by September 2013.

Results of Evaluation

Based on the requirements specified in FISMA and the annual reporting instructions, our independent evaluation focused on 11 key areas of DHS' information security program. Specifically, we reviewed the Department's system inventory, risk management, configuration management, incident response and reporting, security training, POA&M, remote access, identity and access management, continuous monitoring, contingency planning, and security capital planning. We separated the results of our evaluation into these key areas. For each area, we identified any significant progress that DHS has made since our FY 2012 evaluation and issues that need to be addressed to become more successful in the respective information security program area.

Overall Progress

DHS continued to improve its information security program during FY 2013. For example, the CISO—

- implemented a pilot program to migrate the Department from a static paperwork-driven SA process (i.e., security controls are tested and documentation is updated at fixed intervals) to a dynamic framework that can provide authorization officials (AO) access to security-related information on demand (e.g., frequent updates to security plans, security assessment reports, hardware and software inventories, etc.) to make risk-based authorization decisions;

- developed the *Fiscal Year 2013 DHS Information Security Performance Plan* to enhance the Department's information security program and continue to improve existing processes;

- revised the information security scorecard to provide greater focus on risk management and continuous monitoring processes. Specifically, the information security scorecard was divided into two key areas: Continuous Diagnostics & Mitigation (CDM) and Security Processes;[3]

[3] A description of the FY 2013 CDM and security process metrics is included in appendix O.

- updated the DHS Sensitive Systems Policy Directive 4300A to reflect the changes made in various DHS security policies and applicable NIST guidance.

See appendix P for the Department's June 2013 information security scorecard.

Overall Issues To Be Addressed

We identified a number of issues that DHS needs to address to strengthen its security posture. For example, we determined that components are not satisfying all of the Department's information security policies, procedures, and practices. Specifically, we identified deficiencies in component POA&M management, system security authorization, and the consolidation of external network connections. In addition, components have not implemented all system configurations in accordance with DHS policies and procedures. For example, we identified the following deficiencies:

- Components have not incorporated all known information security weaknesses into POA&Ms for the Department's unclassified systems. We reported a similar issue in FY 2012.

- DHS components are continuing to operate information systems with expired authority to operate (ATO). Without a renewed and valid ATO, DHS cannot be assured that effective controls have been implemented to protect the sensitive information stored and processed by these systems.

- Components have not implemented all required United States Government Configuration Baseline (USGCB) settings on the information systems selected for review.

- DHS has not established a formal process to track its external information systems. Currently, external information systems are maintained manually, outside of DHS' enterprise management system. We reported a similar issue in FY 2012.

- Components have not consolidated all of their external connections through an approved DHS TIC.[4] In May 2013, 67 external connections were identified that carry network traffic outside of the DHS TIC.[5]

[4] OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC),* dated November 20, 2007, requires the Federal Government to reduce the number of external connections, including Internet points of presence.

Systems Inventory

DHS continues to maintain and update its FISMA systems inventory, including agency and contractor systems, on an annual basis. In addition, DHS conducts site visits as part of its annual inventory refresh process to engage directly with component personnel, identifying missing systems and resolving any other inventory issues. Furthermore, the new DHS enterprise management system will provide greater functionality, including role-based access control and allow components to develop system security documentation in a more efficient manner.

Progress

- As of May 2013, DHS has a total of 662 information systems that are reported as "operational," which includes a mix of major applications and general support systems that are classified as "Sensitive But Unclassified," "Secret," and "Top Secret."[6]

- DHS adopted a new process to track its mission essential systems (MES), which are vital to ensuring the continuity of essential operations during an emergency event. As of May 2013, DHS has identified 157 MES. Currently, MES are being tracked by the DHS enterprise operations center.

- As of June 2013, DHS has conducted 100 site visits at selected components to ensure its systems inventory is current and accurate.

Issues To Be Addressed

- DHS does not have a central repository to track and monitor information systems that reside in a public cloud.[7] As a result, DHS cannot ensure that it has an accurate inventory or assurance that unaccounted systems have proper security oversight and compliance.

[5] The National Protection and Programs Directorate (NPPD) Federal Network Resilience (FNR) Division conducts annual assessments of Federal agencies' compliance with the OMB TIC Initiative. In the FY 2013 DHS cybersecurity capability validation (CCV) report, FNR reviewed the Department's progress in implementing TIC 2.0 capabilities and external connection consolidation efforts.

[6] For FISMA reporting purposes, DHS' "operational" inventory includes systems in the implementation, modification, and operational system engineering life cycles.

[7] A public cloud is a computing model in which a service provider provides applications, storage, and other services to the general users.

See appendix C for information on DHS' systems inventory and appendix M for status of DHS' Agency Program to Oversee Contractor Systems.

Risk Management Program

DHS requires components to use enterprise-wide tools that incorporate NIST security controls to perform their security authorizations. DHS currently uses the risk management system (RMS) automated tool to provide the basis for the controls to be identified in the various SA documents as well as templates for the SA documents, and its enterprise management tools, to centralize the documents supporting the SA process and ATO for each system.[8]

Components are required to use RMS to apply NIST Special Publication (SP) 800-53 Revision 3 security controls for all system SAs. DHS uses SA artifacts created from RMS and uploaded into its enterprise management tools by the components to monitor their progress in authorizing systems which include:

- Federal Information Processing Standards (FIPS) Publication 199 Categorization;
- Privacy Threshold Analysis and, if required, Privacy Impact Assessment;
- e-Authentication;
- System Plan;
- Contingency Plan;
- Security Assessment Plan;
- Contingency Plan Test Results;
- Security Assessment Report;
- Authorization Decision Letter; and
- Annual Self-Assessments.

Progress

- Four components have met the Department's SA target for FY 2013. For example, OIG, Transportation Security Administration (TSA), United States Citizenship and Immigration Services (USCIS), and United States Customs and Border Protection (CBP) are maintaining SA scores of 92 percent or greater in June 2013.

- Our survey results of selected AOs at seven components [CBP, Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training

[8] During September 2013, DHS expects components to transition to the new enterprise-wide management system to facilitate the risk management and SA process for new systems.

Center (FLETC), Immigration and Customs Enforcement (ICE), United States Coast Guard (USCG), USCIS, and United States Secret Service (USSS)] revealed that officials were informed regularly of potential security threats and/or vulnerabilities to their systems. Specifically, the AOs selected are being provided with relevant security information to make informed risk-based decisions.

