

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

DHS Can Take Actions To Address
Its Additional Cybersecurity Responsibilities



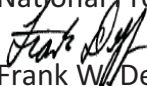


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 5, 2013

MEMORANDUM FOR: Bobbie Stempfley
Acting Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate

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

SUBJECT: *DHS Can Take Actions To Address Its Additional
Cybersecurity Responsibilities*

Attached for your action is our final report, *DHS Can Take Actions To Address Its Additional Cybersecurity Responsibilities*. We incorporated the National Protection and Programs Directorate's formal comments in the final report.

The report contains six recommendations aimed at addressing the National Protection and Programs Directorate's cybersecurity responsibilities to improve the security posture of the Federal Government. The National Protection and Programs Directorate concurred with all recommendations. As prescribed by the Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

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

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

Attachment



Table of Contents

Executive Summary.....	1
Background	2
Results of Audit	5
Actions Taken To Improve Cybersecurity at Federal Agencies.....	5
Strategic Implementation Plan Needed for Effective Cybersecurity Oversight	6
Recommendations	7
Management Comments and OIG Analysis	7
Improved Communication and Collaboration With Federal Agencies Can Help Improve the FISMA Reporting Process	8
Recommendations	10
Management Comments and OIG Analysis	10
CS&C Does Not Maintain an Adequate Security Training Program for Contractors.....	12
Recommendation	13
Management Comments and OIG Analysis	13
Technical Enhancements Can Improve CyberScope Security.....	13
Recommendation	14
Management Comments and OIG Analysis	15

Appendixes

Appendix A: Objectives, Scope, and Methodology.....	16
Appendix B: Management Comments to the Draft Report	17
Appendix C: Major Contributors to This Report	20
Appendix D: Report Distribution	21

Abbreviations

CDM	Continuous Diagnostics Mitigation
CIO	Chief Information Officer
CONOPS	Concept of Operations
CPM	Cybersecurity Performance Management
CS&C	Office of Cybersecurity and Communications



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

DHS	Department of Homeland Security
FISMA	<i>Federal Information Security Management Act</i>
FNR	Federal Network Resilience
FY	fiscal year
ISSO	Information System Security Officer
IT	information technology
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
TIC	Trusted Internet Connection



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

Executive Summary

In 2010, the Office of Management and Budget designated the Department of Homeland Security (DHS) with the primary responsibilities of overseeing the Federal-wide information security program and evaluating its compliance with the *Federal Information Security Management Act of 2002*. The National Protection and Programs Directorate (NPPD), which is primarily responsible for fulfilling DHS security missions, assumed this responsibility for the Department. Subsequent to the President's issuance of Executive Order 13618 in July 2012, NPPD's Office of Cybersecurity and Communications was reorganized in an effort to promote security, resiliency, and reliability of the Nation's cyber and communications infrastructure.

We audited NPPD to determine whether the Office of Cybersecurity and Communications has implemented its additional cybersecurity responsibilities effectively to improve the security posture of the Federal Government.

The Federal Network Resilience division, within the Office of Cybersecurity and Communications, has taken actions to address its assigned responsibilities and to improve the information security posture at Government agencies. For example, the Federal Network Resilience division manages the annual *Federal Information Security Management Act* reporting process and takes an active approach toward evaluating agencies' compliance with the President's cybersecurity initiatives. Further, it conducts information security assessments at selected Federal agencies.

Although actions have been taken, NPPD can make further improvements to address its additional cybersecurity responsibilities. For example, the Federal Network Resilience division must develop a strategic implementation plan to define its long-term goals on improving agencies' information security programs. Further, increased communication and coordination with Government agencies can improve the *Federal Information Security Management Act* reporting process. Finally, NPPD must address deficiencies in maintaining and tracking the training records of CyberScope contractor personnel and implement the required DHS baseline configuration settings.

We are making six recommendations to the Acting Assistant Secretary, Office of Cybersecurity and Communications. NPPD concurred with all recommendations and has begun to take actions to implement them. NPPD's responses are summarized and evaluated in the body of this report and are included, in their entirety, as appendix B.



Background

To help secure agency information systems against cyber threats, the *Federal Information Security Management Act of 2002* (FISMA) was enacted to set forth a comprehensive framework for ensuring effective information security.¹ To ensure the implementation of this framework, FISMA assigned specific responsibilities to the Office of Management and Budget (OMB) to develop and oversee the implementation of policies and standards on information security.

On July 6, 2010, OMB designated DHS with the primary responsibility of overseeing a Federal-wide information security program designed to better protect Federal agencies' information systems and networks.² NPPD, which serves as the lead for protecting and enhancing the resilience of the Nation's physical and cyber infrastructure, assumed this responsibility for the Department.

