# Department of Homeland Security
# Office of Inspector General

## Evaluation of
## DHS' Information Security Program for
## Fiscal Year 2012

OIG-13-04

October 2012

**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

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

October 24, 2012

MEMORANDUM FOR: Emery Csulak
Acting Chief Information Security Officer

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

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2012*

Attached for your action is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2012.* We incorporated the formal comments from the Director, Departmental GAO-OIG Liaison Office, in the final report.

The report contains six recommendations aimed at improving the Department's information security program. The Department concurred with all recommendations. As prescribed by the Department of Homeland Security Directive 077-1, Follow-Up and Resolutions for the Office of Inspector General Report Recommendations, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing 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

| | |
|---|---|
| ATO | Authority to Operate |
| CBP | Customs and Border Protection |
| 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* |
| 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 |
| ISSO | Information System Security Officer |
| IT | information technology |
| MGMT | Management Directorate |
| NIST | National Institute of Standards and Technology |
| NPPD | National Protection and Programs Directorate |
| 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 |
| S&T | Science and Technology Directorate |
| SA | System Administrator |
| SOC | Security Operations Center |
| SP | Special Publication |
| 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. We performed fieldwork at both the program and component levels.

DHS continues to improve and strengthen its security program. During the past year, DHS developed and implemented the *Fiscal Year 2012 Information Security Performance Plan* to focus on areas that the Department would like to improve upon throughout the year. Specifically, DHS identified in the performance plan several key elements that are indicative of a strong security program, such as plans of action and milestones weakness remediation. In addition, DHS has taken actions to address the Administration's cybersecurity priorities, which include implementing trusted Internet connections, continuously monitoring DHS information systems, and employing personal identity verification compliant credentials to improve logical access for its systems.

While these efforts have resulted in some improvements, components still are not executing all of the Department's policies, procedures, and practices. In addition, our review identified the following more significant exceptions to a strong and effective information security program: (1) systems are being authorized though key information is missing or outdated; (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 configurations 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 (1) consolidate all of its external connections, (2) implement a near-real-time monitoring capability, and (3) employ personal identity verification compliant cards for logical access on its information systems.

We are making six 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

Due to the increasing threat to information systems and the highly networked nature of the Federal computing environment, Congress, in conjunction with the Office of Management and Budget (OMB), requires an annual review and reporting of agencies' compliance with *Federal Information Security Management Act* (FISMA) requirements. FISMA focuses on the program management, implementation, and evaluation of the security of unclassified and national security systems.

Recognizing the importance of information security to the economic and national security interests of the United States, 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 FISMA, provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets.

FISMA requires each Federal agency to 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 Generals (OIG) must independently evaluate the effectiveness of an agency's information security program and practices on an annual basis.

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 draft reporting guidance dated March 6, 2012.[1]

In March 2012, the Cybersecurity Coordinator and Special Assistant to the President identified three Administration priorities and recommended that Federal agencies focus

[1] On October 2, 2012, OMB issued Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

their resources on the most effective controls to improve cybersecurity and the security of Federal information systems:[2]

- **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 dynamic risk mitigation program that provides essential, near real-time security status and remediation, increasing visibility into system 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.

The Administration's goal is that, by the end of 2014, Federal agencies will achieve 95 percent utilization of critical Administration cybersecurity capabilities on Federal information systems, including TIC, continuous monitoring, and strong authentication. The Administration's priorities are integrated with other Federal cybersecurity activities, including OMB's fiscal year (FY) 2011 FISMA report and FY 2012 FISMA metrics.

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 2012 DHS Information Security Performance Plan* to enhance DHS' information security program and continued to improve existing processes, such as continuous monitoring of its information systems, system security authorizations, and plan of action and milestones (POA&M) remediation. DHS uses enterprise management tools[3] to collect and track data related to all unclassified and classified POA&M activities, including weaknesses identified during self-assessments and the security authorization process.[4] DHS'

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

[3] DHS enterprise management tools collect and track only Sensitive But Unclassified and Secret POA&M data.

[4] According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 - *Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life*

enterprise management tools also collect data on other FISMA metrics, such as the number of systems that have implemented DHS' security baseline configurations and the number of employees who have received information technology (IT) security training.

## Results of Evaluation

Based on the requirements outlined 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 across 10 components and offices.[5] We separated the results of our evaluation into these key areas. For each area, we identified the progress that DHS has made since our FY 2011 evaluation and any issues that DHS needs to address to become more successful in the respective information security program area.

### Overall Progress

DHS continued to improve its information security program during FY 2012. For example, the CISO:

- Developed the *Fiscal Year 2012 DHS Information Security Performance Plan* to enhance DHS' information security program and continue to improve existing processes, such as continuous monitoring, POA&M, and security authorization.

- Updated the Department's baseline IT security policies and procedures in DHS Sensitive Systems Policy Directive 4300A and its companion, DHS 4300A Sensitive Systems Handbook, to reflect the changes made in DHS security policies and various NIST guidance.

*Cycle Approach*, Revision 1, security authorization is 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.

[5] Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), Immigration and Customs Enforcement (ICE), Management Directorate (MGMT), National Protection and Programs Directorate (NPPD), Science and Technology Directorate (S&T), Transportation Security Administration (TSA), United States Citizenship and Immigration Services (USCIS), United States Coast Guard (USCG), and United States Secret Service (USSS).

- In April 2012, the DHS CISO issued its second *State of Cybersecurity at The Department of Homeland Security* report. The report outlines how DHS anticipates and addresses emerging security risks from new technology products and advanced threat actor techniques, including its new initiatives and programs that ensure a secure computing environment within the Department. The report presents relevant information to employees for protecting their information and increasing the Department's cybersecurity awareness.

- The overall quality of security authorization documentation continues to improve in FY 2012. Compared with FY 2011, we identified fewer deficiencies in the security authorization documentation for the systems that were selected for review.

## Overall Issues To Be Addressed

Despite the actions taken by the CISO to improve the Department's overall information security program, we identified several issues that should be addressed to strengthen DHS' 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 with component POA&M management, system security authorization, and continuous monitoring. In addition, components have not implemented all of the information system baseline configurations in accordance with DHS policies and procedures. For example, we identified the following deficiencies:

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

- Components have not incorporated all known information security weaknesses into POA&Ms for the Department's unclassified systems.

- Artifacts supporting the authorization of selected systems were either missing key information or outdated, which restricts the ability of authorizing officials to make credible risk-based decisions.

- DHS has not established a formal process to track its external information systems and cloud-based systems inventory. Currently, external information systems and cloud-based systems are maintained manually, outside of the DHS systems' enterprise management inventory tools.

- As part of DHS' Cybersecurity Capability Validation assessment conducted in April 2012, the National Cyber Security Division's[6] Federal Network Security branch reported that nine external connections are not consolidated through an approved TIC access point.[7] As required under OMB's *Implementation of Trusted Internet Connections (TIC)* memorandum, the Federal Government shall reduce the number of external connections, including Internet points of presence.[8]

- DHS has not provided adequate oversight on its contractor-hosted websites to ensure that these external information systems are tested annually and that effective security controls have been implemented.

## System 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 update process.

### Progress

- As of June 2012, DHS has a total of 675 systems, which include a mix of major applications and general support systems that are categorized as Sensitive But Unclassified, Secret, or Top Secret.

- As of June 2012, DHS has conducted 71 component site visits as part of its annual refresh process, which includes providing components with additional guidance in the discovery of new systems, identification of system boundaries, and the resolution of any other inventory issues.

### Issues To Be Addressed

[6] The National Cyber Security Division, which is a division under the Office of Cybersecurity and Communications within NPPD, is responsible for implementing OMB's TIC initiative for the Federal Government.

[7] *Trusted Internet Connection Initiative Department of Homeland Security Cybersecurity Capability Validation Report*, April 2012.

[8] OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC),* November 20, 2007.

- As of July 2012, DHS has not established an automated capability to track the hardware devices and software deployed at all component sites.

See appendix C for information on DHS' system inventory and appendix M for the 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 uses the risk management system (RMS) automated tool to provide the basis for the controls to be identified in the various security authorization documents as well as templates for the security authorization documents, and its enterprise management tools to centralize the documents supporting the security authorization process and authority to operate (ATO) for each system.

Components are required to use RMS to apply NIST SP 800-53 security controls for all system self-assessments. DHS uses security authorization artifacts created from RMS and uploaded into its enterprise management tools by the components to monitor their progress in authorizing systems, including the following:

- Federal Information Processing Standards (FIPS) 199 Categorization
- Privacy Threshold Analysis and, if required, Privacy Impact Assessment
- e-Authentication
- Security Plan
- Contingency Plan
- Security Assessment Plan
- Contingency Plan Test Results
- Security Assessment Report
- Authorization Decision Letter which includes an updated Security Plan, POA&M, and Security Assessment Report
- Annual Self-Assessments

For some of the systems that were granted ATO, the artifacts that are required to support the authorization were missing, incomplete, or outdated. We identified a similar issue in our FY 2010 and FY 2011 FISMA reports.[9]

[9] *Evaluation of DHS' Information Security Program for Fiscal Year 2010* (OIG-11-01, October 2010), *Evaluation of DHS' Information Security Program for* Fiscal Year *2011* (OIG-11-113, September 2011).

**Progress**

- The overall quality of security authorization documentation has continued to improve in FY 2012. For example, compared with FY 2011, we identified fewer deficiencies within the security authorization documentation for the systems that were selected for review.

