



# Department of Homeland Security Office of Inspector General

## Evaluation of DHS' Information Security Program for Fiscal Year 2011





Homeland  
Security

September 27, 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (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.

This report addresses the strengths and weaknesses of controls over the information security program and practices at DHS. It is based on interviews with selected program officials at the Department and components, direct observations, a review of applicable documents, and system testing.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "Frank Deffer".

Frank W. Deffer  
Assistant Inspector General  
Information Technology Audits

# Table of Contents/Abbreviations

---

Executive Summary .....	1
Background .....	2
Results of Independent Evaluation .....	3
Recommendations .....	22
Management Comments and OIG Analysis .....	22

## Appendices

Appendix A: Purpose, Scope, and Methodology.....	25
Appendix B: Management Response to Draft Report.....	27
Appendix C: System Inventory .....	29
Appendix D: Status of Risk Management Program .....	32
Appendix E: Status of Configuration Management Program .....	34
Appendix F: Status of Incident Response and Reporting Program .....	36
Appendix G: Status of Security Training Program.....	38
Appendix H: Status of Plans of Actions and Milestones Program.....	40
Appendix I: Status of Remote Access Program.....	42
Appendix J: Status of Account and Identity Management Program.....	44
Appendix K: Status of Continuous Monitoring Program.....	46
Appendix L: Status of Contingency Planning Program.....	47
Appendix M: Status of Agency Program to Oversee Contractor Systems.....	49
Appendix N: Status of Security Capital Planning Program .....	51
Appendix O: Major Contributors to this Report.....	53
Appendix P: Report Distribution .....	54

## Abbreviations

ATO	authority to operate
CBP	Customs and Border Protection
CIO	Chief Information Officer
CIS	Citizenship and Immigration Services
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center

# Table of Contents/Abbreviations

---

FY	fiscal year
HSPD-12	Homeland Security Presidential Directive 12
ICE	Immigration and Customs Enforcement
I&A	Office of Intelligence and Analysis
ISO	Information Security Office
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 Actions and Milestones
S&T	Science and Technology
SP	Special Publication
TSA	Transportation Security Administration
USCG	United States Coast Guard
USGCB	United States Government Configuration Baseline
USSS	United States Secret Service

# OIG

---

*Department of Homeland Security  
Office of Inspector General*

## **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. Fieldwork was performed 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 2011 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.

While these efforts have resulted in some improvements, components are still 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 configuration management, incident detection and analysis, specialized training, account and identity management, continuous monitoring, and contingency planning.

We are making five recommendations to the Department. The Chief Information Security Officer concurred with all of our recommendations and has already begun to take actions to implement them. The Department's response is summarized and

---

evaluated in the body of this report and included, in its entirety, as appendix B.

## Background

Due to the increasing threat to information systems and the highly networked nature of the federal computing environment, the 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, the Congress enacted Title III of the *E-Government Act of 2002* (Public Law 107-347, Sections 301-305) to improve security within the federal government. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Title III of the *E-Government Act*, entitled 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 agency's security program should protect the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As specified in FISMA, agency heads are charged with conducting an annual evaluation of information programs and systems under their purview, as well as an assessment of related security policies and procedures. Offices of Inspector General (OIG) must independently evaluate the effectiveness of an agency's information security program and practices on an annual basis.

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 issued in June 2011.

---

The Chief Information Security Officer (CISO) leads the Information Security Office (ISO) and is responsible for managing DHS' information security program. To aid in managing its security program, the CISO developed the *Fiscal Year 2011 DHS Information Security Performance Plan* to enhance DHS' information security program and continue to make additional improvements on existing processes, such as continuous monitoring, system security authorizations, and plan of actions and milestones (POA&M) remediation. DHS uses enterprise management tools 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.<sup>1</sup> DHS' 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 Independent 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, account and identity management, continuous monitoring, contingency planning, and Capital Planning and Investment Control (CPIC) programs across 13 components and offices.<sup>2</sup> We separated the results of our evaluation into these key areas. For each area, we identified the progress that DHS has made since our fiscal year (FY) 2010 evaluation and any issues that need to be addressed to be more successful in the respective information security program area.

---

<sup>1</sup> 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 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.

<sup>2</sup> Customs and Border Protection (CBP), Citizenship and Immigration Services (CIS), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration and Customs Enforcement (ICE), Office of Intelligence and Analysis (I&A), Management Directorate (MGMT), National Protection and Programs Directorate (NPPD), OIG, Science and Technology (S&T), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service (USSS).

---

This report also includes the results of a limited number of systems evaluated during the year and our on-going financial statement review.<sup>3</sup> In addition, it includes the results of our security audits at NPPD and TSA.<sup>4</sup>

## **OVERALL PROGRESS**

DHS continued to improve its information security program during FY 2011. For example, the CISO:

- Developed the *DHS IT Security Continuous Monitoring Strategy: An Enterprise View* in January 2011. This document outlined the Department's strategy for implementing an enterprise-wide continuous monitoring and response capability for IT security.
- Revised 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.
- Revised the FISMA scorecard to better evaluate the Department's information security program with increased emphasis on continuous monitoring, further aligning with OMB and NIST priorities. The revised FISMA scorecard includes asset reporting, security authorization, weakness management, vulnerability management, configuration management, Security Operations Center effectiveness, and log integration. These seven metrics contribute to the components overall information security grade. See figure 1 for the Department's July 2011 information security scorecard.

---

<sup>3</sup> *Information Technology Management Letter for the FY 2010 DHS Financial Statement Audit* (OIG-11-103, August 2011).

<sup>4</sup> *Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure* (OIG-11-89, June 2011) and *Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices* (OIG-11-99, July 2011).



**Figure 1: July 2011 FISMA Information Security Scorecard**

	General Support Systems	Major Applications	Major Applications Reported in DC1 or DC2	HSPD-12		Asset Reporting	Security Authorization (formerly C&A)	Weakness Management	Vulnerability Management	Configuration Management	SOC Effectiveness	Log Integration	PIA	SORN	Information Security Grade
				Target	Actual										
CBP	27	48	0	NP	27%	92%	87%	88%	67%	82%	80%	100%	43%	77%	85%
DHS HQ	19	25	29	NP	54%	77%	85%	77%	77%	85%	100%	100%	87%	92%	85%
FEMA	17	55	3	NP	33%	69%	73%	80%	53%	26%	100%	100%	76%	95%	72%
FLETC	6	8	0	P	68%	93%	90%	100%	93%	100%	80%	100%	33%	100%	93%
ICE	18	46	4(29)	P	56%	79%	71%	81%	100%	56%	100%	100%	77%	96%	84%
NPPD	14	27	6	NP	54%	93%	70%	83%	88%	53%	100%	100%	100%	100%	84%
OIG	2	1	0	NP	54%	100%	90%	100%	100%	100%	100%	100%	100%	100%	98%
S&T	11	20	10	NP	54%	83%	84%	93%	72%	14%	100%	100%	100%	100%	80%
TSA	23	56	24	P	57%	100%	100%	89%	92%	94%	100%	100%	88%	100%	97%
USCG	74	64	0	P	99%	49%	83%	88%	39%	19%	100%	100%	96%	100%	68%
USCIS	16	36	0	P	66%	79%	50%	90%	0%	0%	60%	100%	83%	89%	34%
USSS	4	7	0	NP	35%	91%	85%	90%	73%	56%	60%	100%	25%	100%	80%
Department	238	399	76(29)	--	58%	78%	81%	83%	64%	50%	93%	100%	79%	94%	79%

**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 in order to strengthen DHS’ security posture. For example, the CISO did not issue the *Fiscal Year 2011 DHS Information Security Performance Plan* until June 2011. The delay in issuing the performance plan has caused confusion among components, as they were not sure which area of their information security programs they should focus on, or which security controls they should test. One component indicated that it had to delay its annual key control reviews until DHS finalized the performance plan. Thus, the delay in issuing the performance plan limited the components’ ability to complete their testing requirements in FY 2011. According to ISO personnel, the delay in issuing the performance plan was caused by OMB’s revised FISMA reporting requirements, which emphasized “continuous monitoring.”<sup>5</sup>

<sup>5</sup> NIST defines “continuous monitoring” as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Continuous monitoring, which is a critical aspect of the organization-wide risk management process, is most effective when automated mechanisms are employed where possible. It can support frequent updates to security plans, security assessment reports, POA&M, hardware and software inventories, and other system information. In addition, a well defined continuous monitoring strategy supports operational processes, such as incident response, configuration management, identity and access management, and strategies for addressing threats.