NPPD's Office of Cybersecurity and Communications (CS&C) is responsible for developing and collecting FISMA metrics, in conjunction with OMB, that are submitted either annually or quarterly by the Office of Chief Information Officer (OCIO) and Office of Inspector General (OIG) at each agency. In addition, Federal agencies are required to provide monthly information security and vulnerability data feeds through a web-based application, CyberScope, allowing for improved risk-management decisions and increased situational awareness.³

To gain access to CyberScope, users must authenticate with their Homeland Security Presidential Directive 12 compliant credential that contains a digital certificate and personal identification number through OMB's Max Portal.⁴ Authenticated users are then directed to CyberScope to input or review FISMA-related data. Figure 1 shows a high-level view of CyberScope's system and encryption architecture.

¹ *Federal Information Security Management Act of 2002* (Public Law 107-347, Section 301-305).

² OMB M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010, assigned DHS with the primary responsibility within the Executive Branch for the operational aspects of Federal agency cybersecurity regarding Federal information systems that fall within FISMA.

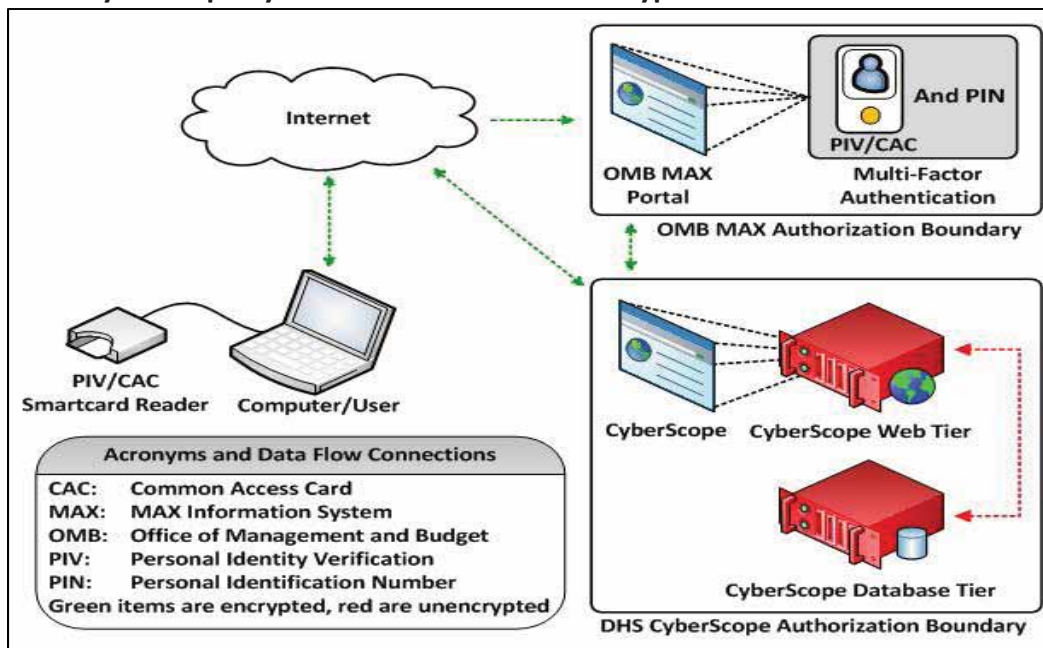
³ Agencies must load data from their security management tools into CyberScope on a monthly basis. Small and micro agencies are not required to submit monthly data feeds.

⁴ An OMB waiver is required for agencies to use single-factor authentication (username and password) to access CyberScope.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 1. CyberScope System Architecture and Encryption Elements



Further, DHS has been tasked with developing, managing, and overseeing OMB’s Trusted Internet Connection (TIC) initiative for the Federal Government.⁵ Identified as one of the Administration’s three priorities to improve cybersecurity and the security of Federal information systems, the TIC initiative aims to further improve agencies’ security posture and incident response capabilities through enhanced monitoring and situational awareness of all external network connections.⁶

Additionally, the President issued Executive Order 13618 to improve emergency communication throughout the Federal Government.⁷ Under the Executive Order, DHS was required to provide the President with a detailed plan within 60 days of issuance, describing the organization and management structure for its national security/emergency preparedness communications functions. Subsequently, CS&C was reorganized in October 2012 to support these requirements better and improve the security and dependability of the Nation’s cyber and communications infrastructure. Specifically, CS&C is now composed of five divisions: Federal Network Resilience (FNR),

⁵ OMB M-08-05, *Implementation of Trusted Internet Connections (TIC)*, November 20, 2007, established the TIC initiative, which requires departments and agencies to secure Federal external network connections, including Internet connections, and improve the government's incident response capability by reducing the number of agencies' external network connections and implementing security controls over the connections that remain.