Issues To Be Addressed

- As of May 2013, we identified the following deficiencies:
  - 47 systems that are identified as operational have an expired ATO. Specifically, 13 of the 47 systems have been operating without ATO for more than one year.
  - 17 classified "Secret" systems are operating with an expired ATO.
- As of June 2013, the Department's overall score for SA is 79 percent, significantly less than DHS' FY 2013 target of 95 percent. In addition, FEMA, FLETC, and USCG are maintaining SA scores of 71 percent or less.
- As of May 2013, the Department has not performed any quality reviews on the security authorization artifacts to ensure the required security controls are implemented for the Department's "Top Secret" systems.

See appendix D for status on DHS' Risk Management Program.

Plans of Action and Milestones Program

DHS requires components to create and maintain POA&Ms for all known IT security weaknesses. In addition, DHS performs automated quality reviews on its unclassified and classified POA&Ms (i.e., "Secret") for accuracy and completeness and the results are provided to components daily. Despite these efforts, components are not entering and tracking all IT security weaknesses in DHS' unclassified and classified enterprise management tools, or ensuring that all of the data entered are accurate and updated in a timely manner.

Progress

- Components have created POA&Ms for 178 (99 percent) of 180 notices of findings and recommendations for the weaknesses identified during our FY 2012 financial statement audit.[9]

Issues To Be Addressed

- Components are not correcting all deficiencies identified during DHS' POA&M quality reviews. Our review of DHS' quality reports identified repeated deficiencies, such as inaccurate milestones, lack of resources to mitigate the weaknesses, and delays in resolving the POA&Ms that are not being corrected by the components. We identified similar problems in our FY 2011 and FY 2012 FISMA reports.

- DHS does not monitor the adequacy of the POA&Ms for its "Top Secret" systems. For example, DHS has yet to perform any reviews or oversight functions on "Top Secret" POA&Ms that are manually tracked outside of the Department's enterprise management tools. As a result, DHS cannot ensure that POA&Ms have been created to mitigate the security vulnerabilities identified on its "Top Secret" systems and ensure they are managed in accordance with DHS' policies and procedures. We identified this issue in our FY 2012 report.

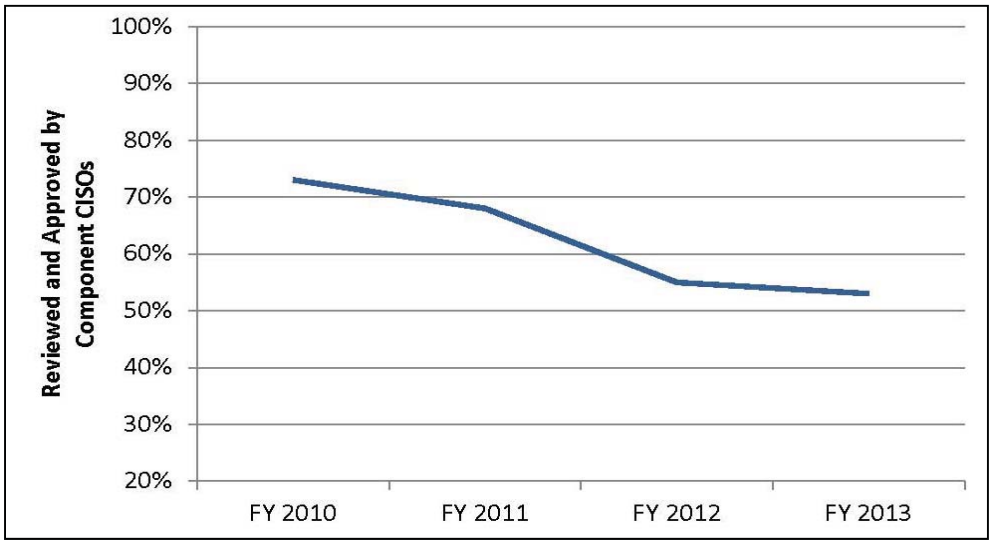
- Our analysis of data from DHS' enterprise management tools revealed that components are not maintaining current information on the progress of security weakness remediation, and not all POA&Ms are being resolved in a timely manner. As of May 31, 2013, we identified the following deficiencies for POA&Ms that are classified as "Sensitive But Unclassified" and "Secret."

    - Components are not monitoring the status of their high priority POA&Ms or reviewing them for consistency and completeness. DHS requires component CISOs to monitor the progress of the POA&M implementation and remediation efforts. Specifically, component CISOs are required to review and approve all priority 4 and priority 5 POA&Ms to ensure that the weaknesses are properly prioritized, and that appropriate resources are identified

[9] *Information Technology Management Letter for the FY 2012 Department of Homeland Security Financial Statement Audit* (OIG-13-58, April 2013).

for remediation.[10] As of May 31, 2013, only 114 (53 percent) of 216 priority 4 and 5 POA&Ms have been reviewed and approved by a component CISO. The decreasing trend of priority 4 and 5 POA&Ms that have been reviewed and approved by component CISOs since FY 2010 is illustrated in figure 2.

Figure 2: Number of Priority 4 and 5 POA&Ms reviewed by Component CISOs



- Component CISOs are not updating information concerning all weaknesses. Of the 3,412 open POA&Ms with estimated completion dates, 496 (15 percent) were delayed by at least 3 months (prior to March 1, 2013). Further, 160 of the delayed POA&Ms had an estimated completion date of more than 1 year old, some dating back to July 2008. In addition, while 15 of open POA&Ms have been designated as significant deficiencies, they have not been identified as material weaknesses as required by DHS POA&M guidance.

- Specifically, 338 (10 percent) of open POA&Ms are scheduled to take more than 2 years to remediate. OMB requires POA&Ms to be completed in a timely manner. In addition, DHS requires that POA&Ms be completed within six months.

[10] According to DHS policy, priority 1 weaknesses are unprioritized, priority 2 weaknesses result from annual assessment findings, and priority 3 weaknesses may result from SA findings. In addition, priority 4 weaknesses are assigned to initial audit findings and priority 5 weaknesses to repeat audit findings.

- DHS requires that POA&M data be monitored and updated on a continuous basis, as events occur. In addition, all information in the POA&M must be updated at least monthly and be accurate on the first day of each month for Department tracking and reporting purposes. We determined that 1,267 POA&Ms (37 percent) of open POA&Ms, have not been updated for 90 days, as of March 1, 2013. Furthermore, 328 POA&Ms have not been updated for a year (i.e., since May 31, 2012).

- DHS requires POA&Ms to be updated at least monthly. However, 40 (45 percent) of 89 open POA&Ms classified as "Secret" have not been updated within the past 90 days. All 40 POA&Ms have not been updated in more than 5 months.

See appendix H for status on DHS' POA&M Program.