**Issues To Be Addressed**

- We selected 25 systems (20 Sensitive But Unclassified, 5 Secret) from 10 components and offices to evaluate the quality of documents that support DHS' security authorization process. For some of the systems that were granted ATO, the artifacts that are required to support the authorization were missing, incomplete, or outdated. Without this information, agency officials cannot make credible, risk-based decisions on whether to authorize the system to operate. Specifically, we determined that:

  ➢ For 17 security plans, certain elements within the plans are missing, including sections that describe operational and configuration security controls.

  ➢ Two systems did not have completed or updated FIPS-199 categorization worksheets. The FIPS-199 determination, when applied properly during the risk assessment process, helps agency officials to select applicable controls for the information systems.

  ➢ Six classified systems are operating with an expired ATO. Some of these systems have been operating without an ATO since 2007.

  ➢ Two systems did not have the outstanding risks and/or acceptance of those risks documented in the authorization decision letter and/or POA&M.

  ➢ Two systems had outdated or nonexistent memorandums of understanding with organizations (external to the component) with which they are sharing data.

  ➢ One system did not have a completed and approved privacy impact assessment.

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 reviews on its unclassified and classified POA&Ms for accuracy and completeness and provides the results 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 all notices of findings and recommendations for the weaknesses identified during our FY 2011 financial statement audit.

### 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 2010 and FY 2011 FISMA reports.

- DHS did not monitor the adequacy of the POA&Ms for its Top Secret systems. For example, DHS did not 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 that they are managed in accordance with the Department's policies and procedures. We identified this issue in our FY 2011 report.

- Based on our analysis of data from DHS' enterprise management tools, component CISOs and information system security officers 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 June 30, 2012, we identified the following deficiencies for POA&Ms that are classified as Sensitive But Unclassified and Secret.

Sensitive But Unclassified POA&Ms

- 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 for remediation.[10] As of June 30, 2012, only 132 (55 percent) of 241 priority 4 and 5 POA&Ms have been reviewed and approved by a component CISO.

- Component CISOs are not updating information concerning all weaknesses. Of the 4,377 open POA&Ms with estimated completion dates, 348 (8 percent) were delayed by at least 3 months (prior to April 1, 2012). Further, 127 POA&Ms had an estimated completion date more than 1 year old, dating as far back as March 2008. In addition, while 36 POA&Ms have been designated as significant deficiencies, they have not been identified as material weaknesses as required by DHS POA&M guidance.

- DHS requires that a reasonable resources estimate of at least $50 be provided to mitigate the weakness identified. Resources required for the remediation of 81 (2 percent) of 4,377 open POA&Ms either were not identified or did not meet the $50 requirement. Further, 307 (7 percent) of open POA&Ms are scheduled to take more than 2 years to mitigate the weaknesses. DHS and OMB require POA&Ms to be completed timely.

- 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 1,245 POA&Ms, or 28 percent of open POA&Ms, have not been updated for 90 days as of June 30, 2012. Further, 157 POA&Ms have not been updated for a year (i.e., since June 30, 2011).

[10] Priority 4 weaknesses can be assigned to initial audit findings and priority 5 weaknesses to repeat audit findings.

- DHS requires components to develop a POA&M for its operational systems that have not received an ATO. We identified five instances where POA&Ms have not been created for operational systems that have not received an ATO.

Secret POA&Ms

- DHS and OMB require POA&Ms to be completed timely. However, we identified 40 (98 percent) of 41 open POA&Ms that are currently delayed. Further, 35 (88 percent) of the 40 POA&Ms have been delayed by at least 3 months (prior to April 1, 2012), including 12 (30 percent) POA&Ms that have been delayed by more than 1 year (prior to June 30, 2011).

- Thirty-seven (90 percent) of 41 open POA&Ms have not been updated within the past 90 days. Twelve of the 37 POA&Ms have not been updated in more than 1 year. DHS requires POA&Ms to be updated at least monthly.

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

### Configuration Management

We evaluated the compliance with USGCB requirements on Windows workstations at CBP, DHS Headquarters (HQ), FEMA, ICE, NPPD, TSA, USCG, USCIS, and USSS. Results from our testing indicated that components have not implemented all required DHS baseline configuration settings. We reported a similar issue in our FY 2010 and FY 2011 reports.

Additionally, we reviewed the servers and databases of nine systems that are categorized as high potential impact and contain personal information, as well as seven public-facing component websites, to determine whether DHS has implemented effective controls to secure its databases and websites. We identified vulnerabilities that may weaken the controls implemented to protect the data stored and processed by DHS' databases and websites.

Finally, we reviewed 24 different systems for compliance with applicable DHS baseline configuration requirements. Our results indicated that DHS baseline configuration guidelines have not been fully implemented, resulting in deficiencies in the areas of access controls, registry settings, user access, and general security controls.

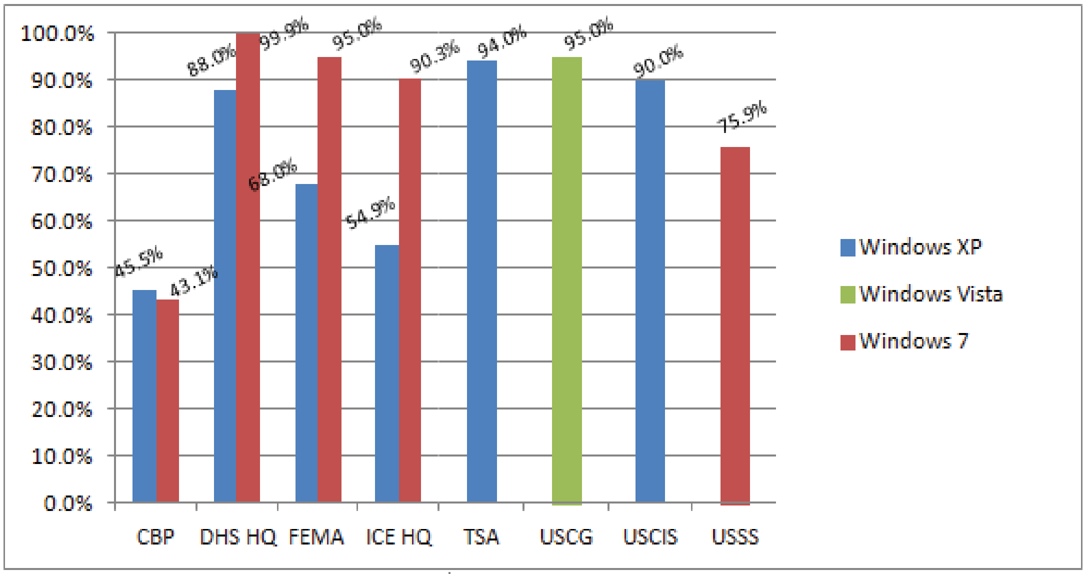
## Progress

- DHS HQ, TSA, USCG, and USCIS have implemented more than 85 percent of USGCB configuration settings on their workstations.
- DHS HQ has developed and begun deploying a Windows 7 image that complies with 99.9 percent of USGCB requirements. DHS HQ anticipates that the migration to Windows 7 will be completed by April 2013.

## Issues To Be Addressed

Components have not fully implemented all USGCB required settings on their workstations. Specifically, we determined that CBP, FEMA, and ICE have implemented fewer than 70 percent of the required USGCB settings on their Windows XP workstations, putting their machines at a greater risk of potential exploitation. Components believe that once migration to Windows 7 is complete, Windows XP will become obsolete. However, the majority of DHS' workstations are based on Windows XP operating systems, which Microsoft will stop supporting in 2014. Further, while six components are migrating to Windows 7, two components have not established an estimated completion date for their Windows 7 migration. Figure 1 depicts component USGCB compliance by operating system.

**Figure 1. Component USGCB Compliance by Operating System**[11]



- CBP has not established a standard USGCB baseline image for its Windows XP and Windows 7 user workstations, resulting in an average USGCB compliance of less than 50 percent. We reported a similar issue in our FY 2011 report.

- Results from our vulnerability scans on databases and servers indicated that components are not applying security patches timely or implementing the required security controls. Components included CBP, DHS HQ, FEMA, ICE, TSA, NPPD, USCG, USCIS, and USSS. Deficiencies identified include:

  - ➢ Missing security patches for operating systems, database applications, and installed software, such as Adobe Flash, Adobe Acrobat, Java, and Apache;

  - ➢ Microsoft Server 2003 and 2008 servers running antivirus software with definitions last updated in August 2011; and

  - ➢ DHS databases that have accounts with default passwords, weak password controls, missing software patches, excess user privileges, and vulnerable functionality packages made available to users with the "public" role.

[11] Due to workstation management controls, we were not able to evaluate the compliance of Windows XP workstations at USSS. In addition, NPPD user workstations are managed under the DHS HQ local area network.

- Our security scans identified vulnerabilities in the six public-facing websites at CBP, FEMA, ICE, NPPD, USCG, and USCIS. For example, we determined that:

  - ➢ Six websites have cross-site scripting vulnerabilities that could allow an attacker to hijack user accounts, execute malicious scripts, or access sensitive information.

  - ➢ Two websites are vulnerable to structured query language injection attacks that could allow an attacker to read, change, or delete information from databases that support vulnerable websites.

  - ➢ Two websites have accessible backup files, potentially allowing an attacker to gain unauthorized knowledge of how the website is constructed and use it to exploit weaknesses.

  - ➢ Two websites have vulnerabilities related to logins sent over an unencrypted connection or via unencrypted forms, potentially leading to impersonation of a legitimate user or unauthorized access to information.

- We reported in June 2012 that, while FEMA had established a Windows XP image based on USGCB settings, laptops in the field were not being configured with the standard laptop image.[12] As a result, our scan results from a selection of laptops revealed an average of 55percent Windows XP compliance.