---

Further, we determined that components are not satisfying all of the Department's information security policies, procedures, and practices. For example, identified deficiencies (i.e., POA&M, security authorization) revealed that not all components are sustaining their information security programs on a year-round basis or performing continuous monitoring as required. In addition, we determined that 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 are operating information systems whose authority to operate (ATO) has expired. For example, we identified 49 unclassified systems with expired ATOs, and some systems have been operating without a valid ATO since 2008.
- As of July 2011, CIS is maintaining an overall FISMA information security score of 34%.
- Components have not incorporated all known information security weaknesses into POA&Ms for the Department's unclassified and classified systems.
- Artifacts supporting authorization of unclassified and classified systems were missing key information or were outdated, restricting the ability of authorizing officials to make credible risk-based decisions.
- Components have not implemented all required DHS baseline configuration, Federal Desktop Core Configuration (FDCC), and United States Government Configuration Baseline (USGCB) settings on the information systems selected for review.<sup>6</sup>

---

<sup>6</sup> OMB Memorandum M-07-11 *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* requires federal agencies to implement minimum baseline FDCC settings on all Microsoft Windows XP workstations. USGCB replaces FDCC and provides the baseline settings for Microsoft Windows 7 and Internet Explorer 8 that federal agencies are required to implement for security reasons.

---

## **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 2011, DHS has a total of 625 systems, which include a mix of major applications and general support systems that are classified as “Sensitive But Unclassified,” “Secret,” and “Top Secret.”
- As of June 2011, DHS has conducted 102 component site visits as part of the annual refresh process.

### **ISSUES TO BE ADDRESSED**

- As of July 2011, DHS has not established an automated capability to keep track of the hardware devices and software deployed at all component sites.
- DHS did not determine whether components had developed new classified systems during site visits as part of the annual inventory refresh process. As a result, DHS cannot be sure that it has an accurate inventory of its classified systems.

See appendix C, System Inventory and appendix M, Status of Agency Program to Oversee Contractor Systems.

## **Risk Management Program**

As part of its risk management program, DHS follows the guidance outlined in 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 national security systems, components follow the Defense Information Assurance Certification and Accreditation Process and *DHS Sensitive Systems Policy Directive 4300B* policy. Components are required to use the Department’s enterprise-wide management tools to incorporate NIST recommended security controls required for its system security authorizations. In addition, DHS requires components to upload security artifacts into its enterprise management tools to monitor the progress in authorizing

---

systems to operate. The artifacts include: ATO letter, system security plan, security assessment report, security test and evaluation, contingency plan, contingency plan test results, Federal Information Processing Standards (FIPS) 199 determination, E-authentication determination, privacy threshold analysis/privacy impact assessment, and NIST SP 800-53 self-assessments.

For some of the systems that were granted ATO, the artifacts that are required to support the authorization were either missing, incomplete, or outdated. We identified a similar issue in our FY 2008, FY 2009, and FY 2010 FISMA reports.<sup>7</sup>

### PROGRESS

- The overall quality of security authorization documentation has improved in FY 2011, compared with FY 2010. For example, we identified fewer deficiencies within the security authorization documentation for the systems that were selected for review.

### ISSUES TO BE ADDRESSED

- We selected 28 systems from 12 components and offices to evaluate the quality of documents that support DHS' security authorization process. Our review revealed that the component CISOs have not performed adequate reviews to ensure that the artifacts contain the required information to meet all applicable DHS, OMB, and NIST guidelines. For some of the systems that were granted ATO, the artifacts that are required to support the authorization were either 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:
  - Two operational systems did not have signed ATO letters.
  - Components did not complete the FIPS-199 categorization worksheet tool correctly or did not update the categorization for three systems. The FIPS 199 determination, when applied properly during the

---

<sup>7</sup> *Evaluation of DHS' Information Security Program for Fiscal Year 2008* (OIG-08-94, September 2008), *Evaluation of DHS' Information Security Program for Fiscal Year 2009* (OIG-09-109, September 2009), and *Evaluation of DHS' Information Security Program for Fiscal Year 2010* (OIG-11-01, October 2010).

---

risk assessment process, helps agency officials to select applicable controls for the information systems.

- For 17 system security plans, certain elements are missing, including sections that describe management plans, security controls, emergency changes, and incident handling procedures. In addition, we identified three instances where system security plans were out of date. The system security plan should be current, provide an overview of the information system, and describe the security controls implemented or planned to protect the system.
  - Contingency plans and/or testing reports for six systems are missing certain elements, including the identification of alternate processing facilities, or restoration procedures, and data sensitivity handling procedures at the alternate site or off-site storage.
  - Two systems have outdated or non-existing memorandums of understandings with organizations (external to the component) with which they are sharing data.
  - Seven systems did not have completed and approved privacy threshold analyses.
- During our NPPD audit, we reviewed the authorization packages for two systems to determine whether the systems were granted an ATO in compliance with applicable OMB, NIST, and DHS requirements. We reported in June 2011 that one system was operating without a valid ATO and its security documentation was outdated.<sup>8</sup>

See appendix D for our assessment of 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 the results are provided to components daily. Despite these efforts, components are not entering and tracking all IT security weaknesses in DHS'

---

<sup>8</sup> *Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure* (OIG-11-89, June 2011).

---

unclassified and classified enterprise management tools, nor are all of the data entered by the components accurate and updated in a timely manner.

### PROGRESS

- Components have created POA&Ms for all 153 notice of findings and recommendations for the weaknesses identified during the FY 2010 financial statement audit.<sup>9</sup>

### 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 corrected by the components. We identified similar problems in our FY 2009 and FY 2010 FISMA reports.
- In FY 2011, 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 for the security vulnerabilities identified on its "Top Secret" systems and are managed in accordance with the Department's policies and procedures.
- DHS requires components to develop a POA&M for its operational systems that have not received an ATO. We identified instances where POA&Ms have not been created for operational systems that have not received an ATO. For example, one system has been operating since September 2008 without a valid ATO and no POA&M has been created to obtain the authorization.
- Based on our analysis of data from DHS' enterprise management tools, component CISOs and information system security officers are not maintaining current information as to

---

<sup>9</sup> *Information Technology Management Letter for the FY 2010 DHS Financial Statement Audit* (OIG-11-103, August 2011).

---

the progress of security weakness remediation, and not all POA&Ms are being resolved in a timely manner. As of June 30, 2011, 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 have been identified for remediation. Priority 4 weaknesses are assigned to initial audit findings and priority 5 weaknesses are assigned to repeat audit findings. As of June 30, 2011, only 192 (68%) of 284 priority 4 and 5 POA&Ms have been reviewed and approved by a component CISO.
- Component CISOs are not updating information concerning all weaknesses where the estimated completion date has been delayed. Of the 4,559 open POA&Ms with estimated completion dates, 768 (17%) were delayed by at least 3 months (prior to April 1, 2011). Furthermore, 255 POA&Ms had an estimated completion date more than 1 year old, dating as far back as January 2008.
- DHS requires that a reasonable resources estimate of at least \$50 be provided to mitigate the weakness identified. Resources required for the remediation of 103 (2%) of 4,559 open POA&Ms were either not identified or did not meet the \$50 requirement.
- 399 (9%) of 4,559 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.

#### Secret POA&Ms

- 37 of 70 open POA&Ms are delayed. For example, 28 (76%) of 37 delayed POA&Ms are more than 1 year past due.

- 
- 38 (54%) of 70 open POA&Ms have not been updated within the past 90 days. DHS requires POA&Ms to be updated at least monthly.

See appendix H for the evaluation of DHS' POA&M Program.

### **Configuration Management**

We reviewed 41 systems, including servers and databases to evaluate the compliance with DHS baseline configuration requirements. Additionally, we evaluated the compliance with FDCC and USGCB requirements at CIS, FEMA, FLETC, ICE, MGMT, NPPD, OIG, S&T, TSA, USCG and USSS. Results from our testing indicated that components have not implemented all of the required DHS baseline configuration settings. We reported a similar issue in our FY 2009 and FY 2010 reports.

Additionally, we conducted testing across DHS' wide-area network, known as OneNet, using Network Mapper to search for vulnerable ports and services to test the Security Operations Center's response to an unannounced network scan. We also evaluated router configuration files on four gateway routers that provide access to OneNet.

### **PROGRESS**

- Three components (FLETC, TSA, and USCG) are more than 90% compliant with FDCC configuration settings.
- Components have established pilot programs to deploy USGCB-compliant configuration settings on their Windows 7 workstations.