Configuration Management

DHS monitors components' compliance with configuration management policies and procedures through the Department's continuous monitoring program. Specifically, components are required to submit configuration and patch management data for Windows XP, Windows Vista, and Windows 7 workstations, monthly. Data is compiled and reported as part of DHS' information security scorecard. However, the information security scorecard does not include configuration management settings for non-Windows assets.

Progress

- According to the DHS Desktop Working Group Office, USSS has migrated to a Windows 7 platform and implemented USGCB configuration settings on its workstations in March 2013.[11]

[11] *DHS Desktop Working Group - Senior Infrastructure Officer Council United States Government Configuration Baseline (USGCB) Compliance Update*, March 27, 2013.

Issues To Be Addressed

- Our audits during the year revealed that components have not fully implemented all of the required DHS and USGCB baseline configuration settings. For example:

  - USCG has not configured its laptops with all required USGCB settings. Specifically, we identified deficiencies related to Telnet, Internet Protocol Version 6 routing protection, and Transmission Control Protocols settings.[12]

  - NPPD had not configured the CyberScope database with all required DHS baseline configuration settings. Specifically, we identified three instances of non-compliance.[13]

- According to the May 2013 information security scorecard, six components (CBP, FEMA, FLETC, ICE, NPPD, and TSA) have received scores of below 65 percent for the configuration management metric. In addition, four components (CBP, FEMA, ICE, and NPPD) received scores of below 65 percent for the patch management metric.

- As of March 2013, CBP has not fully implemented USGCB configuration settings on its workstations and has not established USGCB compliance. Additionally, six components (CBP, FLETC, DHS HQ, OIG, TSA, and USCIS) are still using the Windows XP operating system which may lead to potential security risks as Microsoft will stop providing support to include service packs and updates to mitigate potential security vulnerabilities in 2014.

See appendix E for status on DHS' Configuration Management Program.

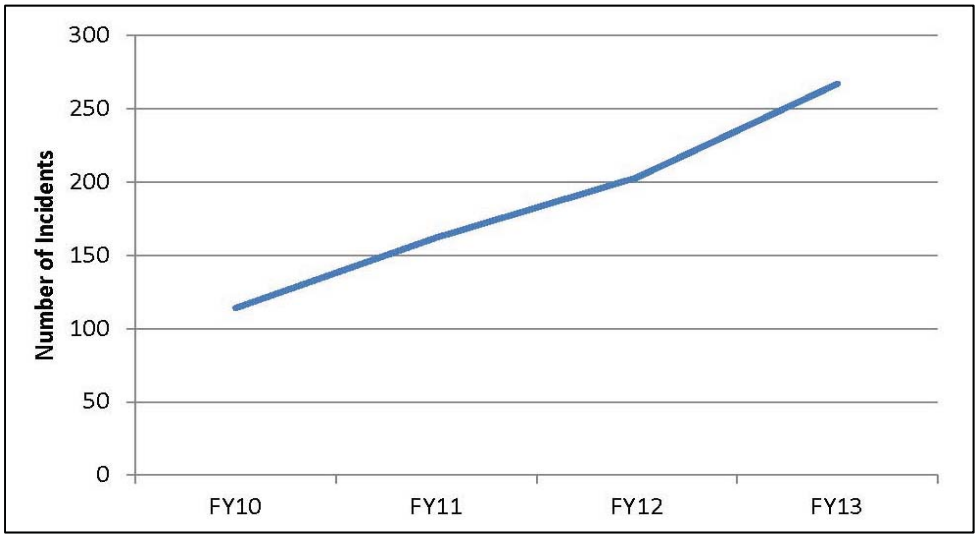
Incident Response and Reporting Program

DHS has established incident detection, handling, and analysis procedures. In addition, the number of all security incidents reported to the DHS SOC has increased by 17 percent from FY 2012 (1,611) to FY 2013 (1,882).[14] As illustrated

[12] *USCG Must Improve the Security and Strengthen the Management of Its Laptops* (OIG-13-93, May 2013).
[13] *DHS Can Take Actions To Address Its Additional Cybersecurity Responsibilities* (OIG-13-95, June 2013).
[14] We evaluated the number of incidents reported by the DHS SOC between October 1 and May 31 for both FY 2012 and FY 2013.

in figure 3, the number of significant malicious logic incidents reported to the DHS SOC has increased by 134 percent from FY 2010 to FY 2013.[15]

Figure 3: Number of Significant Malicious Logic Incidents Reported from FY 2010 - FY 2013



Issues To Be Addressed

- During FY 2013, the Domestic Nuclear Detection Office, FLETC, Office of Intelligence and Analysis, Management, NPPD, OIG, Office of Operations Coordination and Planning, TSA, USCG, and USSS did not consistently submit weekly incident reports to the DHS SOC, as required.

- According to the June 2013 information security scorecard, CBP (70 percent), FEMA (27 percent), ICE (69 percent), and USSS (21 percent) have received a score of less than 80 percent for the incident response metric.

- During FY 2013, CISO added the event management metric to the information security scorecard to track the security alert and logging capabilities of the Department's MES. As of June 2013, four of the nine components (i.e., CBP, FEMA, USCG, and USSS) with MES have received scores of less than 80 percent.

See appendix F for status on DHS' Incident Response and Reporting Program.

[15] Significant malicious logic incidents include critical systems infected by malicious logic (i.e., virus, Trojan, worm, etc.), widespread (10+) infections affecting line of business systems, and malicious logic discovered but not detected by system protective measures.

Security Training Program

The DHS training office continues to oversee component-level security training programs through monthly training status updates and annual site visits. Specifically, the DHS training office verifies that all DHS employees, contractors, and privileged users identified by components receive the required annual IT security awareness and specialized security training accordingly.

Progress

- The DHS training office provides components with access to more than 4,000 IT training courses via Microsoft SharePoint.

Issues to be Addressed

- DHS has not established or provided enterprise-wide training requirements for privileged users. For example, the Department has yet to define the roles and/or functions of a "privileged user." As a result, it may be difficult for components to determine the number of personnel who require specialized training. Furthermore, the type or amount of training required to satisfy specialized security needs has not been standardized throughout the Department.

See appendix G for status on DHS' Security Training Program.

Remote Access Program

DHS has established policies and procedures to mitigate the risks associated with remote access and dial-in capabilities. Specifically, components are responsible for managing all remote access and dial-in connections to their systems through the use of two-factor authentication, enabling audit capabilities, and protecting sensitive information throughout transmission. Overall, components using remote access have developed policies to outline the controls needed to protect remote connections and have implemented mitigating security controls (i.e., multi-factor authentication, firewalls, virtual private network concentrators, etc.) to protect against external threats.