See appendix E for the status of DHS' Configuration Management Program.

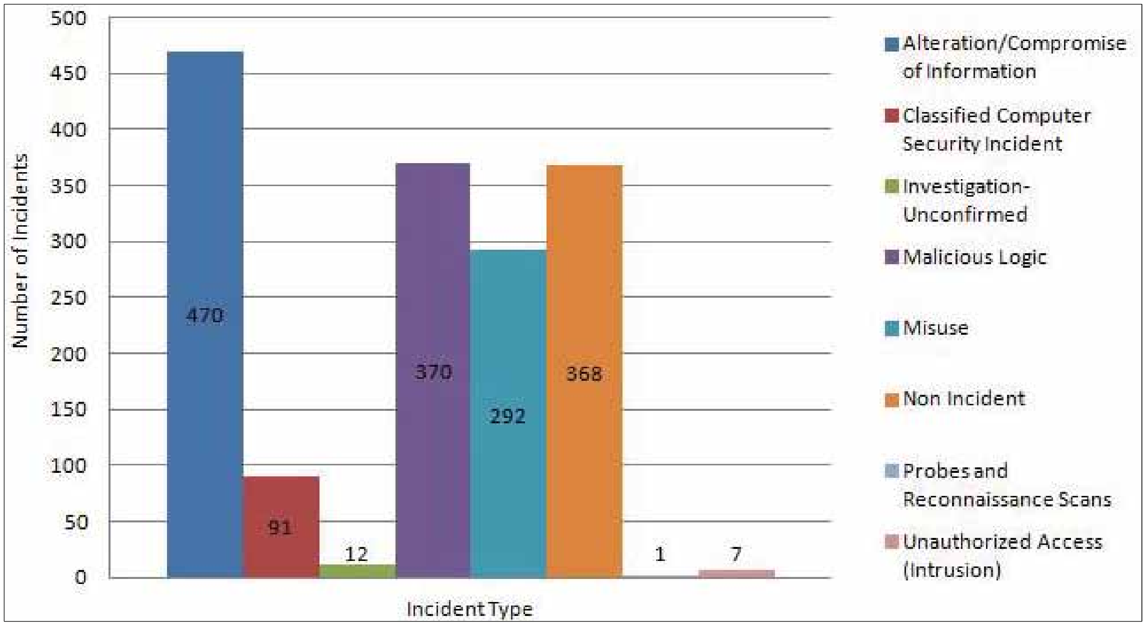
## Incident Response and Reporting Program

DHS has established adequate incident detection, handling, and analysis procedures. In addition, the number of all security incidents reported by the DHS Security Operations Center (SOC) has increased by 1 percent, from 1,589 in FY 2011 to 1,611 to FY 2012.[13] However, there was an overall increase of

[12] *Progress Has Been Made in Securing Laptops and Wireless Networks at FEMA* (OIG-12-93, June 2012).
[13] We evaluated the number of incidents reported by the SOC between October 1 and May 31 for both FY 2011 and FY 2012.

30 percent for significant incidents reported to the DHS SOC.[14] See figure 2 for an overview of the incidents that were reported in FY 2012.

**Figure 2. FY 2012 SOC Incident Summary**



### Progress

- DHS SOC conducts incident analysis and correlation to identify trends along with supporting strategy and decision-making. The June 2012 DHS FISMA Scorecard identified each component as having received a 100 percent SOC and Log metric score.

### Issues To Be Addressed

- During FY 2012, the Domestic Nuclear Detection Office, Office of Intelligence and Analysis, Federal Law Enforcement Training Center, MGMT, NPPD, Office of Operations Coordination and Planning, OIG, S&T, TSA, USCG, and USSS did not consistently submit weekly incident reports to the DHS SOC, as required.

- Based on the June 2012 FISMA scorecard, S&T (52 percent) and USCG (64 percent) received a score below 75 percent for the vulnerability

[14] A significant incident is defined as a computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate notification of leadership.

management metric, which evaluates components' ability to detect and assess weaknesses in their information systems.

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

### Security Training Program

The CISO continues to operate an effective security training program. Specifically, the CISO Training Office has established a process to validate components' security training and has implemented Information System Security Officer (ISSO) and System Administrator (SA) role-based training courses. However, the CISO is in the process of revising its role-based training program to ensure that all personnel with significant security responsibilities receive appropriate training content.

**Progress**

- During FY 2012, DHS began to revise its role-based training program. Specifically, DHS is establishing a process that allows components to share training work products, content, and opportunities via Microsoft SharePoint for employees with similar significant security roles. As part of this effort, DHS has identified more than 100 unique significant security roles across the Department.
- During FY 2012, the number of ISSO role-based training courses provided by DHS has increased from 8 in FY 2011 to 12 in FY 2012. In addition, the number of SA courses offered has doubled from two in FY 2011 to four in FY 2012.

**Issues To Be Addressed**

- As of August 2012, DHS is in the planning phase of using Microsoft SharePoint to enhance its revised role-based training program. According to CISO personnel, the implementation should be completed by FY 2013.

- As of July 2012, ISO (31 percent), S&T (38 percent), and USCG (42 percent) are maintaining a completion percentage of 42 percent or below for specialized training.

See appendix G for the status of DHS' Security Training Program.

## Remote Access Program

According to DHS policy, components are responsible for managing all remote access and dial-in connections to their systems through the use of two-factor authentication, providing audit capabilities, and protecting sensitive information throughout transmission. We reviewed the remote access programs at CBP, FEMA, ICE, TSA, USCG, USCIS, and USSS.

Overall, components utilizing remote access have developed policies to outline the controls needed to protect remote connections and have implemented mitigating security controls (multi-factor authentication, firewalls, virtual private network concentrators, etc.) to protect against external threats.

See appendix I for the status of DHS' Remote Access Program.

## Account and Identity Management Program

DHS has made progress in implementing an agency-wide system access management program. However, DHS does not have a centralized capability to identify users and devices connected to its systems. Specifically, components are currently maintaining their own account and identity management programs.

### Progress

- DHS has issued Homeland Security Presidential Directive 12 (HSPD-12) PIV-compliant cards to all employees and contractors across the Department.

- On July 31, 2012, the Undersecretary for Management issued a memorandum providing components with additional guidance regarding the use of PIV-compliant cards to access DHS unclassified networks. Components are required to develop an executable plan and allocate sufficient funding to achieve full implementation.[15]

- Components have provided the DHS Identity, Credential, and Access Program Management Office (ICAM PMO) with PIV card implementation plans, as required.

[15] *Implementation of Mandatory Use of the Personal Identity Verification (PIV) Card to Access DHS Networks*, July 31, 2012.

- The ICAM PMO has reviewed component implementation plans to develop a Department-wide PIV-enabled logical access plan, which includes milestones, cost estimates, and technical requirements. Furthermore, the ICAM PMO has issued concept of operations and other PIV user guidance.

- DHS has revised its Information Technology Acquisition Review process to require components to include a PIV credential compliance clause when procuring IT products, systems, services, hardware, or software.

### Issues To Be Addressed

- DHS is not utilizing PIV-compliant cards to access its information systems, as required by OMB. The Department's goal is to achieve 20 percent compliance by the end of FY 2012, 50 percent by the end of FY 2013, and 75 percent by the end of FY 2014 for accessing components' local area networks. However, DHS has not established milestones to address the use of PIV cards to access its major applications.

- DHS has yet to employ HSPD-12-compliant cards to access its classified systems. The National Security Systems Joint Program Management Office has developed a department-wide implementation plan, which has not been approved as of June 30, 2012. Further, the plan does not address PIV credential access to stand-alone classified systems.

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

## Continuous Monitoring Program

DHS has further improved the automated collection capability of its assets by disseminating a standardized monthly feed template to components, developing a parser to organize scan data, and providing installation and technical support for components' data feed submissions. During FY 2012, the CISO performed 41 critical control reviews on selected information systems to ensure that key controls have been implemented and to help components identify potential weaknesses or vulnerabilities.

### Progress

- The CISO conducts continuous monitoring working group meetings with the components monthly. The focus of these meetings is to discuss the

Enterprise Continuous Monitoring Strategy Development status and monthly data feed status and issues.

- As part of its effort to establish a robust, enterprise-wide continuous monitoring program, DHS has revised its information security scorecard to include an HSPD-12 PIV card logical access, monthly asset reporting, and SOC log aggregation metrics to monitor components' progress.

**Issues to Be Addressed**

- DHS and its components have not established a real-time and fully automated continuous monitoring capability to track all hardware and network devices, external connections, and software associated with their information systems.

- As of June 2012, five components (FEMA, ICE, S&T, USCG, and USCIS) have scores of 75 percent or below for the overall information security.

- As of June 2012, DHS has not performed any critical control reviews on its Top Secret systems.

See appendix K for the status of DHS' Continuous Monitoring Program.

## 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 has developed or updated the following documents during FY 2012:

  - ➢ *DHS Test, Training and Exercise (TTE) Program Plan* – January 2012
  - ➢ *DHS Headquarters Reconstitution* Plan – March 5, 2012
  - ➢ *DHS Headquarters Continuity of Operations (COOP) Plan* – June 4, 2012

- DHS has developed training, testing, and exercise approaches for its business continuity and disaster recovery programs. For example, from March to June 2012, DHS and its components participated in Federal Government continuity exercises to test activation continuity plans, information sharing, systems and procedures, and operational capabilities.

**Issues To Be Addressed**

- The *DHS Continuity Plan* is under development. According to a DHS Business Continuity and Emergency Preparedness Branch official, the plan will be completed by September 2012.