### **ISSUES TO BE ADDRESSED**

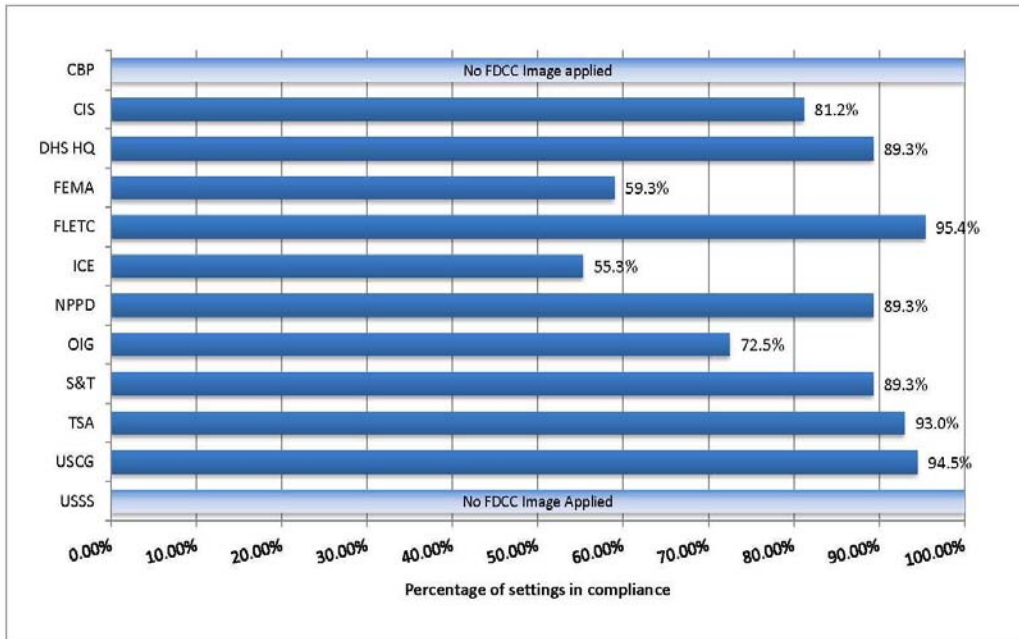
- Results from our configuration reviews indicated that components had not fully configured their systems based on DHS' secure baseline configuration guidelines. Components included CBP, CIS, FEMA, ICE, MGMT, NPPD, S&T, TSA, USCG, and USSS. Deficiencies identified include:
  - Insecure Windows authentication protocols are in use.



- Oracle databases were not consistently compliant with DHS secure baseline configuration guides. For example, our review of 8 databases revealed that 36 out of 80 settings were non-compliant.
- Linux password management is not in compliance with DHS guidance.
- Simple Network Management Protocol, a network management tool, is in use despite being expressly prohibited by DHS. We reported a similar issue in our FY 2010 report.

Components have not fully implemented all FDCC settings. For example, we identified six specific FDCC settings (five Internet Explorer 7, one Microsoft Outlook) that were not applied at the components. If these settings are not implemented, DHS may be vulnerable to computer viruses or social engineering attacks. Figure 2 summarizes the Department’s FDCC compliance.

**Figure 2: Component FDCC Compliance<sup>10</sup>**



<sup>10</sup> DHS Headquarters, NPPD and S&T are all managed by the same policy. As a result, these three components will have identical compliance for FDCC and USGCB settings. CBP, ICE and USSS currently have no plans to implement an FDCC-compliant image and are instead focusing efforts on USGCB compliance.

- 
- Although components are developing and implementing USGCB-compliant Windows 7 images, no component is using Windows 7 as the primary operating system for its workstations. Further, none of the images that we evaluated were 100% USGCB compliant.
  - Gateway routers for OneNet were not configured according to all DHS policies. The following deficiencies were identified:
    - The minimum password length requirement for the local user on two routers was configured to one character.
    - A weak password encryption algorithm is being used for a local user on one router.
    - DHS guidance requires that only one local user account be defined for disaster recovery when using an authentication server. Two of the routers were configured with two local user accounts. Having more than one disaster recovery account is unnecessary and creates additional avenues of attack.
  - During our NPPD audit, we identified several system configuration and account access vulnerabilities that may lead to risks associated with internal and external threats, unauthorized access, and misuse of the Department's critical infrastructure information.
  - We reported in July 2011 that TSA had not implemented DHS baseline configuration controls on all of its wireless devices and supporting infrastructure systems.

See appendix E for a summary of DHS' configuration management.

---

## **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 has increased by 13%, from 1,402 in FY 2010 to 1,589 in FY 2011.<sup>11</sup> For example, the number of malicious code attacks on DHS systems increased from 180 to 602 between 2008 and 2009.<sup>12</sup> However, DHS has not fully implemented its department-wide vulnerability assessment program to evaluate the security posture at all components.

### **PROGRESS**

- DHS continues to implement its vulnerability assessment program. For example, the DHS Security Operations Center has the ability to perform full credential scanning on workstations and servers at CBP, CIS, and FLETC.<sup>13</sup>
- The DHS Security Operations Center logged all traffic resulting from our unannounced scan on OneNet.

### **ISSUES TO BE ADDRESSED**

- DHS has not deployed its vulnerability assessment program department-wide. The program includes a comprehensive vulnerability alert, assessment, remediation, and reporting process to effectively identify computer security vulnerabilities and track mitigation efforts to resolution. However, the DHS Security Operations Center has no access at FEMA, ICE, OIG, S&T, USCG, and USSS. As a result, DHS cannot perform vulnerability assessments on all component workstations and servers to evaluate the effectiveness of controls implemented.
- During FY 2011, I&A, NPPD, Office of Operations Coordination and Planning, OIG, and USSS did not submit weekly incident reports to the DHS Security Operations Center, as required.

---

<sup>11</sup> We evaluated the number of incidents reported by the Security Operations Center between October 1<sup>st</sup> and May 31<sup>st</sup> for both FY 2010 and FY 2011.

<sup>12</sup> *State of Cybersecurity at DHS*, December 15, 2010.

<sup>13</sup> Full credential scanning involves unrestricted access to component networks and enables the use of software tools (i.e., Nessus, WebInspect) to perform comprehensive vulnerability scans.

- 
- Although the DHS Security Operations Center logged all traffic resulting from our unannounced scan on OneNet, the scan was not immediately identified and terminated.

See appendix F for information regarding DHS' Incident Response and Reporting Program.

### **Security Training Program**

The CISO has established a process to validate components' security training and has taken a more active role in developing the content for DHS training requirements. During FY 2011, DHS developed and implemented specialized training courses for those with significant IT security responsibilities. However, specific training content for system owners and authorizing officials has yet to be finalized.

### **PROGRESS**

- DHS has developed and implemented specialized training courses for information system security officers and system administrators in FY 2011. As of July 2011, DHS had conducted eight information system security officer and two system administrator training sessions.

### **ISSUES TO BE ADDRESSED**

- DHS has not yet finalized and implemented its specialized training courses for system owners and authorizing officials.
- DHS uses an enterprise management tool to identify and track the status of specialized training for all personnel with significant information security responsibilities, as described in NIST SP 800-50 and NIST SP 800-16.<sup>14</sup> Four components (CIS, ISO, S&T, and USCG) are maintaining a completion percentage of 35% or below for all personnel with significant IT security responsibilities.

---

<sup>14</sup> NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003 and NIST SP 800-16, *Information Technology Security Training Requirements: A Role - and Performance-Based Model*, April 1998.

---

See appendix G for information regarding 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 and audit logging capabilities to protect sensitive information throughout transmission. All components utilizing remote access have developed policies to outline the controls needed to protect remote connections (i.e., multi-factor authentication, firewalls) from external threats.

See appendix I for DHS' Remote Access Program.

### **Account and Identity Management Program**

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. However, DHS plans to implement Homeland Security Presidential Directive 12 (HSPD-12) personal identification verification credentials enterprise-wide, which will be used to provide agency-wide system access management by the end of FY 2011.<sup>15</sup>

### **PROGRESS**

- As of July 2011, DHS has issued more than 244,000 HSPD-12 compliant cards across the Department.
- Five components (CIS, DHS Headquarters, FEMA, FLETC, and TSA) have issued HSPD-12 compliant cards to all employees and contractors.

---

<sup>15</sup> According to NIST FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006, a personal identity verification card is a form of standard identification credentials issued by the Federal government to its employees and contractors. The personal identity verification credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications.

---

## ISSUES TO BE ADDRESSED

- OMB granted DHS an exception from the requirement that agencies issue personal identity verification credentials to current employees and contractors and use the credentials for both physical and logical access by October 27, 2008. However, DHS is not scheduled to complete the issuance of HSPD-12 compliant cards to all its employees and contractors until September 30, 2011, three years after OMB's original due date.<sup>16</sup>
- In response to OMB's requirement that agencies upgrade existing physical and logical access control systems to use PIV credentials by the beginning of FY 2012, the DHS Identity, Credential and Access Management Program Management Office requested components to develop a credential implementation plan by July 31, 2011.<sup>17</sup> However, as of August 2011, four components (CBP, DHS Headquarters, FEMA, and USSS) have not submitted implementation plans.

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

## Continuous Monitoring Program

During FY 2011, DHS made significant changes to its enterprise-wide continuous monitoring program. For example, in FY 2010, the Department's continuous monitoring program focused on key control reviews, contingency testing, incident response reporting, and ongoing annual security control testing on its FISMA reportable information systems. However, beginning in FY 2011, DHS shifted its focus on continuous monitoring to the asset level, which includes the monitoring of system vulnerabilities, configuration settings, malware, patch information, hardware, and software installed on its systems. As of August 2011, CISO has performed 60 critical control reviews on selected information systems to ensure that key controls have been

---

<sup>16</sup> *Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12* (OIG-10-40, January 2010).

<sup>17</sup> OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011.

---

implemented and to help components identify potential weaknesses or vulnerabilities.

### PROGRESS

- DHS has developed policies and procedures to implement its continuous monitoring functions and requirements. For example, the CISO developed the *DHS IT Security Continuous Monitoring Strategy: An Enterprise View* in January 2011.
- As part of its effort to establish a robust, enterprise-wide continuous monitoring program, DHS has revised its information security scorecard to include asset reporting, Security Operations Center effectiveness, and log integration.