Issues To Be Addressed

- It was reported that DHS' TIC traffic consolidation was below OMB's target of 95 percent for FY 2013. For example, OMB reported that only 72 percent of

DHS' network traffic was consolidated through a TIC, less than the target.[16]

- Components have not consolidated their external network connections to a DHS TIC. For example, 67 external connections were identified that carry network traffic outside of a DHS TIC at CBP, FEMA, FLETC, ICE , NPPD, OIG, Science and Technology (S&T), TSA, USCIS, and USSS, compared to 9 in FY 2012. Further, OIG has 17 external network connections that are not consolidated through an approved DHS TIC access point.[17]

See appendix I for status on DHS' Remote Access Program.

Account and Identity Management Program

DHS' account and identity management program is decentralized. Specifically, each component is using account management software (e.g., Active Directory) to enforce access policies consistent with DHS procedures and guidance. To strengthen security, the Department continues its effort to implement Homeland Security Presidential Directive 12 (HSPD-12) PIV for logical access enterprise wide. However, DHS has made limited progress and is projected to miss the Administration's target goal for Federal agencies.[18] By expediting the implementation of strong authentication with PIV cards and digital signatures in place of traditional passwords, the Department can greatly increase security to its information systems while decreasing the potential of incidents and outside attacks.

Progress

- The Identity, Credential, and Access Management Program Management Office (ICAM PMO) monitors the Department's PIV logical implementation progress at the component level on a monthly basis, which includes the status of PIV hardware and middleware deployed and estimated performance target dates. These figures are incorporated into the monthly DHS information security scorecard.

[16] *Cross Agency Priority Goal: Cybersecurity, FY 2013 Q2 Status Update.*
[17] *Trusted Internet Connections Initiative Department of Homeland Security Cybersecurity Capability Validation Report*, May 10, 2013.
[18] "Mandatory PIV logical access" disallows the use of the traditional user name and password as opposed to "optional PIV logical access," which provides the user the choice of using either method.

- DHS has begun to implement two-factor authentication on its classified Homeland Secure Data Network to reduce anonymity and improve security. This effort is scheduled to be completed by June 2016.

Issues To Be Addressed

- As of May 31, 2013, only two components (DHS Headquarters (HQ) and USCG) have fully implemented mandatory HSPD-12 PIV logical access. The ICAM PMO anticipates 34 percent compliance by the end of FY 2013, less than the Department's and OMB's minimum target of 50 percent for FY 2013.[19]

- The 134 percent increase of significant malicious logic incidents reported between FY 2010 and FY 2013 illustrates the importance of a comprehensive information security program and the need for strong two-factor authentication for logical access to DHS' information systems.

See appendix J for status on DHS' Account and Identity Management Program.

Continuous Monitoring Program

DHS has taken steps to further strengthen its continuous monitoring program. For example, during FY 2013, the CISO drafted the ongoing authorization (OA) methodology to help components improve near real-time risk management, obtain greater efficiencies in resource management, and improve the maintenance of security controls of information systems and data that support the DHS mission. DHS' OA methodology, which was developed based on applicable OMB and NIST's guidance, is a layered approach centered on the: (1) implementation of common controls and reciprocity; (2) continuous monitoring activities and event-driven monitoring; (3) risk mitigation; and (4) risk acceptance.[20]

[19] DHS' PIV logical access compliance progress consists of only "mandatory PIV logical access" implementation.

[20] DHS leveraged NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach* and NIST SP 800-39, *Managing Information Security Risk* to help develop the OA methodology.

Progress

- The CISO is currently piloting the OA methodology at three components (DHS HQ, ICE, and TSA). The pilot program is intended to review and evaluate the process, identify potential challenges, and demonstrate the benefits of OA methodology to the Department.

- As part of its effort to strengthen the Department's enterprise-wide continuous monitoring program, DHS has revised its information security scorecard to provide greater focus on continuous diagnostics and mitigation efforts. Specifically, the metrics include hardware managed assets, software managed assets, anti-virus, patch management, configuration management, vulnerability management, mandatory access, and TIC consolidation.[21]

- During FY 2013, CISO performed 17 critical control reviews (CCR) on selected information systems to ensure that key controls have been implemented and to help components identify potential weaknesses and vulnerabilities.

Issues to Be Addressed

- Our review of the June 2013 information security scorecard identified the following deficiencies:

  - Four components (CBP, FEMA, ICE, and NPPD) have overall CDM scores of 65 percent or lower.

  - The Department has overall scores of 59 percent for patch management and 57 percent for configuration management, significantly less than the FY 2013 target of 90 percent for each.

- DHS has yet to perform any CCRs on its "Top Secret" systems as of June 2013. Consequently, all of DHS' classified systems are not being reviewed independently for potential risks or vulnerabilities. We reported a similar issue in FY 2012.

See appendix K for status on DHS' Continuous Monitoring Program.

[21] A brief description of the FY 2013 CDM metrics can be seen in appendix O.

Contingency Planning Program

DHS maintains an entity-wide business continuity and contingency planning program. However, components have not complied with all of the Department's contingency planning requirements.

Progress

- DHS has updated its policies and procedures for its continuity and contingency planning program. Specifically, DHS developed or updated its continuity plan and continuity directive in October 2012.[22]

- DHS has developed testing and exercise approaches for its business continuity and disaster recovery programs. For example, DHS participated in a national-level exercise to validate the Department's Reconstitution Plan and its capability to define a process to reconstitute following hazardous events in March and April 2013.

Issues To Be Addressed

- While the *DHS Continuity Plan* was finalized in October 2012, the Department is in the process of developing the 15 annexes to the plan to further define component responsibilities on how to execute continuity during any threat or hazardous event.

- As of May 2013, 48 operational systems did not have their contingency plans tested within the last year. DHS requires contingency plans be developed to document the actions that will be taken when a system becomes inoperable due to unexpected circumstances. In addition, contingency plans must be tested annually to ensure that the system can be recovered and key personnel can perform their assigned roles.

See appendix L for status on DHS' Contingency Planning Program.

Security Capital Planning Program

DHS' Capital Planning and Investment Control (CPIC) process is based on OMB's Circular A-11, Part 7 - *Planning, Budgeting, Acquisition, and Management of Capital Assets* which defines the policies for planning, budgeting, acquiring, and

[22] *DHS Continuity Plan*, October 29, 2012 and *Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements*, October 2012.

managing Federal capital assets.[23] DHS' CPIC Guide provides components with policies and procedures for planning, budgeting, managing, and maintaining the Department's portfolio of investments as critical assets for achieving agency strategic goals and missions.[24]

Progress

- DHS issued the *DHS Capital Planning and Investment Control Guide,* version 7.8, in April 2013 to provide components with the latest CPIC guidance from OMB and DHS.