- Our review of 25 security authorization packages revealed that contingency plans and/or testing reports for 6 systems are missing certain elements, including the identification of alternate processing facilities, or restoration procedures. In addition, one contingency plan is not up-to-date. As part of the Department's overall contingency planning and disaster recovery efforts, DHS requires an IT contingency plan be developed for all IT systems, detailing how the system will be recovered in the event of an emergency or disaster.

See appendix L for the status of DHS' Contingency Planning Program.

## Security Capital Planning Program

DHS continues to base its Capital Planning and Investment Control (CPIC) process 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 managing Federal capital assets.[16] The DHS CPIC Guide provides components with policies and procedures for selecting, monitoring, and evaluating the Department's IT and non-IT investments to ensure that each investment is successfully managed, cost-effective, and supports DHS' mission and strategic goals.[17] In addition, as part of its Information Technology Acquisition Review process, the Chief Information Officer reviews any proposed IT acquisition of $2.5 million and above. Finally, DHS has developed an automated process to ensure that the Department's IT and non- IT investments are successfully managed, cost-effective, and support its mission and strategic goals.

[16] OMB's Circular A-11, Part 7 – *Planning, Budgeting, Acquisition, and Management of Capital Assets*, June 2008.
[17] *Department of Homeland Security Capital Planning and Investment Control (CPIC) Guide*, version 7.1, August 2010.

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

**Recommendations**

We recommend that the CISO:

**Recommendation #1:**

Establish a process to ensure that USGCB settings are implemented and maintained at components.

**Recommendation #2:**

Strengthen the ISO review process to ensure that all applicable controls are included in the security documentation when authorizing systems.

**Recommendation #3:**

Improve the process to ensure that DHS baseline configuration settings are implemented and maintained on components' information systems. The process should include testing and the use of automated tools and security templates.

**Recommendation #4:**

Strengthen the ISO review process to ensure that POA&Ms, including those for classified systems, are complete and current.

**Recommendation #5:**

Enhance the Department's revised role-based training program to ensure that appropriate role-based training is provided to enable all individuals with significant security responsibilities to perform their required security functions.

**Recommendation #6:**

Establish a process to ensure that security patches and service packs are applied timely and effective controls are implemented on components' databases and servers.

## Management Comments and OIG Analysis

### Management Comments to Recommendation #1

DHS concurred with recommendation 1. The DHS FY 2013 Information Security Scorecard will be utilizing continuous monitoring data feeds from component tools to monitor the implementation of USGCB settings. The Scorecard will be used to communicate progress in addressing gaps and to ensure continued compliance. Estimated completion date: December 31, 2012.

### OIG Analysis

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

### Management Comments to Recommendation #2

DHS concurred with recommendation 2. The Department provides an enterprise security authorization tool to ensure the required security controls and documentation are completed. The tool will be revised with improved, streamlined templates and controls to increase the quality of security packages reviewed by the ISO Document Review Team.

### OIG Analysis

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

### Management Comments to Recommendation #3

DHS concurred with recommendation 3. The DHS FY 2013 Information Security Scorecard will utilize continuous monitoring data feeds from component tools to monitor the implementation of USGCB settings. The Scorecard will be used to communicate progress in addressing gaps and to ensure continued compliance. The continuous monitoring capabilities can be customized by components to monitor their individual baseline control templates. Estimated completion date: December 31, 2012.

## OIG Analysis

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

## Management Comments to Recommendation #4

DHS concurred with recommendation 4. The ISO continues to strengthen the POA&M review process to ensure POA&Ms, including those for classified systems, are complete and current. ISO has begun closely tracking components' progress towards POA&M completion and contacting components when POA&M indicators show inadequate progress. Additionally, ISO has begun educating components on methods within the DHS compliance tool for checking POA&M completeness and monitoring milestone progress so that timely revisions can be made to POA&Ms not meeting expectations.

## OIG Analysis

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

## Management Comments to Recommendation #5

DHS concurred with recommendation 5. The ISO is developing sample courseware and identifying pre-existing federally available courseware to supplement existing component role-based training programs. In conjunction with component training coordinators, plans are being developed to ensure minimum standards can be deployed in a more consistent manner across the Department.

## OIG Analysis

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

## Management Comments to Recommendation #6

DHS concurred with recommendation 6. The DHS FY 2013 Information Security Scorecard will utilize continuous monitoring data feeds from component tools to monitor security patching of databases and servers. The Scorecard will be used to communicate progress in addressing gaps and to ensure continued compliance. Estimated completion date: December 31, 2012.

**OIG Analysis**

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

## Appendix A
## Objectives, Scope, and Methodology

The 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 draft FY 2012 FISMA reporting metrics dated March 2012. We conducted our fieldwork at the departmental level and at DHS' organizational components and offices, including CBP, DHS HQ, FEMA, ICE, NPPD, S&T, TSA, USCG, USCIS, and USSS.

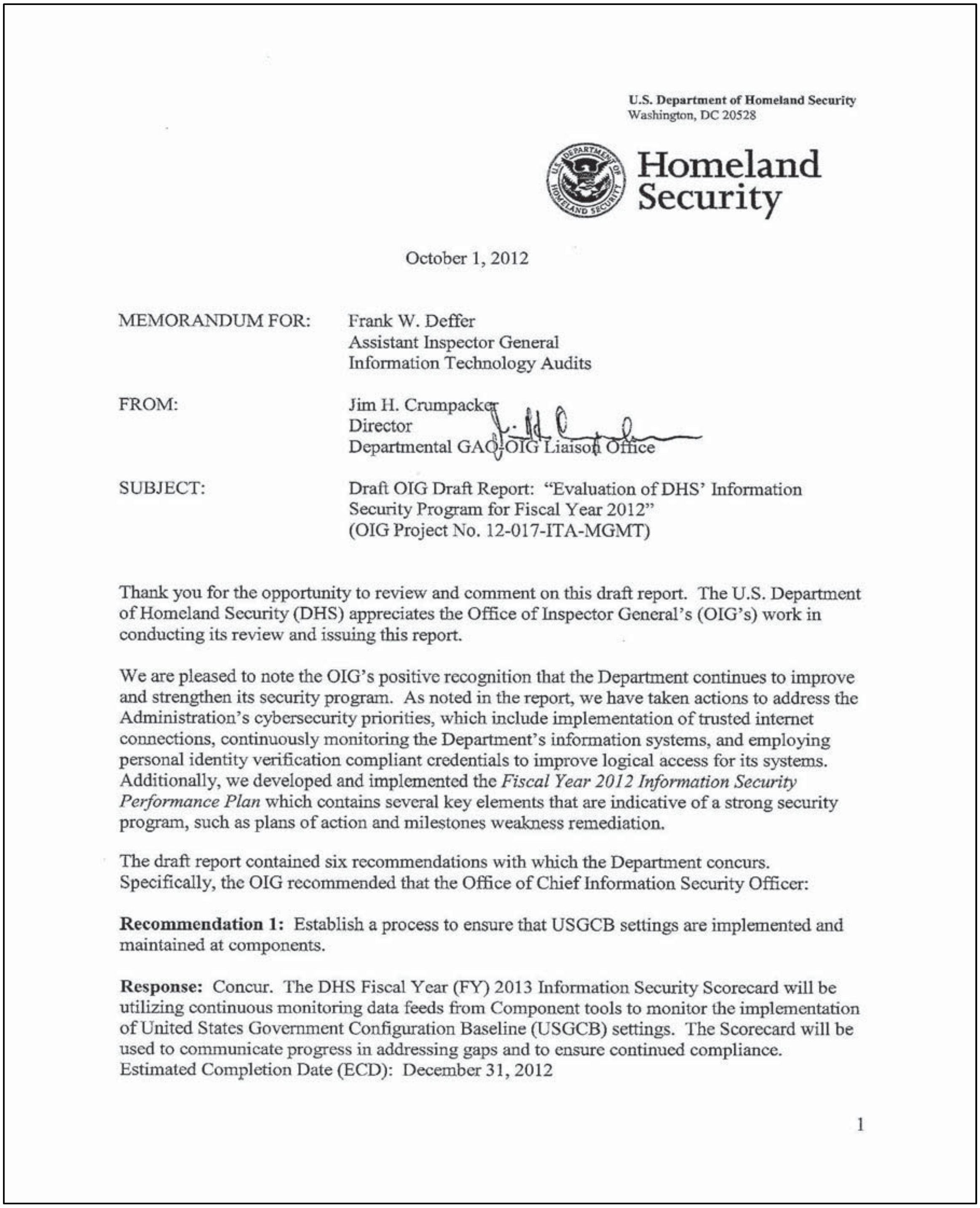
In addition, we conducted reviews of DHS' information systems and security program-related areas throughout FY 2012. This report includes the results of a limited number of systems evaluated during the year and our ongoing financial statement review.

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 the 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 reviewed the quality of security authorization packages for a sample of 25 systems at CBP, DHS HQ, FEMA, ICE, NPPD, S&T, TSA, USCG, USCIS, and USSS to ensure that all of the required documents were completed prior to system authorization. In addition, we evaluated the implementation of DHS' baseline configurations for 24 systems as well as the use of industry standard best standards for securing 9 databases and 6 public-facing component websites at CBP, FEMA, ICE, NPPD, USCG, and USCIS. We also reviewed the USGCB settings on user workstations at these components.

We conducted this review between April and August 2012 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 1, 2012

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

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

SUBJECT: Draft OIG Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2012"
(OIG Project No. 12-017-ITA-MGMT)

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 conducting its review and issuing this report.