### ISSUES TO BE ADDRESSED

- Self-assessments have yet to be completed for 13 systems as DHS has not identified the key controls.
- DHS and its components have not established a real-time and automated continuous monitoring capability to keep track of all hardware and network devices, external connections, and software associated with their information systems.
- As of June 2011, three components (CIS, NPPD, and USSS) have information security scores of 60% or below for the Security Operations Center metric.<sup>18</sup>
- Components have not provided authorizing officials with up-to-date security documentation. For example, our review of 28 system security plans identified three instances where documentation was out of date. Without current information, authorizing officials cannot make a credible risk-based decision on whether to authorize the system.

See appendix K for DHS' Continuous Monitoring Program.

---

<sup>18</sup> Security Operations Center effectiveness is a key metric for the Department's continuous monitoring program. Several factors are included in this metric, including 1) participation in daily headquarters security operations center calls; 2) access to classified networks within 30 minutes; 3) development of service-level agreements between components and Security Operations Center; 4) monthly incident reviews; and 5) components' ability to provide 24x7x365 continuous monitoring and real-time response.

---

## Contingency Planning Program

DHS has established and is maintaining an entity-wide business continuity and contingency planning program. However, components have not complied with all DHS' contingency planning requirements.

### PROGRESS

- DHS has developed training, testing, and exercise approaches for its business continuity and disaster recovery programs. For example, DHS and its components participated in the federal government continuity exercise in June 2011 to test activation continuity plans, systems and procedures, and mission-essential functions.
- DHS has developed a business impact assessment that incorporates the Department's mission essential functions and primary mission essential functions.

### ISSUES TO BE ADDRESSED

- DHS has not updated the *Department of Homeland Security Headquarters Continuity of Operations Plan* since 2008. According to an official from the DHS Business Continuity and Emergency Preparedness Branch, the continuity plan is being revised.
- 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. Our review of 28 security authorization packages revealed that contingency plans and/or testing reports for six systems are missing certain elements, including the identification of alternate processing facilities, or restoration procedures, and data sensitivity handling procedures at the alternate site or offsite storage. In addition, one contingency plan is out of date.

See appendix L for DHS' Contingency Planning Program.



---

## Security Capital Planning Program

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.<sup>19</sup> In addition, DHS developed the *CPIC Guide* in August 2010. The 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. In addition, DHS has also implemented an Information Technology Acquisition Review process which requires that any proposed IT acquisition of \$2.5 million and above be reviewed and approved by the DHS Chief Information Officer (CIO). Finally, 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.

### PROGRESS

- In January 2011, DHS issued the *DHS Capital Planning & Investment Control - OMB Exhibit 300/DHS Business Case Guidebook* to provide agency program and investment managers with guidance and best practices for preparing the OMB Exhibit 300/DHS Business Case.
- DHS requires components to complete an Exhibit 300 for all major IT investments, which includes estimated information security costs. During FY 2011, the Department completed 94 Exhibit 300s for its major IT investments.
- DHS has developed the FY 2012 Exhibit 53B which identifies the Department's enterprise-wide information security costs for its IT investments. For example, the FY 2012 Exhibit 53B identifies the staffing costs for personnel with information security responsibilities and costs associated with IT security tools (i.e., anti-virus software, intrusion detection systems, and web-filtering software), annual FISMA testing, network

---

<sup>19</sup> OMB's Circular A-11, Part 7 – *Planning, Budgeting, Acquisition, and Management of Capital Assets*, June 2008.

---

penetration, security awareness training, and the authorization of an information system.

## **Recommendations**

We recommend that the CISO:

**Recommendation #1:** Improve the ISO review process to ensure that POA&Ms, including those for classified systems, are complete and current.

**Recommendation #2:** Include all applicable controls in the security documentation when authorizing systems. Systems authorized with outdated documents or without all applicable controls should not be accepted by the Department.

**Recommendation #3:** Improve the process to implement and maintain DHS baseline configuration requirements on all systems. The process should include testing and the use of automated tools and security templates.

**Recommendation #4:** Evaluate and revise the Department's current FDCC implementation strategy to ensure that the requirements outlined in OMB M-07-11 and M-07-18 are implemented expeditiously.

**Recommendation #5:** In accordance with applicable OMB and NIST guidance, develop a strategy to implement an automated continuous monitoring process for tracking the Department's inventory, including hardware devices, external connections, and software installed on DHS systems. In addition, the continuous monitoring program should include performing periodic testing to evaluate the security posture at all components.

## **Management Comments and OIG Analysis**

### **Management Comments to Recommendation #1**

DHS concurred with recommendation 1. The Information Security Office's (ISO) POA&M process is being further improved to ensure that all POA&Ms, including those POA&Ms for classified systems, are complete and current. Improvements include the implementation of the *FY 2011 Information Security Performance*

---

*Plan* automated POA&M quality review checks. These include checking for the existence of POA&Ms for identified security control weaknesses, timely updates and completion of POA&Ms, and reasonableness of estimated remediation costs. Manual reviews of POA&Ms are also being conducted to ensure they meet the remaining criteria identified in the *DHS 4300A Sensitive Systems Handbook, POA&M Process Guide*.

**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 security document templates are generated with the applicable controls by the DHS security authorization tool at the time the security authorization process is initiated. Enhancements to the DHS compliance tool scheduled for the end of FY 2011 will implement more stringent controls that prevent the upload of outdated documents.

Additionally, the required security authorization documents are reviewed by the ISO Document Review Team to ensure that all applicable controls are included and adequately addressed.

Documents identified as outdated or which lack all applicable controls by the Team are returned to the Component for corrective action.

**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. In FY 2011, configuration management focused on establishing and maintaining consistency of baseline configurations and inventories of organizational information systems. The CISO's strategy for achieving automated compliance reporting of baseline configuration requirements was described in the *"IT Security Continuous Monitoring Strategy: An Enterprise View"* and implemented in FY2011 as part of the continuous monitoring High Priority Initiative 11-14. Additionally, the DHS FY2011

---

Information Security Scorecard was revised to show Component status towards meeting the DHS configuration requirements. Periodic testing and use of automated tools and security templates to evaluate the security posture at DHS are also being implemented as part of the strategy.

**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. DHS continues to make progress in implementing the FDCC requirements outlined in OMB M-07-11 and M-07-18. The Desktop Working Group tracks and monitors component progress on FDCC implementation. The expected completion date for implementing FDCC has been revised to December 31, 2011, for all DHS components.

**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 CISO has developed and issued “*IT Security Continuous Monitoring Strategy: An Enterprise View*,” v1.0, to achieve an automated and real-time monitoring process for the Department’s inventory, including hardware devices, external connections, and software installed on its systems that complies with applicable OMB and NIST guidance. The strategy also addresses the need to perform periodic testing to evaluate the security posture at DHS.

**OIG Analysis**

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and closed.

## Appendix A

### Purpose, Scope, and Methodology

---

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 2011 reporting instructions dated June 2011. We conducted our fieldwork at the departmental level and at DHS' organizational components and offices, including CBP, CIS, FEMA, FLETC, I&A, ICE, MGMT, NPPD, OIG, S&T, TSA, USCG, and USSS.

In addition, we conducted reviews of DHS' information systems and security program-related areas throughout FY 2011. This report includes the results of a limited number of systems evaluated during the year and our on-going financial statement review, including our security audits at NPPD and TSA.

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

We reviewed the quality of security authorization packages for a sample of 28 systems at CBP, CIS, FEMA, FLETC, I&A, ICE, MGMT, NPPD, OIG, S&T, TSA, USCG, 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 and compliance with selected NIST SP 800-53 controls for 41 systems at CBP, CIS, FEMA, I&A, ICE, MGMT, NPPD, S&T, TSA, USCG, and USSS. FDCC and

## **Appendix A**

### **Purpose, Scope, and Methodology**

---

USGCB settings for 16 systems were also reviewed at these 11 components.

We conducted our evaluation between April and August 2011 under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency. Major OIG contributors to the evaluation are identified in appendix O.

The principal OIG point of contact for the evaluation is Frank W. Deffer, Assistant Inspector General, IT Audits at (202) 254-4041.

## Appendix B Management Response to Draft Report


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



**Homeland  
Security**

SEP 06 2011

MEMORANDUM FOR: Frank Deffer  
Assistant Inspector General  
Information Technology Audits

FROM: Robert West   
Chief Information Security Officer

SUBJECT: Response to OIG Draft Report: *Evaluation of DHS' Information Security Program for Fiscal Year 2011 - For Official Use Only*  
OIG Project No. 11-039-ITA-MGMT

This memorandum responds to the Office of Inspector General draft report titled, *Evaluation of DHS' Information Security Program for Fiscal Year 2011 - For Official Use Only*, dated September 1, 2011.

The Office of Chief Information Officer concurs with the five recommendations within the report. The following actions are already underway to address these recommendations.