- DHS utilizes OMB Exhibit 53B to track the costs associated with information security tools, training, and testing. In addition, OMB Exhibit 53C is used to identify cloud computing costs, such as public and private cloud expenditures.

Issues To Be Addressed

- DHS is in the process of updating its CPIC guidance to incorporate the latest changes from OMB and the Department. Specifically:

  - As of June 2013, the *DHS Capital Planning & Investment Control OMB Exhibit 300/DHS Guidebook For IT Investments,* version 8.3, has not been finalized. The guide provides agency programs and investment managers with guidance and best practices when preparing OMB Exhibit 300.

  - As of May 2013, the *DHS Instruction Manual 102-02-002-01, Operational Analysis* is still under development. The instruction provides guidance on conducting operational analysis for steady state programs within DHS. Operational analysis evaluates the effectiveness of an investment relating to customer results, strategic and business results, and financial performance. OMB requires that operational analysis be conducted each year on operational capabilities.

See appendix N for status of DHS' Security Capital Planning Program.

[23] OMB's Circular A-11, Part 7 – *Planning, Budgeting, Acquisition, and Management of Capital Assets,* June 2008.
[24] *Department of Homeland Security Capital Planning and Investment Control (CPIC) Guide*, version 7.8, April 2013.

Recommendations

We recommend that the CISO:

Recommendation #1:

Establish a process to ensure that baseline configuration settings are being implemented and maintained on all workstations and servers, including non-Windows platforms.

Recommendation #2:

Ensure that all operational information systems have current authorization to operate.

Recommendation #3:

Improve the ISO's POA&M review process to ensure that all POA&Ms, including "Top Secret" systems, are being remediated timely and in compliance with DHS guidance.

Recommendation #4:

Establish enterprise-wide security training requirements to ensure all privileged users receive necessary role-based specialized security training.

Recommendation #5:

Strengthen the Department's oversight on its "Top Secret" systems by performing critical control reviews on selected systems to ensure the required controls are implemented.

Management Comments and OIG Analysis

Management Comments to Recommendation #1

DHS concurred with recommendation 1. During FY 2013, DHS completed major steps toward achieving this goal. There are 11 out of 12 Components now using the approved baseline configuration settings. The rigor of configuration management will be increased in FY 2014 by expanding relevant scorecard metrics to include devices beyond Windows platforms. The DHS FY 2014 Information Security Scorecard will employ continuous monitoring data feeds

from component tools to monitor the implementation of baseline configuration settings. The scorecard will continue to be used to communicate progress in addressing gaps and ensure continued compliance. Estimated completion date: December 31, 2013.

OIG Analysis

We agree that the steps DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until DHS provides supporting documentation that all planned corrective actions are completed.

Management Comments to Recommendation #2

DHS concurred with recommendation 2. During FY 2013, the DHS ISO procured a new security authorization tool with more dynamic settings to improve stakeholders' visibility into the security posture of operational systems. Also, the FY 2014 Information Security Scorecard will continue monitoring and communicating these systems' authorization statuses. In addition, the introduction of the OA Program in DHS will assist with making authorization activities more efficient and more collaborative with other security activities, such as Continuous Monitoring data collection and analysis. Estimated completion date: December 31, 2013.

OIG Analysis

We agree that the steps DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until DHS provides supporting documentation that all planned corrective actions are completed.

Management Comments to Recommendation #3

DHS concurred with recommendation 3. The DHS ISO will continue to strengthen the POA&M review process to ensure POA&Ms, including those for classified and "Top Secret" systems, are remediated in a timely manner and in compliance with DHS guidance. ISO is exploring options within the automated compliance tool that can be leveraged to improve the POA&M review process. Estimated completion date: February 28, 2014.

OIG Analysis

We agree that the steps DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until DHS provides supporting documentation that all planned corrective actions are completed.

Management Comments to Recommendation #4

DHS concurred with recommendation 4. The DHS ISO will seek to better address privileged user role-based specialized security training requirements in the DHS 4300A, *Sensitive Systems Handbook*. The privileged user training metric in the FY 2014 Performance Plan will be enhanced by tracking specific categories of privileged users such as database administrators or system administrators. Estimated completion date: March 31, 2014.

OIG Analysis

We agree that the steps DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until DHS provides supporting documentation that all planned corrective actions are completed.

Management Comments to Recommendation #5

DHS concurred with recommendation 5. During FY 2014, the DHS ISO will strengthen its oversight of "Top Secret" systems by conducting modified CCRs of select systems. These modified CCRs will act as external "spot checks" that will accompany our currently active on-site quality reviews of SA artifacts of these systems. Estimated completion date: August 31, 2014.

OIG Analysis

We agree that the steps DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until DHS provides supporting documentation that all planned corrective actions are completed.

Appendix A
Objectives, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objective of this review was to determine whether DHS has developed adequate and effective information security policies, procedures, and practices, in compliance with FISMA. In addition, we evaluated DHS' progress in developing, managing, and implementing its information security program.

Our independent evaluation focused on DHS' information security program, the requirements outlined in FISMA, and the FY 2013 FISMA reporting metrics dated November 30, 2012. We conducted our fieldwork at the Departmental level and collected comments from selected AOs at CBP, FEMA, FLETC, ICE, USCG, USCIS, and USSS. In addition, we conducted reviews of DHS' information systems and security program-related areas throughout FY 2013. This report includes the results of a limited number of systems evaluated during the year and our ongoing financial statement review.

As part of our evaluation of DHS' compliance with FISMA, we assessed DHS and its components with the security requirements mandated by FISMA and other Federal information security policies, procedures, standards, and guidelines. Specifically, we: (1) used last year's FISMA independent evaluation as a baseline for this year's evaluation; (2) reviewed policies, procedures, and practices that DHS has implemented at the program and component levels; (3) reviewed DHS' POA&M process to ensure that all security weaknesses are identified, tracked, and addressed; (4) reviewed the processes and status of DHS' department-wide information security program, including system inventory, risk management, configuration management, incident response and reporting, security training, remote access, identity and access management, continuous monitoring, contingency planning, and security capital planning; and, (5) developed our independent evaluation of DHS' information security program.

We conducted this review between April and August 2013 under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B
Management Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 24, 2013

MEMORANDUM FOR: Frank W. Deffer
Assistant Inspector General
Office of Information Technology Audits

FROM: Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Draft Report OIG-13-005-ITA-MGMT: "Evaluation of DHS' Information Security Program for Fiscal Year 2013"

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

DHS is pleased to note OIG's recognition that the Department continues to improve and strengthen its information security program. Specifically, "during the past year, DHS drafted an ongoing authorization (OA) methodology to help improve the security of the Department's information systems through a new risk management approach." This OA methodology will help Components improve near real-time risk management, obtain greater efficiencies in resource management, and improve the maintenance of security controls of information systems and data that support the DHS mission.