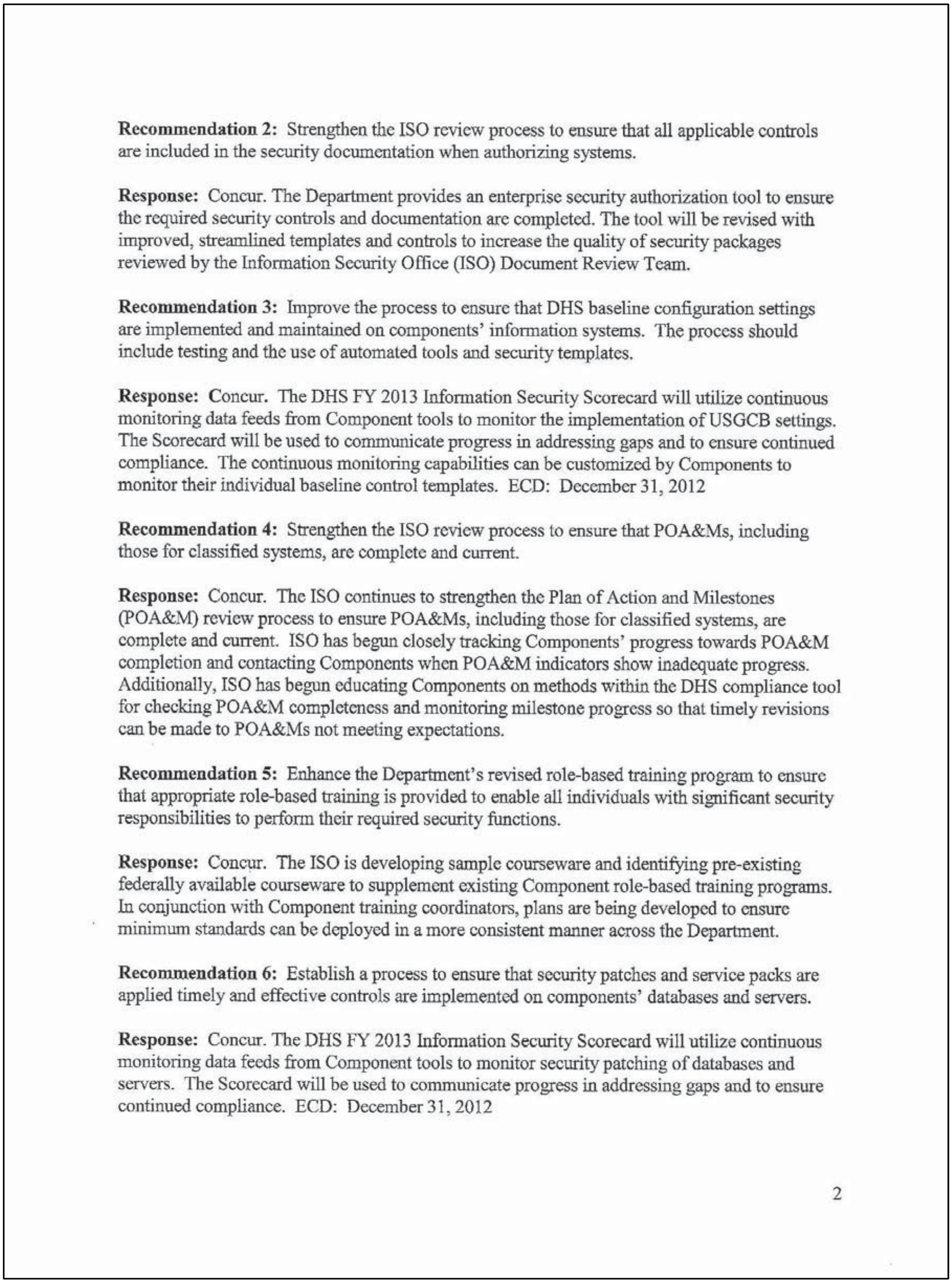
We are pleased to note the OIG's positive recognition that the Department continues to improve and strengthen its security program. As noted in the report, we have taken actions to address the Administration's cybersecurity priorities, which include implementation of trusted internet connections, continuously monitoring the Department's information systems, and employing personal identity verification compliant credentials to improve logical access for its systems. Additionally, we developed and implemented the *Fiscal Year 2012 Information Security Performance Plan* which contains several key elements that are indicative of a strong security program, such as plans of action and milestones weakness remediation.

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

**Recommendation 1:** Establish a process to ensure that USGCB settings are implemented and maintained at components.

**Response:** Concur. The DHS Fiscal Year (FY) 2013 Information Security Scorecard will be utilizing continuous monitoring data feeds from Component tools to monitor the implementation of United States Government Configuration Baseline (USGCB) settings. The Scorecard will be used to communicate progress in addressing gaps and to ensure continued compliance. Estimated Completion Date (ECD): December 31, 2012

1



**Recommendation 2:** Strengthen the ISO review process to ensure that all applicable controls are included in the security documentation when authorizing systems.

**Response:** Concur. The Department provides an enterprise security authorization tool to ensure the required security controls and documentation are completed. The tool will be revised with improved, streamlined templates and controls to increase the quality of security packages reviewed by the Information Security Office (ISO) Document Review Team.

**Recommendation 3:** Improve the process to ensure that DHS baseline configuration settings are implemented and maintained on components' information systems. The process should include testing and the use of automated tools and security templates.

**Response:** Concur. The DHS FY 2013 Information Security Scorecard will utilize continuous monitoring data feeds from Component tools to monitor the implementation of USGCB settings. The Scorecard will be used to communicate progress in addressing gaps and to ensure continued compliance. The continuous monitoring capabilities can be customized by Components to monitor their individual baseline control templates. ECD: December 31, 2012

**Recommendation 4:** Strengthen the ISO review process to ensure that POA&Ms, including those for classified systems, are complete and current.

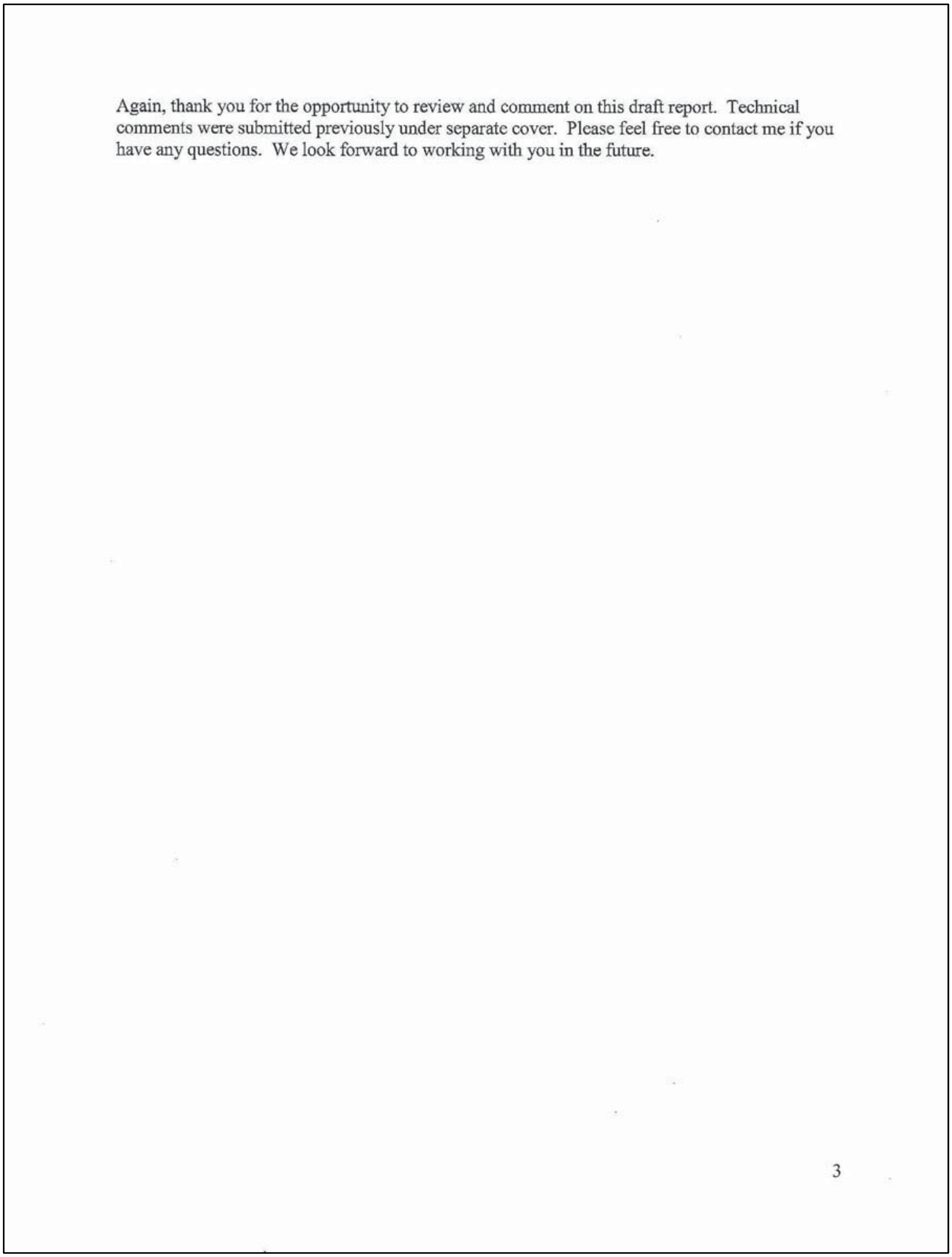
**Response:** Concur. The ISO continues to strengthen the Plan of Action and Milestones (POA&M) review process to ensure POA&Ms, including those for classified systems, are complete and current. ISO has begun closely tracking Components' progress towards POA&M completion and contacting Components when POA&M indicators show inadequate progress. Additionally, ISO has begun educating Components on methods within the DHS compliance tool for checking POA&M completeness and monitoring milestone progress so that timely revisions can be made to POA&Ms not meeting expectations.