**Recommendation #1:** Improve the ISO review process to ensure that POA&Ms, including those for classified systems, are complete and current.

**DHS CISO concurs:** The Information Security Office (ISO) plan of actions and milestones (POA&M) process is being further improved to ensure that all POA&Ms, including those POA&Ms for classified systems, are complete and current. Improvements include the implementation of the *FY 2011 Information Security Performance Plan* automated POA&M quality review checks. These include checking for the existence of POA&Ms for identified security control weaknesses, timely updates and completion of POA&Ms, and reasonableness of estimated remediation costs. Manual reviews of POA&Ms are also being conducted to ensure they meet the remaining criteria identified in the *DHS 4300A Sensitive Systems Handbook, POA&M Process Guide*.

**Recommendation #2:** Include all applicable controls in the security documentation when authorizing systems. Systems authorized with outdated documents or without all applicable controls should not be accepted by the department.

**DHS CISO concurs:** The security document templates are generated with the applicable controls by the DHS security authorization tool at the time the security authorization process is initiated. Enhancements to the DHS compliance tool scheduled for the end of FY 2011 will

## Appendix B

### Management Response to Draft Report

---

implement more stringent controls that prevent the upload of outdated documents. Additionally, the required security authorization documents are reviewed by the ISO Document Review Team to ensure that all applicable controls are included and adequately addressed. Documents identified as outdated or lack all applicable controls by the Team are returned to the Component for corrective action.

**Recommendation #3:** Improve the process to implement and maintain DHS baseline configuration requirements on all systems. The process should include testing and the use of automated tools and security templates.

**DHS CISO concurs:** In FY2011, configuration management focused on establishing and maintaining consistency of baseline configurations and inventories of organizational information systems. The CISO's strategy for achieving automated compliance reporting of baseline configuration requirements was described in the "*IT Security Continuous Monitoring Strategy: An Enterprise View*" and implemented in FY2011 as part of the continuous monitoring High Priority Initiative 11-14. Additionally, the DHS FY2011 Information Security Scorecard was revised to show Component status towards meeting the DHS configuration requirements. Periodic testing and use of automated tools and security templates to evaluate the security posture at DHS are also being implemented as part of the strategy.

**Recommendation #4:** Evaluate and revise the department's current FDCC implementation strategy to ensure that the requirements outlined in OMB M-07-11 and M-07-18 are implemented expeditiously.

**DHS CISO concurs:** DHS continues to make progress in implementing the FDCC requirements outlined in OMB M-07-11 and M-07-18. The Desktop Working Group tracks and monitors component progress on Federal Desktop Core Configuration (FDCC) implementation. The expected completion date for implementing FDCC has been revised to December 31, 2011, for all DHS components.

**Recommendation #5:** In accordance with applicable OMB and NIST guidance, develop a strategy to implement an automated continuous monitoring process for tracking the department's inventory, including hardware devices, external connections, and software installed on DHS systems. In addition, the continuous monitoring program should include performing periodic testing to evaluate the security posture at all components.

**DHS CISO concurs:** The CISO has developed and issued "*IT Security Continuous Monitoring Strategy: An Enterprise View*", v1.0, to achieve an automated and real-time monitoring process for the department's inventory, including hardware devices, external connections, and software installed on its systems that complies with applicable OMB and NIST guidance. The strategy also addresses the need to perform periodic testing to evaluate the security posture at DHS.

Should you have any questions, please call me at (202) 357-6110, or your staff may contact Emery Csulak, Director of Compliance and Technology at (202) 357-6113.

cc: Chief Information Officer  
Component CIOs  
Component CISOs



**Appendix C  
System Inventory**

Section 1: DHS System Inventory as of June 2011													
Bureau Name	FIPS 199 System Impact Level	a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems) (Column A + Column B)		d. Number of systems receiving authority to operate		e. Number of systems for which security controls have been tested and reviewed in the past year		f. Number of systems for which contingency plans have been tested in accordance with policy	
		Number	Number Reviewed by OIG	Number	Number Reviewed by OIG	Total Number	Total Number Reviewed by OIG	Number	Number Reviewed by OIG	Number	Number Reviewed by OIG	Number	Number Reviewed by OIG
CBP	High	15	3	0	0	15	3	15	3	13	3	13	2
	Moderate	48	2	1	0	49	2	46	2	42	2	42	2
	Low	1	0	2	0	3	0	2	0	2	0	1	0
	Not Categorized	1	0	0	0	1	0	0	0	0	0	0	0
CIS	<b>Sub-total</b>	<b>65</b>	<b>5</b>	<b>3</b>	<b>0</b>	<b>68</b>	<b>5</b>	<b>63</b>	<b>5</b>	<b>57</b>	<b>5</b>	<b>56</b>	<b>4</b>
	High	4	1	5	1	9	2	9	2	9	2	3	2
	Moderate	19	1	16	2	35	3	23	2	26	3	24	3
	Low	1	0	3	1	4	1	4	1	4	1	4	0
DHSHQ	Not Categorized	2	0	0	0	2	0	0	0	0	0	0	0
	<b>Sub-total</b>	<b>26</b>	<b>2</b>	<b>24</b>	<b>4</b>	<b>50</b>	<b>6</b>	<b>36</b>	<b>5</b>	<b>39</b>	<b>6</b>	<b>31</b>	<b>5</b>
	High	8	1	8	0	16	1	14	1	6	1	13	1
	Moderate	11	0	9	1	20	1	19	1	8	1	13	1
FEMA	Low	0	0	3	0	3	0	3	0	1	0	3	0
	Not Categorized	3	0	3	0	6	0	5	0	3	0	1	0
	<b>Sub-Total</b>	<b>22</b>	<b>1</b>	<b>23</b>	<b>1</b>	<b>45</b>	<b>2</b>	<b>41</b>	<b>2</b>	<b>18</b>	<b>2</b>	<b>30</b>	<b>2</b>
	High	19	2	3	0	22	2	17	1	18	2	10	2
	Moderate	32	3	14	0	46	3	44	3	41	3	33	3
	Low	4	0	1	0	5	0	4	0	3	0	3	0

**Appendix C  
System Inventory**

	Not Categorized	10	0	0	0	10	0	5	0	6	0	2	0
	<b>Sub-total</b>	<b>65</b>	<b>5</b>	<b>18</b>	<b>0</b>	<b>83</b>	<b>4</b>	<b>70</b>	<b>4</b>	<b>68</b>	<b>5</b>	<b>48</b>	<b>5</b>
	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	13	4	1	0	14	4	13	4	11	4	14	3
	Low	0	0	0	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	<b>Sub-total</b>	<b>13</b>	<b>4</b>	<b>1</b>	<b>0</b>	<b>14</b>	<b>4</b>	<b>13</b>	<b>4</b>	<b>11</b>	<b>4</b>	<b>14</b>	<b>3</b>
	High	12	1	1	0	13	1	11	1	9	1	8	0
	Moderate	31	3	15	0	46	3	41	3	31	3	33	1
	Low	3	0	0	0	3	0	3	0	2	0	3	0
	Not Categorized	1	0	1	0	2	0	1	0	0	0	0	0
	<b>Sub-total</b>	<b>47</b>	<b>4</b>	<b>17</b>	<b>0</b>	<b>64</b>	<b>4</b>	<b>56</b>	<b>4</b>	<b>42</b>	<b>4</b>	<b>44</b>	<b>1</b>
	High	4	1	8	2	12	3	7	3	9	3	9	3
	Moderate	5	0	21	1	26	1	26	1	24	1	22	1
	Low	1	0	6	0	7	0	3	0	5	0	5	0
	Not Categorized	1	0	0	0	1	0	1	0	0	0	1	0
	<b>Sub-total</b>	<b>11</b>	<b>1</b>	<b>35</b>	<b>3</b>	<b>46</b>	<b>4</b>	<b>37</b>	<b>4</b>	<b>38</b>	<b>4</b>	<b>37</b>	<b>4</b>
	High	2	1	0	0	2	1	2	1	1	1	1	1
	Moderate	0	0	0	0	0	0	0	0	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0	0	0	0
	Not Categorized	1	0	0	0	1	0	1	0	0	0	0	0
	<b>Sub-total</b>	<b>3</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>3</b>	<b>1</b>	<b>3</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>
	High	1	0	0	0	1	0	1	0	1	0	1	0
	Moderate	6	0	13	1	19	1	19	1	15	1	18	1
	Low	2	0	2	0	4	0	3	0	3	0	4	0
	Not Categorized	2	0	0	0	2	0	1	0	2	0	2	0
	<b>Sub-total</b>	<b>11</b>	<b>0</b>	<b>15</b>	<b>1</b>	<b>26</b>	<b>1</b>	<b>24</b>	<b>1</b>	<b>21</b>	<b>1</b>	<b>25</b>	<b>1</b>
	High	20	3	3	0	23	3	23	3	23	3	23	3
	Moderate	28	2	16	0	44	2	44	2	44	2	44	2
	Low	6	0	2	0	8	0	8	0	8	0	8	0