In addition, OIG acknowledged that "the Department developed and implemented the *Fiscal Year 2013 Information Security Performance Plan,* which defines the performance requirements, priorities, and overall goals for the Department throughout the year. DHS has also taken actions to address the Administration's Cybersecurity priorities, which included implementation of trusted Internet connections, continuous monitoring of the Department's information systems, and strong authentication."

The draft report contained five recommendations with which the Department concurs. Specifically, OIG recommended that the DHS Chief Information Security Officer:

Recommendation 1: Establish a process to ensure that baseline configuration settings are being implemented and maintained on all workstations and servers, including non-Windows platforms.

Response: Concur. During Fiscal Year (FY) 2013, DHS completed major steps toward achieving this goal. There are 11 out of 12 Components now using the approved baseline configuration settings. The rigor of configuration management will be increased in FY 2014 by

expanding relevant scorecard metrics to include devices beyond Windows platforms. The DHS FY 2014 Information Security Scorecard will employ continuous monitoring data feeds from Component tools to monitor the implementation of baseline configuration settings. The scorecard will continue to be used to communicate progress in addressing gaps and ensure continued compliance. Estimated Completion Date (ECD): December 31, 2013.

Recommendation 2: Ensure that all operational information systems have current authorization to operate.

Response: Concur. During FY 2013, the DHS Information Security Office (ISO) procured a new security authorization tool with more dynamic settings to improve stakeholders' visibility into the security posture of operational information systems. Also, the FY 2014 Information Security Scorecard will continue monitoring and communication of these systems authorization statuses. In addition, the introduction of the OA Program in DHS will assist with making authorization activities more efficient and more collaborative with other security activities, such as Continuous Monitoring data collection and analysis. ECD: December 31, 2013.

Recommendation 3: Improve the ISO's Plans of Action and Milestones (POA&M) review process to ensure that all POA&Ms, including "Top Secret" systems, are being remediated timely and in compliance with DHS guidance.

Response: Concur. The DHS ISO will continue to strengthen the POA&M review process to ensure POA&Ms, including those for classified and Top Secret systems, are remediated in a timely manner and in compliance with DHS guidance. ISO is exploring options within the new automated compliance tool that may be leveraged to improve the POA&M review process. ECD: February 28, 2014.

Recommendation 4: Establish enterprise-wide security training requirements to ensure all privileged users receive necessary role-based specialized security training.

Response: Concur. The DHS ISO will seek to better address privileged user role-based specialized security training requirements in the DHS 4300A, "Sensitive Systems Handbook." The privileged user training metric in the FY 2014 Performance Plan will be enhanced by tracking specific categories of privileged users such as database administrators or system administrators. ECD: March 31, 2014.

Recommendation 5: Strengthen the Department's oversight on its "Top Secret" systems by performing critical control reviews on selected systems to ensure the required controls are implemented.

Response: Concur. During FY 2014, the DHS ISO will strengthen its oversight over Top Secret systems by conducting modified critical control reviews of select systems. These modified critical control reviews will act as external "spot checks" that will accompany our currently active on-site quality reviews of security authorization artifacts of these systems. ECD: August 31, 2014.

2

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

3

Appendix C
System Inventory

Question 1: System Inventory
1. Identify the number of agency and contractors' systems by component and FIPS Pub 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your agency but owned by another Federal agency (i.e., ePayroll, etc.) by component and FIPS Pub 199 impact level.
Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing
2. For the Total Number of Systems identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems) (Column A + Column B)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS Pub 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
CBP	High	18	2	0	0	18	2	18	100%	17	94%	17	94%
	Moderate	68	2	2	0	70	2	70	100%	70	100%	67	96%
	Low	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Undefined	1	0	0	0	1	0	0	0%	0	0%	0	0%
	Sub-total	**88**	**4**	**2**	**0**	**90**	**4**	**89**	**99%**	**88**	**98%**	**85**	**94%**
DHS HQ	High	13	0	3	0	16	0	14	88%	6	38%	16	100%
	Moderate	25	1	10	0	35	1	33	94%	15	43%	33	94%

	Low	0	0	4	0	4	0	3	75%	3	75%	4	100%
	Undefined	0	0	3	0	3	0	0	0%	0	0%	2	67%
	Sub-total	**38**	**1**	**20**	**0**	**58**	**1**	**50**	**86%**	**24**	**41%**	**55**	**95%**
FEMA	High	21	3	2	0	23	3	20	87%	9	39%	19	83%
	Moderate	38	2	12	0	50	2	38	76%	26	52%	34	68%
	Low	5	0	0	0	5	0	4	80%	1	20%	2	40%
	Undefined	10	0	0	0	10	0	5	50%	5	50%	5	50%
	Sub-Total	**74**	**5**	**14**	**0**	**88**	**5**	**67**	**76%**	**41**	**47%**	**60**	**68%**
FLETC	High	0	0	0	0	0	0	0	-	0	-	0	-
	Moderate	12	0	2	0	14	0	14	100%	9	64%	12	86%
	Low	0	0	0	0	0	0	0	-	0	-	0	-
	Undefined	0	0	0	0	0	0	0	-	0	-	0	-
	Sub-total	**12**	**0**	**2**	**0**	**14**	**0**	**14**	**100%**	**9**	**64%**	**12**	**86%**
ICE	High	10	0	1	0	11	0	11	100%	3	27%	11	100%
	Moderate	31	1	11	0	42	1	41	98%	10	24%	35	83%
	Low	2	0	0	0	2	0	1	50%	0	0%	2	100%
	Undefined	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Sub-total	**44**	**1**	**12**	**0**	**56**	**1**	**54**	**96%**	**14**	**25%**	**49**	**88%**
NPPD	High	6	1	5	0	11	1	11	100%	11	100%	11	100%
	Moderate	9	0	10	0	19	0	19	100%	18	95%	17	89%
	Low	1	0	2	0	3	0	3	100%	3	100%	3	100%
	Undefined	2	0	0	0	2	0	2	100%	2	100%	2	100%
	Sub-total	**18**	**1**	**17**	**0**	**35**	**1**	**35**	100%	**34**	**97%**	**33**	**94%**
OIG	High	2	0	0	0	2	0	2	100%	1	50%	1	50%
	Moderate	0	0	0	0	0	0	0	-	0	-	0	-
	Low	0	0	0	0	0	0	0	-	0	-	0	-
	Undefined	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Sub-total	**3**	**0**	**0**	**0**	**3**	**0**	**3**	**100%**	**2**	**67%**	**2**	**67%**
S&T	High	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Moderate	13	0	11	0	24	0	24	100%	15	63%	23	96%
	Low	1	0	1	0	2	0	2	100%	1	50%	1	50%
	Undefined	2	0	0	0	2	0	1	50%	1	50%	0	0%
	Sub-total	**17**	**0**	**12**	**0**	**29**	**0**	**28**	**97%**	**18**	**62%**	**25**	**86%**