**Recommendation 5:** Enhance the Department's revised role-based training program to ensure that appropriate role-based training is provided to enable all individuals with significant security responsibilities to perform their required security functions.

**Response:** Concur. The ISO is developing sample courseware and identifying pre-existing federally available courseware to supplement existing Component role-based training programs. In conjunction with Component training coordinators, plans are being developed to ensure minimum standards can be deployed in a more consistent manner across the Department.

**Recommendation 6:** Establish a process to ensure that security patches and service packs are applied timely and effective controls are implemented on components' databases and servers.

**Response:** Concur. The DHS FY 2013 Information Security Scorecard will utilize continuous monitoring data feeds from Component tools to monitor security patching of databases and servers. The Scorecard will be used to communicate progress in addressing gaps and to ensure continued compliance. ECD: December 31, 2012



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

# Appendix C
# System Inventory

**Question 1: System Inventory**

**1. Identify the number of agency and contractors' systems by component and FIPS 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 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.<br>Agency Systems** | | **b.<br>Contractor Systems** | | **c.<br>Total Number of Systems (Agency and Contractor systems) (Column A + Column B)** | | **a.<br>Number of systems certified and accredited** | | **b.<br>Number of systems for which security controls have been tested and reviewed in the past year** | | **c.<br>Number of systems for which contingency plans have been tested in accordance with policy** | |
| **Bureau Name** | **FIPS 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 | 17 | 1 | 0 | 0 | 17 | 1 | 17 | 100% | 16 | 94% | 14 | 82% |
| | Moderate | 65 | 8 | 2 | 0 | 67 | 8 | 63 | 94% | 59 | 88% | 55 | 82% |
| | Low | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 100% | 1 | 100% | 1 | 100% |
| | Not Categorized | 3 | 0 | 0 | 0 | 3 | 0 | 1 | 33% | 1 | 33% | 1 | 33% |
| | **Sub-total** | **86** | **9** | **2** | **0** | **88** | **9** | **82** | **93%** | **77** | **88%** | **71** | **81%** |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **DHS HQ** | High | 11 | 2 | 4 | 0 | 15 | 2 | 14 | 93% | 7 | 47% | 14 | 93% |
| | Moderate | 21 | 0 | 11 | 3 | 32 | 3 | 29 | 91% | 13 | 41% | 30 | 94% |
| | Low | 1 | 0 | 3 | 0 | 4 | 0 | 4 | 100% | 2 | 50% | 4 | 100% |
| | Not Categorized | 1 | 0 | 3 | 0 | 4 | 0 | 3 | 75% | 1 | 25% | 0 | 0% |
| | **Sub-total** | **34** | **2** | **21** | **3** | **55** | **5** | **50** | **91%** | **23** | **42%** | **48** | **87%** |
| **FEMA** | High | 20 | 4 | 2 | 0 | 22 | 4 | 18 | 82% | 18 | 82% | 13 | 59% |
| | Moderate | 37 | 2 | 13 | 0 | 50 | 2 | 40 | 80% | 40 | 80% | 39 | 78% |
| | Low | 3 | 0 | 0 | 0 | 3 | 0 | 3 | 100% | 2 | 67% | 2 | 67% |
| | Not Categorized | 10 | 0 | 0 | 0 | 10 | 0 | 6 | 60% | 6 | 60% | 5 | 50% |
| | **Sub-total** | **70** | **6** | **15** | **0** | **85** | **6** | **67** | **79%** | **66** | **78%** | **59** | **69%** |
| **FLETC** | High | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | - | 0 | - |
| | Moderate | 11 | 0 | 2 | 0 | 13 | 0 | 12 | 92% | 10 | 77% | 12 | 92% |
| | Low | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | - | 0 | - |
| | Not Categorized | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | - | 0 | - |
| | **Sub-total** | **11** | **0** | **2** | **0** | **13** | **0** | **12** | **92%** | **10** | **77%** | **12** | **92%** |
| **ICE** | High | 11 | 2 | 1 | 1 | 12 | 3 | 12 | 100% | 12 | 100% | 11 | 92% |
| | Moderate | 38 | 1 | 12 | 1 | 50 | 2 | 48 | 96% | 30 | 60% | 49 | 98% |
| | Low | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 100% | 2 | 100% | 2 | 100% |
| | Not Categorized | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 100% | 1 | 100% | 1 | 100% |
| | **Sub-total** | **52** | **3** | **13** | **2** | **65** | **5** | **63** | **97%** | **45** | **69%** | **63** | **97%** |
| **NPPD** | High | 7 | 1 | 6 | 1 | 13 | 2 | 13 | 100% | 13 | 100% | 12 | 92% |
| | Moderate | 7 | 0 | 11 | 1 | 18 | 1 | 18 | 100% | 16 | 89% | 16 | 89% |
| | Low | 1 | 0 | 6 | 1 | 7 | 1 | 6 | 86% | 6 | 86% | 6 | 86% |
| | Not Categorized | 3 | 1 | 0 | 0 | 3 | 1 | 3 | 100% | 3 | 100% | 2 | 67% |
| | **Sub-total** | **18** | **2** | **23** | **3** | **41** | **5** | **40** | **98%** | **38** | **93%** | **36** | **88%** |
| **OIG** | High | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 100% | 1 | 50% | 2 | 100% |
| | Moderate | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | - | 0 | - |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Low | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | - | 0 | - |
| | Not Categorized | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 100% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **3** | **0** | **0** | **0** | **3** | **0** | **3** | **100%** | **1** | **33%** | **2** | **67%** |
| **S&T** | High | 2 | 0 | 0 | 0 | 2 | 0 | 1 | 50% | 1 | 50% | 1 | 50% |
| | Moderate | 13 | 1 | 13 | 0 | 26 | 1 | 26 | 100% | 22 | 85% | 23 | 88% |
| | Low | 2 | 0 | 1 | 0 | 3 | 0 | 2 | 67% | 0 | 0% | 2 | 67% |
| | Not Categorized | 2 | 0 | 0 | 0 | 2 | 0 | 1 | 50% | 0 | 0% | 1 | 50% |
| | **Sub-total** | **19** | **1** | **14** | **0** | **33** | **1** | **30** | **91%** | **23** | **70%** | **27** | **82%** |
| **TSA** | High | 24 | 1 | 1 | 0 | 25 | 1 | 25 | 100% | 24 | 96% | 24 | 96% |
| | Moderate | 30 | 2 | 13 | 1 | 43 | 3 | 43 | 100% | 39 | 91% | 40 | 93% |
| | Low | 6 | 0 | 2 | 0 | 8 | 0 | 8 | 100% | 7 | 88% | 7 | 88% |
| | Not Categorized | 4 | 1 | 0 | 0 | 4 | 1 | 4 | 100% | 4 | 100% | 3 | 75% |
| | **Sub-total** | **64** | **4** | **16** | **1** | **80** | **5** | **80** | 100% | **74** | **93%** | **74** | **93%** |
| **USCG** | High | 9 | 1 | 5 | 1 | 14 | 2 | 13 | 93% | 13 | 93% | 13 | 93% |
| | Moderate | 67 | 3 | 20 | 0 | 87 | 3 | 67 | 77% | 51 | 59% | 60 | 69% |
| | Low | 7 | 1 | 2 | 0 | 9 | 1 | 4 | 44% | 6 | 67% | 6 | 67% |
| | Not Categorized | 35 | 3 | 0 | 0 | 35 | 3 | 33 | 94% | 16 | 46% | 7 | 20% |
| | **Sub-total** | **118** | **8** | **27** | **1** | **145** | **9** | **117** | **81%** | **86** | **59%** | **86** | **59%** |
| **USCIS** | High | 4 | 1 | 6 | 0 | 10 | 1 | 10 | 100% | 3 | 30% | 0 | 0% |
| | Moderate | 21 | 0 | 16 | 3 | 37 | 3 | 24 | 65% | 21 | 57% | 16 | 43% |
| | Low | 1 | 0 | 3 | 0 | 4 | 0 | 4 | 100% | 2 | 50% | 2 | 50% |
| | Not Categorized | 2 | 0 | 0 | 0 | 2 | 0 | 1 | 50% | 1 | 50% | 1 | 50% |
| | **Sub-total** | **28** | **1** | **25** | **3** | **53** | **4** | **39** | **74%** | **27** | **51%** | **19** | **36%** |
| **USSS** | High | 5 | 1 | 0 | 0 | 5 | 1 | 5 | 100% | 5 | 100% | 4 | 80% |
| | Moderate | 8 | 2 | 0 | 0 | 8 | 2 | 8 | 100% | 8 | 100% | 6 | 75% |
| | Low | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | - | 0 | - |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Not Categorized | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 100% | 1 | 100% | 1 | 100% |
| | **Sub-total** | **14** | **3** | **0** | **0** | **14** | **3** | **14** | **100%** | **14** | **100%** | **11** | **79%** |
| **Agency Totals** | **High** | **112** | **14** | **25** | **3** | **137** | **17** | **130** | **95%** | **113** | **82%** | **108** | **79%** |
| | **Moderate** | **318** | **19** | **113** | **9** | **431** | **28** | **378** | **88%** | **309** | **72%** | **346** | **80%** |
| | **Low** | **24** | **1** | **17** | **1** | **41** | **2** | **34** | **83%** | **28** | **68%** | **32** | **78%** |
| | **Not Categorized** | **63** | **5** | **3** | **0** | **66** | **5** | **55** | **83%** | **34** | **52%** | **22** | **33%** |
| | **Total** | **517** | **39** | **158** | **13** | **675** | **52** | **597** | **88%** | **484** | **72%** | **508** | **75%** |