**Appendix C  
System Inventory**

	Not Categorized	4	0	0	0	4	0	0	4	0	0	0	3	0	0	1	0
	<b>Sub-total</b>	<b>58</b>	<b>5</b>	<b>21</b>	<b>0</b>	<b>79</b>	<b>5</b>	<b>79</b>	<b>5</b>	<b>78</b>	<b>5</b>	<b>76</b>	<b>5</b>	<b>5</b>	<b>5</b>	<b>5</b>	
<b>USCG</b>	High	5	1	5	0	10	1	10	1	5	1	10	1	1	1	1	
	Moderate	55	4	20	3	75	7	65	7	39	6	62	5	5	5	5	
	Low	13	0	2	0	15	0	9	0	6	0	13	0	0	0	0	
	Not Categorized	36	0	0	0	36	0	36	0	19	0	2	0	0	0	0	
	<b>Sub-total</b>	<b>109</b>	<b>5</b>	<b>27</b>	<b>3</b>	<b>136</b>	<b>8</b>	<b>120</b>	<b>8</b>	<b>69</b>	<b>7</b>	<b>87</b>	<b>6</b>	<b>6</b>	<b>6</b>	<b>6</b>	
<b>USSS</b>	High	4	2	0	0	4	2	3	2	3	2	2	2	2	2	2	
	Moderate	6	0	0	0	6	0	6	0	6	0	3	0	0	0	0	
	Low	1	0	0	0	1	0	1	0	1	0	0	0	0	0	0	
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	<b>Sub-total</b>	<b>11</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>11</b>	<b>2</b>	<b>10</b>	<b>2</b>	<b>10</b>	<b>2</b>	<b>5</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	
<b>Agency Totals</b>	<b>High</b>	<b>94</b>	<b>16</b>	<b>33</b>	<b>3</b>	<b>127</b>	<b>19</b>	<b>112</b>	<b>18</b>	<b>97</b>	<b>19</b>	<b>93</b>	<b>17</b>	<b>17</b>	<b>17</b>	<b>17</b>	
	<b>Moderate</b>	<b>254</b>	<b>19</b>	<b>126</b>	<b>8</b>	<b>380</b>	<b>27</b>	<b>346</b>	<b>26</b>	<b>287</b>	<b>26</b>	<b>308</b>	<b>22</b>	<b>22</b>	<b>22</b>	<b>22</b>	
	<b>Low</b>	<b>32</b>	<b>0</b>	<b>21</b>	<b>1</b>	<b>53</b>	<b>1</b>	<b>40</b>	<b>1</b>	<b>35</b>	<b>1</b>	<b>44</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	
	<b>Not Categorized</b>	<b>61</b>	<b>0</b>	<b>4</b>	<b>0</b>	<b>65</b>	<b>0</b>	<b>54</b>	<b>0</b>	<b>33</b>	<b>0</b>	<b>9</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	
	<b>Total</b>	<b>441</b>	<b>35</b>	<b>184</b>	<b>12</b>	<b>625</b>	<b>47</b>	<b>552</b>	<b>45</b>	<b>452</b>	<b>46</b>	<b>454</b>	<b>39</b>	<b>39</b>	<b>39</b>	<b>39</b>	

**Appendix D**  
**Status of Risk Management Program**

Section 2: Status of Risk Management Program	
	Response:
<p><b>1. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li><b>1. Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.</b></li> <li><b>2. Addresses risk from an <i>organizational</i> perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev. 1.</b></li> <li><b>3. Addresses risk from a <i>mission and business process</i> perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.</b></li> <li><b>4. Addresses risk from an <i>information system</i> 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.</b></li> <li><b>5. Categorizes information systems in accordance with government policies.</b></li> <li><b>6. Selects an appropriately tailored set of baseline security controls.</b></li> <li><b>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.</b></li> <li><b>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.</b></li> <li><b>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.</b></li> <li><b>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.</b></li> <li><b>11. Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.</b></li> <li><b>12. Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).</b></li> <li><b>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.</b></li> <li><b>14. Security authorization package contains system security plan, security assessment report, and POA&amp;M in accordance with government policies.</b></li> </ol> <hr/> <p><b>B. The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.</b></p> <hr/> <p><b>C. The Agency has not established a risk management program.</b></p>	

**Appendix D**  
**Status of Risk Management Program**

<p><b>2. If B. is checked above, check areas that need significant improvement:</b></p> <ul style="list-style-type: none"> <li>a. Risk Management policy is not fully developed.</li> <li>b. Risk Management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).</li> <li>c. Risk Management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).</li> <li>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).</li> <li>e. Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53).</li> <li>f. Information systems are not properly categorized (FIPS 199/SP 800-60).</li> <li>g. Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/SP 800-53).</li> <li>h. Risk assessments are not conducted in accordance with government policies (SP 800-30).</li> <li>i. Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).</li> <li>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.</li> <li>k. The process to assess security control effectiveness is not in accordance with government policies (SP800-53A).</li> <li>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).</li> <li>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).</li> <li>n. Security plan is not in accordance with government policies (SP 800-18, SP 800-37).</li> <li>o. Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).</li> <li>p. Accreditation boundaries for agency information systems are not defined in accordance with government policies.</li> <li>q. Other</li> <li>r. Explanation for Other</li> </ul>	
<p><b>3. Comments:</b></p>	<ul style="list-style-type: none"> <li>• DHS bases its risk management program on NIST SP 800-37, Revision 1, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i> and incorporated the security authorization process into the <i>DHS Sensitive Systems Policy Directive 4300A</i> 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.</li> <li>• Based on our review of 28 operational systems, we determined that the artifacts required to authorize a system were either missing, incomplete, or outdated.</li> </ul>

**Appendix E**  
**Status of Configuration Management Program**

Section 3: Status of Configuration Management Program	
	Response:
<p><b>4. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li>1. Documented policies and procedures for configuration management.</li> <li>2. Standard baseline configurations defined.</li> <li>3. Assessing for compliance with baseline configurations.</li> <li>4. Process for timely, as specified in agency policy or standards, remediation of scan result deviations.</li> <li>5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.</li> <li>6. Documented proposed or actual changes to hardware and software configurations.</li> <li>7. Process for timely and secure installation of software patches.</li> </ol> <hr/> <p><b>B. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.</b></p> <hr/> <p><b>C. The Agency has not established a security configuration management program.</b></p>	<p>✓</p>
<p><b>5. If B. is checked above, check areas that need significant improvement:</b></p> <ol style="list-style-type: none"> <li>a. Configuration management policy is not fully developed (NIST 800-53: CM-1).</li> <li>b. Configuration management procedures are not fully developed (NIST 800-53: CM-1).</li> <li>c. Configuration management procedures are not consistently implemented (NIST 800-53: CM-1).</li> <li>d. Standard baseline configurations are not identified for software components (NIST 800-53: CM-2).</li> <li>e. Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).</li> <li>f. Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).</li> <li>g. FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6).</li> <li>h. Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).</li> <li>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).</li> <li>j. Patch management process is not fully developed, as specified in agency policy or standards. (NIST 800-53: CM-3, SI-2).</li> <li>k. Other</li> <li>l. Explanation for Other</li> </ol>	<p>f, g</p>

**Appendix E**  
**Status of Configuration Management Program**

---

<p><b>6. Identify baselines reviewed:</b></p> <ul style="list-style-type: none"> <li>a. Software Name</li> <li>b. Software Version</li> </ul>	<ul style="list-style-type: none"> <li>- Oracle</li> <li>- Security Enhanced Linux/Linux</li> <li>-Solaris</li> <li>- Windows Server 2003</li> <li>- Window Server 2008</li> <li>- Cisco</li> <li>- Windows XP</li> </ul>
<p><b>7. Comments:</b></p>	<ul style="list-style-type: none"> <li>• Based on our review of 41 systems, we determined that DHS components had not fully configured their systems based on DHS' secure baseline configuration guidelines.</li> <li>• We determined that no component has fully implemented FDCC settings across its enterprise.</li> <li>• Although components are developing and implementing USGCB compliant Windows 7 images, no component is using Windows 7 as the primary operating system for its workstations.</li> <li>• OneNet gateway routers were not configured according to all DHS policies.</li> </ul>

**Appendix F**  
**Status of Incident Response and Reporting Program**

Section 4: Status of Incident Response & Reporting Program	
	Response:
<p><b>8. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li><b>1. Documented policies and procedures for detecting, responding to and reporting incidents.</b></li> <li><b>2. Comprehensive analysis, validation and documentation of incidents.</b></li> <li><b>3. When applicable, reports to US-CERT within established timeframes.</b></li> <li><b>4. When applicable, reports to law enforcement within established timeframes.</b></li> <li><b>5. Responds to and resolves incidents in a timely manner, as specified in agency policy or standards, to minimize further damage.</b></li> <li><b>6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.</b></li> <li><b>7. Is capable of correlating incidents.</b></li> </ol> <hr/> <p><b>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.</b></p> <hr/> <p><b>C. The Agency has not established an incident response and reporting program.</b></p>	
<p><b>9. If B. is checked above, check areas that need significant improvement:</b></p> <ol style="list-style-type: none"> <li><b>a. Incident response and reporting policy is not fully developed (NIST 800-53: IR-1).</b></li> <li><b>b. Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1).</b></li> <li><b>c. Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev1).</b></li> <li><b>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).</b></li> <li><b>e. Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).</b></li> <li><b>f. Incidents were not reported to law enforcement as required (SP 800-86).</b></li> <li><b>g. Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).</b></li> <li><b>h. Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).</b></li> <li><b>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).</b></li> <li><b>j. The agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment.</b></li> <li><b>k. The agency does not have the technical capability to correlate incident events.</b></li> <li><b>l. Other</b></li> <li><b>m. Explanation for Other</b></li> </ol>	