TSA	High	21	0	0	0	21	0	21	100%	21	100%	20	95%
	Moderate	36	1	13	0	49	1	49	100%	49	100%	49	100%
	Low	6	0	2	0	8	0	8	100%	8	100%	8	100%
	Undefined	5	0	0	0	5	0	5	100%	5	100%	5	100%
	Sub-total	**68**	**1**	**15**	**0**	**83**	**1**	**83**	**100%**	**83**	**100%**	**82**	**99%**
USCG	High	8	1	5	1	13	2	13	100%	5	38%	8	62%
	Moderate	70	3	18	1	88	4	65	74%	48	55%	55	63%
	Low	7	0	2	0	9	0	6	67%	5	56%	5	56%
	Undefined	36	0	1	0	37	0	25	68%	28	76%	24	65%
	Sub-total	**121**	**4**	**26**	**2**	**147**	**6**	**109**	**74%**	**86**	**59%**	**92**	**63%**
USCIS	High	2	0	3	0	5	0	4	80%	5	100%	5	100%
	Moderate	21	0	15	0	36	0	34	94%	24	67%	36	100%
	Low	0	0	1	0	1	0	0	0%	0	0%	1	100%
	Undefined	0	0	0	0	0	0	0	-	0	-	0	-
	Sub-total	**23**	**0**	**19**	**0**	**42**	**0**	**38**	**90%**	**29**	**69%**	**42**	**100%**
USSS	High	6	0	0	0	6	0	5	83%	3	50%	5	83%
	Moderate	11	0	0	0	11	0	11	100%	6	55%	11	100%
	Low	0	0	0	0	0	0	0	-	0	-	0	-
	Undefined	0	0	0	0	0	0	0	-	0	-	0	-
	Sub-total	**17**	**0**	**0**	**0**	**17**	**0**	**16**	**94%**	**9**	**53%**	**16**	**94%**
Agency Totals	**High**	**108**	**7**	**19**	**1**	**127**	**8**	**120**	**94%**	**82**	**65%**	**114**	**90%**
	Moderate	**334**	**10**	**104**	**1**	**438**	**11**	**398**	**91%**	**290**	**66%**	**372**	**85%**
	Low	**23**	**0**	**12**	**0**	**35**	**0**	**28**	**80%**	**22**	**63%**	**27**	**77%**
	Undefined	**58**	**0**	**4**	**0**	**62**	**0**	**40**	**65%**	**43**	**69%**	**40**	**65%**
	Total	**523**	**17**	**139**	**2**	**662**	**19**	**586**	**89%**	**437**	**66%**	**553**	**84%**

Appendix D
Status of Risk Management Program

Section 2: Status of Risk Management Program	
	Response:
Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.** **2. Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.** **3. Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.** **4. Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.** **5. Has an up-to-date system inventory.** **6. Categorizes information systems in accordance with government policies.** **7. Selects an appropriately tailored set of baseline security controls.** **8. Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.** **9. Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.** **10. Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.** **11. Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.** **12. Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.** **13. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).** **14. Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks.** **15. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies (NIST SP 800-18 Rev.1, 800-37 Rev. 1).** **16. Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.**	✓

Comments:	

Appendix E
Status of Configuration Management Program

Section 3: Status of Configuration Management Program	
	Response:
Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for configuration management.** **2. Defined standard baseline configurations.** **3. Assessments of compliance with baseline configurations.** **4. Process for timely (as specified in organization policy or standards) remediation of scan result deviations.** **5. For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.** **6. Documented proposed or actual changes to hardware and software configurations.** **7. Process for timely and secure installation of software patches.** **8. Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53 Rev. 3: RA-5, SI-2).** **9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53 Rev. 3: CM-4, CM-6, RA-5, SI-2).** **10. Patch management process is fully developed, as specified in organization policy or standards (NIST SP 800-53 Rev. 3: CM-3, SI-2).**	✓
Comments:	

Appendix F
Status of Incident Response and Reporting Program

Section 4: Status of Incident Response & Reporting Program	
	Response:
Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53 Rev. 3: IR-1). Defined standard baseline configurations.** **2. Comprehensive analysis, validation, and documentation of incidents.** **3. When applicable, reports to US-CERT within established timeframes (NIST SP 800-53 Rev. 3, 800 61 Rev. 2; OMB M-07 16, M-06-19).** **4. When applicable, reports to law enforcement within established timeframes (SP 800-61 Rev. 2).** **5. Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53 Rev. 3, 800-61 Rev. 2; OMB M-07-16, M-06-19).** **6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.** **7. Is capable of correlating incidents.** **8. Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53 Rev. 3, 800-61 Rev. 2; OMB M-07-16, M-06-19).**	✓
Comments:	

Appendix G
Status of Security Training Program

Section 5: Status of Security Training Program	
	Response:
Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for security awareness training (NIST SP 800-53 Rev. 3: AT-1).** **2. Documented policies and procedures for specialized training for users with significant information security responsibilities.** **3. Security training content based on the organization and roles, as specified in organization policy or standards.** **4. Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.** **5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.** **6. Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53 Rev. 3).**	✓
Comments:	

Appendix H
Status of Plans of Actions and Milestones Program

Section 6: Status of Plans of Actions & Milestones (POA&M) Program	
	Response:
Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.** **2. Tracks, prioritizes, and remediates weaknesses.** **3. Ensures remediation plans are effective for correcting weaknesses.** **4. Establishes and adheres to milestone remediation dates.** **5. Ensures resources and ownership are provided for correcting weaknesses.** **6. POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).** **7. Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3; OMB M 04-25).** **8. Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25).**	✓
Comments:	