## Appendix D
## Status of Risk Management Program

| Section 2: Status of Risk Management Program | |
|---|---|
| | **Response:** |
| **1. Check one:**<br>**A. The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**<br>**1. Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.**<br>**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 800-37, Rev. 1.**<br>**3. Addresses risk from a *mission and business process* perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.**<br>**4. Addresses risk from an *information system* perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.**<br>**5. Categorizes information systems in accordance with government policies.**<br>**6. Selects an appropriately tailored set of baseline security controls.**<br>**7. Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.**<br>**8. 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.**<br>**9. 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.**<br>**10. 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.**<br>**11. Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.**<br>**12. Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).**<br>**13. 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.**<br>**14. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.**<br>**15. Security authorization package contains Accreditation boundaries for Agency information systems defined in accordance with government policies.** | ✓ |

| | |
|---|---|
| B. The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.<br>C. The Agency has not established a risk management program. | __________ |
| 2. If B. is checked above, check areas that need significant improvement:<br>a. Risk Management policy is not fully developed.<br>b. Risk Management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).<br>c. Risk Management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).<br>d. A Comprehensive governance structure and Agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).<br>e. Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53).<br>f. Information systems are not properly categorized (FIPS-199/SP 800-60).<br>g. Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS-200/SP 800-53).<br>h. Risk assessments are not conducted in accordance with government policies (SP 800-30).<br>i. Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).<br>j. The communication of information system specific risks, mission/business specific risks and organizational level (strategic) risks to appropriate levels of the organization is not in accordance with government policies.<br>k. The process to assess security control effectiveness is not in accordance with government policies (SP800-53A).<br>l. The process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37).<br>m. The process to continuously monitor changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37).<br>n. Security plan is not in accordance with government policies (SP 800-18, SP 800-37).<br>o. Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).<br>p. Accreditation boundaries for agency information systems are not defined in accordance with government policies.<br>q. Other<br>r. Explanation for Other | |
| 3. Comments: | • DHS bases its risk management program on NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and incorporated the security authorization process into the *DHS Sensitive Systems Policy Directive 4300A* for its unclassified systems. For national security systems, components follow the Defense Information Assurance Certification and Accreditation Process and DHS Sensitive Systems Policy Directive 4300B policy. |

# Appendix E
# Status of Configuration Management Program

| Section 3: Status of Configuration Management Program | |
|---|---|
| | **Response:** |
| **4. Check one:**<br>A. The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for configuration management.<br>2. Standard baseline configurations defined.<br>3. Assessing for compliance with baseline configurations.<br>4. Process for timely, as specified in agency policy or standards, remediation of scan result deviations.<br>5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.<br>6. Documented proposed or actual changes to hardware and software configurations.<br>7. Process for timely and secure installation of software patches.<br>8. Software assessing (scanning) capabilities are fully implemented.<br>9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Agency policy or standards.<br>10. Patch management process is fully developed, as specified in Agency policy or standards. | |
| B. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below. | ✓ |
| C. The Agency has not established a security configuration management program. | |
| **5. If B. is checked above, check areas that need significant improvement:**<br>a. Configuration management policy is not fully developed (NIST 800-53: CM-1).<br>b. Configuration management procedures are not fully developed (NIST 800-53: CM-1).<br>c. Configuration management procedures are not consistently implemented (NIST 800-53: CM-1).<br>d. Standard baseline configurations are not identified for software components (NIST 800-53: CM-2).<br>e. Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).<br>f. Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).<br>g. FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6).<br>h. Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).<br>i. Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in agency policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2). | g |

| | |
|---|---|
| **j. Patch management process is not fully developed, as specified in agency policy or standards. (NIST 800-53: CM-3, SI-2).**<br>**k. Other**<br>**l. Explanation for Other** | |
| **6. Identify baselines reviewed:**<br>**a. Software Name**<br>**b. Software Version** | **- Website industry standard best practices**<br>**- Database industry standard best practices** |
| **7. Comments:** | • Based on our review of 27 systems, we determined that DHS components had not fully configured databases and components' public-facing websites based on industry standard best practices.<br>• DHS HQ, TSA, USCG, and USCIS implemented more than 85 percent of USGCB configuration settings on their workstations. |

# Appendix F
# Status of Incident Response and Reporting Program

| Section 4: Status of Incident Response & Reporting Program | |
|---|---|
| | Response: |
| 8. Check one:<br>A. The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for detecting, responding to and reporting incidents.<br>2. Comprehensive analysis, validation and documentation of incidents.<br>3. When applicable, reports to US-CERT within established timeframes.<br>4. When applicable, reports to law enforcement within established timeframes.<br>5. Responds to and resolves incidents in a timely manner, as specified in agency policy or standards, to minimize further damage.<br>6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.<br>7. Is capable of correlating incidents.<br>8. There is sufficient incident monitoring and detection coverage in accordance with government policies. | ✓ |
| B. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency has not established an incident response and reporting program. | |
| 9. If B. is checked above, check areas that need significant improvement:<br>a. Incident response and reporting policy is not fully developed (NIST 800-53: IR-1).<br>b. Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1).<br>c. Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev1).<br>d. Incidents were not identified in a timely manner, as specified in agency policy or standards (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).<br>e. Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).<br>f. Incidents were not reported to law enforcement as required (SP 800-86).<br>g. Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).<br>h. Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).<br>i. There is insufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).<br>j. The agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment.<br>k. The agency does not have the technical capability to correlate incident events. | |
| l. Other<br>m. Explanation for Other | |

| | |
|---|---|
| **10. Comments:** | |

# Appendix G
# Status of Security Training Program

| Section 5: Status of Security Training Program | |
|---|---|
| | Response: |
| 11. Check one:<br>A. The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for security awareness training.<br>2. Documented policies and procedures for specialized training for users with significant information security responsibilities.<br>3. Security training content based on the organization and roles, as specified in agency policy or standards.<br>4. Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training.<br>5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other agency users) with significant information security responsibilities that require specialized training.<br>6. Training material for security awareness training does not contain appropriate content for The Agency. | ✓ |
| B. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency has not established a security training program. | |

| | |
|---|---|
| **12. If B. is checked above, check areas that need significant improvement:**<br>**a. Security awareness training policy is not fully developed (NIST 800-53: AT-1).**<br>**b. Security awareness training procedures are not fully developed and sufficiently detailed (NIST 800-53: AT-1).**<br>**c. Security awareness training procedures are not consistently implemented in accordance with government policies (NIST 800-53: AT-2).**<br>**d. Specialized security training policy is not fully developed (NIST 800-53: AT-3).**<br>**e. Specialized security training procedures are not fully developed or sufficiently detailed in accordance with government policies (SP 800-50, SP 800-53).**<br>**f. Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).**<br>**g. Identification and tracking of the status of security awareness training for personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training is not adequate in accordance with government policies (SP 800-50, SP 800-53).**<br>**h. Identification and tracking of the status of specialized training for personnel (including employees, contractors, and other agency users) with significant information security responsibilities is not adequate in accordance with government policies (SP 800-50, SP 800-53).**<br>**i. Training content for individuals with significant information security responsibilities is not adequate in accordance with government policies (SP 800-53, SP 800-16).**<br>**j. Less than 90% of personnel (including employees, contractors, and other agency users) with access privileges completed security awareness training in the past year.**<br>**k. Less than 90% of employees, contractors, and other users with significant security responsibilities completed specialized security awareness training in the past year.**<br>**l. Other**<br>**m. Explanation for Other** | |
| **13. Comments:** | • DHS has documented policies and procedures for maintaining a security training program.<br>• DHS has established a process to validate components' security training.<br>• DHS has developed and implemented specialized training courses for system security officers and system administrators.<br>• DHS utilizes its enterprise management tool to identify and track the status of specialized training for all personnel with significant information security responsibilities. |

# Appendix H
# Status of Plans of Actions and Milestones Program

| Section 6: Status of Plans of Actions & Milestones (POA&M) Program | |
|---|---|
| | Response: |
| 14. Check one:<br>A. The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.<br>2. Tracks, prioritizes and remediates weaknesses.<br>3. Ensures remediation plans are effective for correcting weaknesses.<br>4. Establishes and adheres to milestone remediation dates.<br>5. Ensures resources are provided for correcting weaknesses.<br>6. POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weaknesses due to a Risk Based Decision to not implement a security control.)<br>7. Costs associated with remediating weaknesses are identified.<br>8. Program officials and contractors 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. | ✓ |
| B. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency has not established a POA&M program. | |

| | |
|---|---|
| **15. If B. is checked above, check areas that need significant improvement:**<br>**a. POA&M Policy is not fully developed.**<br>**b. POA&M procedures are not fully developed and sufficiently detailed.**<br>**c. POA&M procedures are not consistently implemented in accordance with government policies.**<br>**d. POA&Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation (OMB M-04-25).**<br>**e. Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).**<br>**f. Source of security weaknesses are not tracked (OMB M-04-25).**<br>**g. Security weaknesses are not appropriately prioritized (OMB M-04-25).**<br>**h. Milestone dates are not adhered to (OMB M-04-25).**<br>**i. Initial target remediation dates are frequently missed (OMB M-04-25).**<br>**j. POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).**<br>**k. Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).**<br>**l. Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).**<br>**m. Other**<br>**n. Explanation for Other** | |
| **16. Comments:** | • DHS requires components to create and manage POA&Ms for all known IT security weaknesses.<br>• DHS has developed policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.<br>• As of June 30, 2012, DHS has 4,377 open POA&Ms. However, components are not entering and tracking all IT security weaknesses in DHS' unclassified and classified enterprise management tools, nor are all of the data entered by the components accurate and updated in a timely manner.<br>• DHS creates quarterly POA&M progress reports, tracking weakness remediation and maintenance. |