**Appendix F**  
**Status of Incident Response and Reporting Program**

---

<b>10. Comments:</b>	
----------------------	--

**Appendix G**  
**Status of Security Training Program**

Section 5: Status of Security Training Program	
	Response:
<p><b>11. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li><b>1. Documented policies and procedures for security awareness training.</b></li> <li><b>2. Documented policies and procedures for specialized training for users with significant information security responsibilities.</b></li> <li><b>3. Security training content based on the organization and roles, as specified in agency policy or standards.</b></li> <li><b>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.</b></li> <li><b>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.</b></li> </ol> <hr/> <p><b>B. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.</b></p> <hr/> <p><b>C. The Agency has not established a security training program.</b></p>	<p>✓</p>

**Appendix G**  
**Status of Security Training Program**

<p><b>12. If B. is checked above, check areas that need significant improvement:</b></p> <ul style="list-style-type: none"> <li>a. Security awareness training policy is not fully developed (NIST 800-53: AT-1).</li> <li>b. Security awareness training procedures are not fully developed and sufficiently detailed (NIST 800-53: AT-1).</li> <li>c. Security awareness training procedures are not consistently implemented in accordance with government policies (NIST 800-53: AT-2).</li> <li>d. Specialized security training policy is not fully developed (NIST 800-53: AT-3).</li> <li>e. Specialized security training procedures are not fully developed or sufficiently detailed in accordance with government policies (SP 800-50, SP 800-53).</li> <li>f. Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).</li> <li>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).</li> <li>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).</li> <li>i. Training content for individuals with significant information security responsibilities is not adequate in accordance with government policies (SP 800-53, SP 800-16).</li> <li>j. Less than 90% of personnel (including employees, contractors, and other agency users) with access privileges completed security awareness training in the past year.</li> <li>k. Less than 90% of employees, contractors, and other users with significant security responsibilities completed specialized security awareness training in the past year.</li> <li>l. Other</li> <li>m. Explanation for Other</li> </ul>	
<p><b>13. Comments:</b></p>	<ul style="list-style-type: none"> <li>• DHS has documented policies and procedures for maintaining a security training program.</li> <li>• DHS has established a process to validate components' security training and has an active role in developing the content for DHS training requirements.</li> <li>• DHS has developed and implemented specialized training courses for those with significant IT security responsibilities, including information system security officers and system administrators.</li> <li>• Specific training content for system owners and authorizing officials has yet to be finalized.</li> <li>• DHS utilizes an enterprise management tool to identify and track the status of specialized training for all personnel with significant information security responsibilities.</li> </ul>

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

---

<b>Section 6: Status of Plans of Actions &amp; Milestones (POA&amp;M) Program</b>	
<b>14. Check one:</b>	<b>Response:</b>
<b>A. The Agency has established and is maintaining a POA&amp;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:</b>	
<b>1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.</b>	
<b>2. Tracks, prioritizes and remediates weaknesses.</b>	
<b>3. Ensures remediation plans are effective for correcting weaknesses.</b>	
<b>4. Establishes and adheres to milestone remediation dates.</b>	
<b>5. Ensures resources are provided for correcting weaknesses.</b>	
<b>6. 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&amp;M activities at least quarterly.</b>	
<hr/>	
<b>B. The Agency has established and is maintaining a POA&amp;M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.</b>	
<hr/>	
<b>C. The Agency has not established a POA&amp;M program.</b>	

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

<p><b>15. If B. is checked above, check areas that need significant improvement:</b></p> <ul style="list-style-type: none"> <li>a. POA&amp;M policy is not fully developed.</li> <li>b. POA&amp;M procedures are not fully developed and sufficiently detailed.</li> <li>c. POA&amp;M procedures are not consistently implemented in accordance with government policies.</li> <li>d. POA&amp;Ms do not include security weaknesses requiring remediation, discovered during assessments of security controls. (OMB M-04-25).</li> <li>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).</li> <li>f. Source of security weaknesses are not tracked (OMB M-04-25).</li> <li>g. Security weaknesses are not appropriately prioritized (OMB M-04-25).</li> <li>h. Milestone dates are not adhered to. (OMB M-04-25).</li> <li>i. Initial target remediation dates are frequently missed (OMB M-04-25).</li> <li>j. POA&amp;Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).</li> <li>k. Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).</li> <li>l. Agency CIO does not track and review POA&amp;Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).</li> <li>m. Other</li> <li>n. Explanation for Other</li> </ul>	
<p><b>16. Comments:</b></p>	<ul style="list-style-type: none"> <li>• DHS requires components to create and manage POA&amp;Ms for all known IT security weaknesses.</li> <li>• DHS has developed policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.</li> <li>• As of June 30, 2011, DHS has 4,559 open POA&amp;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.</li> <li>• DHS creates quarterly POA&amp;M progress reports, tracking weakness remediation and maintenance.</li> </ul>

**Appendix I**  
**Status of Remote Access Program**

Section 7: Status of Remote Access Program	
	Response:
<p><b>17. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li>1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.</li> <li>2. Protects against unauthorized connections or subversion of authorized connections.</li> <li>3. Users are uniquely identified and authenticated for all access.</li> <li>4. If applicable, multi-factor authentication is required for remote access.</li> <li>5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.</li> <li>6. Defines and implements encryption requirements for information transmitted across public networks.</li> <li>7. Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication is required.</li> </ol> <hr/> <p><b>B. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.</b></p> <hr/> <p><b>C. The Agency has not established a program for providing secure remote access.</b></p>	
<p><b>18. If B. is checked above, check areas that need significant improvement:</b></p> <ol style="list-style-type: none"> <li>a. Remote access policy is not fully developed (NIST 800-53: AC-1, AC-17).</li> <li>b. Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1, AC-17).</li> <li>c. Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1, AC-17).</li> <li>d. Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).</li> <li>e. Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4).</li> <li>f. Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).</li> <li>g. Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).</li> <li>h. Agency has not identified all remote devices (NIST 800-46, Section 2.1).</li> <li>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).</li> <li>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).</li> <li>k. Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).</li> <li>l. Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4).</li> <li>m. Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).</li> <li>n. Other</li> <li>o. Explanation for Other</li> </ol>	

**Appendix I**  
**Status of Remote Access Program**

---

<b>19. Comments:</b>	
----------------------	--

**Appendix J**  
**Status of Account and Identity Management Program**

Section 8: Status of Account and Identity Management Program	
	Response:
<p><b>20. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li><b>1. Documented policies and procedures for account and identity management.</b></li> <li><b>2. Identifies all users, including federal employees, contractors, and others who access Agency systems.</b></li> <li><b>3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary.</b></li> <li><b>4. If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.</b></li> <li><b>5. Ensures that the users are granted access based on needs and separation of duties principles.</b></li> <li><b>6. Identifies devices that are attached to the network and distinguishes these devices from users.</b></li> <li><b>7. Ensures that accounts are terminated or deactivated once access is no longer required.</b></li> <li><b>8. Identifies and controls use of shared accounts.</b></li> </ol>	
<p><b>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.</b></p>	
<p><b>C. The Agency has not established an identity and access management program.</b></p>	



**Appendix J**  
**Status of Account and Identity Management Program**

<p><b>21. If B. is checked above, check areas that need significant improvement:</b></p> <ul style="list-style-type: none"> <li>a. Account management policy is not fully developed (NIST 800-53: AC-1).</li> <li>b. Account management procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1).</li> <li>c. Account management procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-2).</li> <li>d. Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).</li> <li>e. Accounts are not properly issued to new users (NIST 800-53, AC-2).</li> <li>f. Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).</li> <li>g. Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).</li> <li>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).</li> <li>i. Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).</li> <li>j. Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).</li> <li>k. Network devices are not properly authenticated (NIST 800-53, IA-3).</li> <li>l. The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies.</li> <li>m. Use of shared privileged accounts is not necessary or justified.</li> <li>n. When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group.</li> <li>o. Other</li> <li>p. Explanation for Other</li> </ul>	
<p><b>22. Comments:</b></p>	<p>DHS does not use multi-factor authentication for access and identity management. However, DHS is in the process of deploying HSPD-12 compliant credentials to the entire department with plans to use the PIV cards for multi-factor authentication in FY 2012.</p>