Appendix I
Status of Remote Access Program

Section 7: Status of Remote Access Program	
	Response:
Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53 Rev. 3: AC-1, AC-17).** **2. Protects against unauthorized connections or subversion of authorized connections.** **3. Users are uniquely identified and authenticated for all access (NIST SP 800-46 Rev. 1, Section 4.2, Section 5.1).** **4. Telecommuting policy is fully developed (NIST SP 800-46 Rev. 1, Section 5.1).** **5. If applicable, multi-factor authentication is required for remote access (NIST SP 800-46 Rev. 1, Section 2.2, Section 3.3).** **6. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.** **7. Defines and implements encryption requirements for information transmitted across public networks.** **8. Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.** **9. Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46 Rev. 1, Section 4.3; US-CERT Incident Reporting Guidelines).** **10. Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53 Rev. 3, PL-4).** **11. Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46 Rev. 1, Section 5.1; NIST SP 800-53 Rev. 3, PS-6).**	✓
Comments:	

Appendix J
Status of Account and Identity Management Program

Section 8: Status of Account and Identity Management Program	
	Response:
Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for account and identity management (NIST SP 800-53 Rev. 3: AC-1).** **2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53 Rev. 3, AC-2).** **3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary.** **4. If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53 Rev. 3, IA-2).** **5. Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).** **6. Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).** **7. Ensures that the users are granted access based on needs and separation-of duties principles.** **8. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.)** **9. Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)** **10. Ensures that accounts are terminated or deactivated once access is no longer required.** **11. Identifies and controls use of shared accounts.**	✓
Comments:	

Appendix K
Status of Continuous Monitoring Program

Section 9: Status of Continuous Monitoring Program	
	Response:
Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for continuous monitoring (NIST SP 800-53 Rev. 3: CA-7).** **2. Documented strategy and plans for continuous monitoring (NIST SP 800-37 Rev. 1, Appendix G).** **3. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53 Rev. 3, 800-53A Rev. 1).** **4. Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53 Rev. 3, 800-53A Rev. 1).**	✓
Comments:	

Appendix L
Status of Contingency Planning Program

Section 10: Status of Contingency Planning Program	
	Response:
Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53 Rev. 3: CP-1).** **2. The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34 Rev. 1).** **3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34 Rev. 1).** **4. Testing of system-specific contingency plans.** **5. The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34 Rev. 1).** **6. Development of test, training, and exercise programs (FCD1, NIST SP 800-34 Rev. 1, NIST SP 800-53 Rev. 3).** **7. Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.** **8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34 Rev. 1).** **9. Systems that have alternate processing sites (FCD1, NIST SP 800-34 Rev. 1, NIST SP 800-53 Rev. 3).** **10. Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34 Rev. 1, NIST SP 800-53 Rev. 3).** **11. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34 Rev. 1, NIST SP 800-53 Rev. 3).** **12. Contingency planning that considers supply chain threats.**	✓
Comments:	

Appendix M
Status of Agency Program To Oversee Contractor Systems

Section 11: Status of Agency Program to Oversee Contractor Systems	
	Response:
Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.** **2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53 Rev. 3: CA-2).** **3. A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.** **4. The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53 Rev. 3: PM-5).** **5. The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.** **6. The inventory of contractor systems is updated at least annually.** **7. Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.**	✓
Comments:	

Appendix N
Status of Security Capital Planning Program

Section 12: Status of Security Capital Planning Program	
	Response:
Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes? **1. Documented policies and procedures to address information security in the CPIC process.** **2. Includes information security requirements as part of the capital planning and investment process.** **3. Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53 Rev. 3: SA-2).** **4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53 Rev. 3: PM-3).** **5. Ensures that information security resources are available for expenditure as planned.**	✓
Comments:	

Appendix O
FY 2013 Information Security Scorecard Metric Descriptions

Metric	Description
CDM Metrics	
Hardware Managed Assets	Hardware assets scanned.
Software Managed Assets	Software (application) assets scanned.
Whitelisting	Not evaluated during FY 2013.
Anti-Virus	Windows assets with anti-virus installed within past 30 days.
Patch Management	Windows assets with patches applied within past 60 days.
Configuration Management	Windows workstations providing common configuration enumerations.
Vulnerability Management	Number of vulnerabilities per asset.
Mandatory Access	Percentage of mandatory PIV users.
TIC Consolidation	External connections secured through a TIC access point as tracked by traffic utilization.
Overall CDM Score	Aggregated weighted CDM metric scores.
Security Process Metrics (SPM)	
Systems	Total number of sensitive but unclassified and classified systems.
MES	Total number of MES.
Security Authorization	Percentage of systems with validated SA packages.
Privacy	Percentage of systems with validated privacy documentation.
Weakness Remediation	Percentage of POA&Ms neither overdue, delayed, or incomplete.
Training	Percentage of users compliant with annual training requirements.
Event Management	Percentage of MES providing logs or alerts to the appropriate SOC.
Incident Response	Number of hours a security event notification remains open before being closed or escalated.
Overall SPM Score	Aggregated weighted SPM scores.

Appendix P
June 2013 Information Security Scorecard

Department of Homeland Security
FY13 Information Security Scorecard – Security Processes
June 2013

METRIC	CBP	DHS HQ	FEMA	FLETC	ICE	NPPD	OIG	S&T	TSA	USCG	USCIS	USSS	Monthly Threshold*	FY13 Target	DHS
Total Systems	91	57	91	14	56	35	3	30	83	148	42	17	N/A	N/A	667
Security Authorization	92%	88%	56%	71%	89%	80%	100%	87%	100%	63%	93%	82%	Green: 90% Yellow: 80%	95%	79%
Privacy Documentation	38%	91%	70%	100%	80%	97%	100%	96%	99%	75%	76%	82%	N/A	N/A	77%
Weakness Remediation	87%	97%	76%	81%	93%	97%	100%	85%	85%	80%	91%	88%	Green: 90% Yellow: 80%	95%	87%
Training	80%	99%	90%	92%	99%	100%	92%	82%	97%	86%	66%	92%	Green: 80% Yellow: 70%	95%	87%
Event Management	77%	88%	0%	100%	100%	90%	100%	100%	88%	57%	92%	50%	Green: 90% Yellow: 80%	100%	66%
Incident Response	70%	100%	27%	100%	69%	100%	100%	100%	98%	100%	100%	21%	Green: 90% Yellow: 80%	90%	87%
Overall SPM Score	84%	92%	51%	85%	92%	90%	98%	89%	96%	72%	92%	72%	Green: 80% Yellow: 70%	90%	80%

Appendix Q
Major Contributors to This Report

Chiu-Tong Tsang, Director
Aaron Zappone, Team Lead
Michael Kim, IT Auditor
Pachern Thapanawat, IT Auditor

Appendix R
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
Chief Information Officer
Acting Chief Information Security Officer
Acting Director, Compliance and Oversight, Office of CISO
Chief Information Officer Audit Liaison
Chief Information Security Officer Audit Liaison
Component Chief Information Officers
Component Chief Information Security Officers

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.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.