# Appendix I
# Status of Remote Access Program

| Section 7: Status of Remote Access Program | |
|---|---|
| | Response: |
| 17. Check one:<br>A. The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.<br>2. Protects against unauthorized connections or subversion of authorized connections.<br>3. Users are uniquely identified and authenticated for all access.<br>4. Telecommuting policy is fully developed.<br>5. If applicable, multi-factor authentication is required for remote access.<br>6. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.<br>7. Defines and implements encryption requirements for information transmitted across public networks.<br>8. Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication is required.<br>9. Lost or stolen devices are disabled and appropriately reported.<br>10. Remote access rules of behavior are adequate in accordance with government policies.<br>11. Remote access user agreements are adequate in accordance with government policies. | ✓ |
| B. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency has not established a program for providing secure remote access. | |
| 18. If B. is checked above, check areas that need significant improvement:<br>a. Remote access policy is not fully developed (NIST 800-53: AC-1, AC-17).<br>b. Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1, AC-17).<br>c. Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1, AC-17).<br>d. Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).<br>e. Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4).<br>f. Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).<br>g. Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).<br>h. Agency has not identified all remote devices (NIST 800-46, Section 2.1).<br>i. Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).<br>j. Agency does not adequately monitor remote devices when connected to the agency's networks remotely in accordance with government policies (NIST 800-46, Section 3.2). | |

| | |
|---|---|
| k. Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).<br>l. Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4).<br>m. Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).<br>n. Other<br>o. Explanation for Other | |
| 19. Comments: | |

# Appendix J
# Status of Account and Identity Management Program

| Section 8: Status of Account and Identity Management Program | |
|---|---|
| | Response: |
| 20. Check one:<br>A. The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for account and identity management.<br>2. Identifies all users, including Federal employees, contractors, and others who access Agency systems.<br>3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary.<br>4. If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.<br>5. Agency has adequately planned for implementation of PIV for logical access in accordance with government policies.<br>6. Ensures that the users are granted access based on needs and separation of duties principles.<br>7. Identifies devices that are attached to the network and distinguishes these devices from users.<br>8. Identifies all User and Non-User Accounts (refers to user accounts that are on a system).<br>9. Ensures that accounts are terminated or deactivated once access is no longer required.<br>10. Identifies and controls use of shared accounts. | ✓ |
| B. The Agency has established and is maintaining an identity and access management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency has not established an identity and access management program. | |
| 21. If B. is checked above, check areas that need significant improvement:<br>a. Account management policy is not fully developed (NIST 800-53: AC-1).<br>b. Account management procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1).<br>c. Account management procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-2).<br>d. Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).<br>e. Accounts are not properly issued to new users (NIST 800-53, AC-2).<br>f. Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).<br>g. Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).<br>h. Agency has not adequately 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).<br>i. Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).<br>j. Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).<br>k. Network devices are not properly authenticated (NIST 800-53, IA-3). | |

| | |
|---|---|
| **l. The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies.**<br>**m. Use of shared privileged accounts is not necessary or justified.**<br>**n. When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group.**<br>**o. Other**<br>**p. Explanation for Other** | |
| **22. Comments:** | DHS has not yet fully implemented required multi-factor authentication across the Department. DHS has issued HSPD 12 PIV compliant cards to all employees and contractors across the Department. However, the Department is not utilizing PIV compliant cards to access all its information systems, and plans to achieve only 20 percent compliance by the end of FY 2012. |

# Appendix K
# Status of Continuous Monitoring Program

| Section 9: Status of Continuous Monitoring Program | |
|---|---|
| | Response: |
| 23. Check one:<br>A. The Agency has 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. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for continuous monitoring.<br>2. Documented strategy and plans for continuous monitoring.<br>3. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.<br>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 POA&M additions and updates with the frequency defined in the strategy and/or plans. | ✓ |
| B. The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency has not established a continuous monitoring program. | |
| 24. If B. is checked above, check areas that need significant improvement:<br>a. Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).<br>b. Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).<br>c. Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).<br>d. Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).<br>e. Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).<br>f. The following were not provided to the authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).<br>g. Other<br>h. Explanation for Other | |

| | |
|---|---|
| **25. Comments:** | DHS has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with applicable NIST guidance. For example, we determined:<br>• DHS' continuous monitoring program is focused at the asset level, which includes the monitoring of system vulnerabilities, configuration settings, malware, patch information, hardware, and software installed on its systems.<br>• DHS collects component data through manual and automated processes that is compiled into a monthly FISMA scorecard. The scorecard provides an information security grade that is comprised of various continuous monitoring metrics (i.e., security authorization, weakness remediation, asset management). |

# Appendix L
# Status of Contingency Planning Program

| Section 10: Status of Contingency Planning Program | |
|---|---|
| | Response: |
| 26. Check one:<br>A. The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.<br>2. The agency has performed an overall Business Impact Analysis (BIA).<br>3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.<br>4. Testing of system specific contingency plans.<br>5. The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.<br>6. Development of test, training, and exercise (TT&E) programs.<br>7. Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.<br>8. After-action report that addresses issues identified during contingency/disaster recovery exercises.<br>9. Systems that have alternate processing sites.<br>10. Alternate processing sites are subject to the same risks as primary sites.<br>11. Backups of information that are performed in a timely manner.<br>12. Contingency planning that consider supply chain threats. | ✓ |
| B. The Agency has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency has not established a business continuity/disaster recovery program. | |
| 27. If B. is checked above, check areas that need significant improvement:<br>a. Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (NIST 800-53: CP-1).<br>b. Contingency planning procedures are not fully developed (NIST 800-53: CP-1).<br>c. Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34).<br>d. An overall business impact assessment has not been performed (NIST SP 800-34).<br>e. Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).<br>f. A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).<br>g. A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).<br>h. System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).<br>i. Systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53). | |

| | |
|---|---|
| j. Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-34, NIST 800-53).<br>k. Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).<br>l. After-action report did not address issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).<br>m. Systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).<br>n. Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).<br>o. Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).<br>p. Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).<br>q. Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).<br>r. Contingency planning does not consider supply chain threats.<br>s. Other<br>t. Explanation for Other | |
| 28. Comments: | |

# Appendix M
# Status of Agency Program to Oversee Contractor Systems

| Section 11: Status of Agency Program to Oversee Contractor Systems | |
|---|---|
| | Response: |
| 29. Choose one:<br>A. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:<br>1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.<br>2. The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and agency guidelines.<br>3. A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.<br>4. The inventory identifies interfaces between these systems and Agency-operated systems.<br>5. The Agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.<br>6. The inventory of contractor systems is updated at least annually.<br>7. Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. | ✓ |
| B. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud. However, the Agency needs to make significant improvements as noted below. | |
| C. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud. | |

# Appendix N
# Status of Security Capital Planning Program

| Section 12: Status of Security Capital Planning Program | |
|---|---|
| | **Response:** |
| **32. Check one:**<br>**A. The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**<br>1. **Documented policies and procedures to address information security in the capital planning and investment control process.**<br>2. **Includes information security requirements as part of the capital planning and investment process.**<br>3. **Establishes a discrete line item for information security in organizational programming and documentation.**<br>4. **Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.**<br>5. **Ensures that information security resources are available for expenditure as planned.** | ✓ |
| **B. The Agency has established and maintains a capital planning and investment program. However, the Agency needs to make significant improvements as noted below.** | |
| **C. The Agency does not have a capital planning and investment program.** | |
| **33. If B. is checked above, check areas that need significant improvement:**<br>**a. CPIC information security policy is not fully developed.**<br>**b. CPIC information security procedures are not fully developed.**<br>**c. CPIC information security procedures are not consistently implemented.**<br>**d. The Agency does not adequately plan for IT security during the CPIC process (SP 800-65).**<br>**e. The Agency does not include a separate line for information security in appropriate documentation (NIST 800-53: SA-2).**<br>**f. Exhibits 300/53 or business cases do not adequately address or identify information security costs (NIST 800-53: PM-3).**<br>**g. The Agency does not provide IT security funding to maintain the security levels identified.**<br>**h. Other**<br>**i. Explanation for Other** | |

| | |
|---|---|
| **34. Comments:** | DHS maintains a security capital planning and investment program for information security. For example:<br>• DHS bases its CPIC process 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 managing Federal capital assets.[18]<br>• DHS has developed an automated process to help ensure that the department's IT and non-IT investments are successfully managed, cost effective, and support DHS' mission and strategic goals.<br>• DHS produces a supplementary budgetary document known as an exhibit 53b which specifically outlines the Department's information security costs. |

[18] OMB's Circular A-11, Part 7 – *Planning, Budgeting, Acquisition, and Management of Capital Assets,* June 2008.

## Appendix O
## Major Contributors to This Report

Chiu-Tong Tsang, Director
Aaron Zappone, Team Lead
Amanda Strickler, IT Specialist
Michael Kim, IT Auditor
David Bunning, IT Specialist
Pachern Thapanawat, IT Auditor
Greg Wilson, Management/Program Assistant
Thomas Rohrback, Referencer

## Appendix P
## 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
Acting 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 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: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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