**Appendix K**  
**Status of Continuous Monitoring Program**

Section 9: Status of Continuous Monitoring Program	
	Response:
<p><b>23. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li>1. Documented policies and procedures for continuous monitoring.</li> <li>2. Documented strategy and plans for continuous monitoring.</li> <li>3. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.</li> <li>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&amp;M additions and updates with the frequency defined in the strategy and/or plans.</li> </ol> <hr/> <p><b>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.</b></p> <hr/> <p><b>C. The Agency has not established a continuous monitoring program.</b></p>	
<p><b>24. If B. is checked above, check areas that need significant improvement:</b></p> <ol style="list-style-type: none"> <li>a. Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).</li> <li>b. Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).</li> <li>c. Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).</li> <li>d. Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).</li> <li>e. Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).</li> <li>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&amp;Ms (NIST 800-53, NIST 800-53A).</li> <li>g. Other</li> <li>h. Explanation for Other</li> </ol>	
<p><b>25. Comments:</b></p>	<p>DHS has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST and OMB FISMA requirements. For example, DHS requires components to complete NIST SP 800-53 assessments and key control reviews. In addition, we determined that:</p> <ul style="list-style-type: none"> <li>• DHS has developed policies and procedures to implement its continuous monitoring functions and requirements. For example, CISO developed the <i>DHS IT Security Continuous Monitoring Strategy: An Enterprise View</i> in January 2011.</li> <li>• DHS' revised continuous monitoring program is now focused at the asset level, which includes the monitoring of system vulnerabilities, configuration settings, malware, patch information, hardware, and software installed on its systems.</li> <li>• Not all components have provided authorizing officials with up-to-date security status reports and documentation for all security authorization packages. For example, during our review of 28 system security plans, we identified three instances where documentation was out of date.</li> </ul>

**Appendix L**  
**Status of Contingency Planning Program**

Section 10: Status of Contingency Planning Program	
	Response:
<p><b>26. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li><b>1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.</b></li> <li><b>2. The agency has performed an overall Business Impact Analysis (BIA).</b></li> <li><b>3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.</b></li> <li><b>4. Testing of system specific contingency plans.</b></li> <li><b>5. The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.</b></li> <li><b>6. Development of test, training, and exercise (TT&amp;E) programs.</b></li> <li><b>7. Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.</b></li> </ol> <hr/> <p><b>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.</b></p> <hr/> <p><b>C. The Agency has not established a business continuity/disaster recovery program.</b></p>	
<p><b>27. If B. is checked above, check areas that need significant improvement:</b></p> <ol style="list-style-type: none"> <li><b>a. Contingency planning policy is not fully developed and contingency planning policy is not consistently implemented (NIST 800-53: CP-1).</b></li> <li><b>b. Contingency planning procedures are not fully developed (NIST 800-53: CP-1).</b></li> <li><b>c. Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34).</b></li> <li><b>d. An overall business impact assessment has not been performed (NIST SP 800-34).</b></li> <li><b>e. Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).</b></li> <li><b>f. A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).</b></li> <li><b>g. A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).</b></li> <li><b>h. System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).</b></li> <li><b>i. Systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).</b></li> <li><b>j. Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-34, NIST 800-53).</b></li> <li><b>k. Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).</b></li> <li><b>l. After-action report did not address issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).</b></li> <li><b>m. Systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).</b></li> <li><b>n. Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).</b></li> <li><b>o. Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).</b></li> <li><b>p. Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).</b></li> </ol>	

**Appendix L**  
**Status of Contingency Planning Program**

---

	<p><b>q. Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).</b></p> <p><b>r. Contingency planning does not consider supply chain threats.</b></p> <p><b>s. Other</b></p> <p><b>t. Explanation for Other</b></p>	
<p><b>28. Comments:</b></p>	<p>DHS has established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. However, based on our review of 28 security authorization packages, we determined that contingency plans and/or testing reports for 6 systems are missing certain elements, including the identification of alternate processing facilities, or restoration procedures, data sensitivity handling procedures at the alternate site or offsite storage. In addition, one contingency plan is out of date.</p>	

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

---

Section 11: Status of Agency Program to Oversee Contractor Systems	
	Response:
<p><b>29. Choose one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li><b>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.</b></li> <li><b>2. The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and agency guidelines.</b></li> <li><b>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.</b></li> <li><b>4. The inventory identifies interfaces between these systems and Agency-operated systems.</b></li> <li><b>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.</b></li> <li><b>6. The inventory of contractor systems is updated at least annually.</b></li> <li><b>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></li> </ol> <hr/> <p><b>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.</b></p> <hr/> <p><b>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.</b></p>	<p>✓</p>

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

---

<p><b>30. If B. is checked above, check areas that need significant improvement:</b></p> <ul style="list-style-type: none"> <li>a. Policies to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</li> <li>b. Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</li> <li>c. Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud are not consistently implemented.</li> <li>d. The inventory of systems owned or operated by contractors or other entities, including Agency systems and services residing in public cloud, is not complete in accordance with government policies (NIST 800-53: PM-5).</li> <li>e. The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.</li> <li>f. The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.</li> <li>g. Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., security requirements).</li> <li>h. Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., security requirements).</li> <li>i. Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.</li> <li>j. Other</li> <li>k. Explanation for Other</li> </ul>	
<p><b>31. Comments:</b></p>	<ul style="list-style-type: none"> <li>• DHS has established and maintains a program to oversee systems operated on its behalf by contractors or other entities.</li> </ul>

**Appendix N**  
**Status of Security Capital Planning Program**

---

<b>Section 12: Status of Security Capital Planning Program</b>	
	<b>Response:</b>
<p><b>32. Check one:</b></p> <p><b>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:</b></p> <ol style="list-style-type: none"> <li><b>1. Documented policies and procedures to address information security in the capital planning and investment control process.</b></li> <li><b>2. Includes information security requirements as part of the capital planning and investment process.</b></li> <li><b>3. Establishes a discrete line item for information security in organizational programming and documentation.</b></li> <li><b>4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.</b></li> <li><b>5. Ensures that information security resources are available for expenditure as planned.</b></li> </ol> <hr/> <p><b>B. The Agency has established and maintains a capital planning and investment program. However, the Agency needs to make significant improvements as noted below.</b></p> <hr/> <p><b>C. The Agency does not have a capital planning and investment program.</b></p>	
<p><b>33. If B. is checked above, check areas that need significant improvement:</b></p> <ol style="list-style-type: none"> <li><b>a. CPIC information security policy is not fully developed.</b></li> <li><b>b. CPIC information security procedures are not fully developed.</b></li> <li><b>c. CPIC information security procedures are not consistently implemented.</b></li> <li><b>d. The Agency does not adequately plan for IT security during the CPIC process (SP 800-65).</b></li> <li><b>e. The Agency does not include a separate line for information security in appropriate documentation (NIST 800-53: SA-2).</b></li> <li><b>f. Exhibits 300/53 or business cases do not adequately address or identify information security costs (NIST 800-53: PM-3).</b></li> <li><b>g. The Agency does not provide IT security funding to maintain the security levels identified.</b></li> <li><b>h. Other</b></li> <li><b>i. Explanation for Other</b></li> </ol>	

## Appendix N

### Status of Security Capital Planning Program

---

<b>34. Comments:</b>	<p>DHS has established and maintains a security capital planning and investment program for information security. For example:</p> <ul style="list-style-type: none"><li>• DHS bases its CPIC process on OMB's Circular A-11, Part 7 - <i>Planning, Budgeting, Acquisition, and Management of Capital Assets</i> which defines the policies for planning, budgeting, acquiring, and managing federal capital assets.<sup>20</sup> In addition, DHS developed the <i>CPIC Guide</i> in August 2010.</li><li>• 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.</li><li>• During FY 2011, DHS has completed 94 Exhibit 300s for its major IT investments.</li></ul>
----------------------	--

---

<sup>20</sup> OMB's Circular A-11, Part 7 – *Planning, Budgeting, Acquisition, and Management of Capital Assets*, June 2008.



## **Appendix O**

### **Major Contributors to this Report**

---

#### **Information Security Audit Division**

Chiu-Tong Tsang, Director  
Aaron Zappone, Team Lead  
Amanda Strickler, IT Specialist  
Michael Kim, IT Auditor  
David Bunning, IT Specialist  
Joseph Landas, Management/Program Assistant  
Angeline De Chiara, Management/Program Assistant  
Hannah Schneider, Management/Program Assistant  
Gregory Wilson, Management/Program Assistant  
Hans Petrich, Management/Program Assistant  
Erin Dunham, Referencer

## **Appendix P**

### **Report Distribution**

---

#### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretary  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
Chief Information Officer  
Deputy Chief Information Officer  
Chief Financial Officer  
Chief Information Security Officer  
Director, GAO/OIG Liaison Office  
Director, Compliance and Oversight Program, Office of CIO  
Deputy Director, Compliance and Oversight Program, Office of CIO  
Chief Information Officer Audit Liaison  
Chief Information Security Officer Audit Liaison  
Component CIOs  
Component CISOs

#### **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 report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at [www.dhs.gov/oig](http://www.dhs.gov/oig).

#### OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov); or
- Write to us at:  
DHS Office of Inspector General/MAIL STOP 2600,  
Attention: Office of Investigations - Hotline,  
245 Murray Drive, SW, Building 410,  
Washington, DC 20528.

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