⁶ The three Administrative Cybersecurity Priorities are continuous monitoring of Federal information systems, TIC capabilities and traffic consolidation, and strong authentication with Homeland Security Presidential Directive 12 compliant credentials for logical access control.

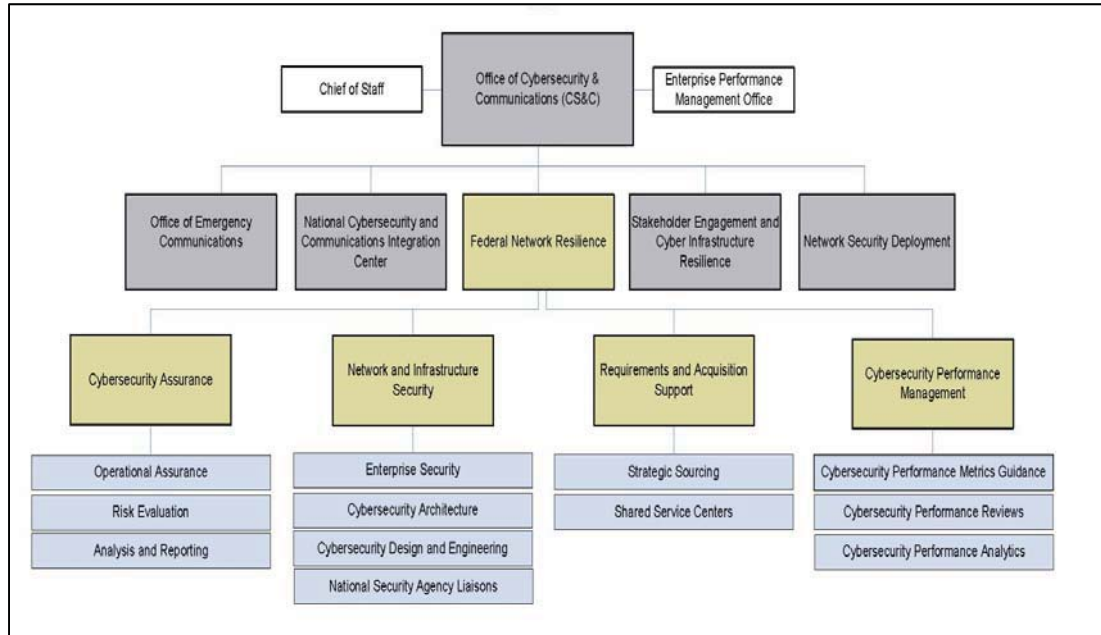
⁷ Executive Order 13618, *Assignment of National Security and Emergency Preparedness (NS/EP) Communications Functions*, was issued on July 6, 2012.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

Network Security Deployment, National Cybersecurity and Communications Integration Center, Office of Emergency Communications, and the Stakeholder Engagement and Cyber Infrastructure Resilience divisions. Figure 2 illustrates the realignment of CS&C.

Figure 2. Realigned CS&C Organizational Chart as of October 2012



Within the FNR division, the Cybersecurity Performance Management (CPM) Branch is responsible for (1) developing and disseminating FISMA reporting metrics, (2) managing the CyberScope web-based application, and (3) collecting and reviewing Federal agencies' cybersecurity data submissions and monthly data feeds. In addition, FNR's Cybersecurity Assurance Program Branch is responsible for conducting cybersecurity reviews and assessments at Federal agencies to evaluate the effectiveness of agencies' information security programs and compliance with OMB initiatives.



Results of Audit

Actions Taken To Improve Cybersecurity at Federal Agencies

CS&C has taken actions to implement its additional FISMA responsibilities and improve the cybersecurity programs at Federal agencies. For example, CS&C has assumed the responsibility to manage the annual FISMA reporting process on behalf of OMB and conducted reviews and technical assessments to assess and improve cybersecurity capabilities at Federal agencies. Specifically, CS&C has—

- Developed and refined the annual FISMA reporting metrics in conjunction with OMB, which are used to assess agency information security programs and cybersecurity risks across the Federal Government. Some Federal agencies we interviewed indicated that CS&C has taken positive steps to refine the annual reporting metrics by including agencies' input and feedback into the process.
- Conducted seven CyberStat reviews, as of October 2012, to assist Federal agencies in identifying capability limitations and developing action plans to improve information security operations.⁸
- Developed the *Department of Homeland Security Plan for Organization and Management of National Security and Emergency Preparedness (NS/EP) Communications Functions* in September 2012, as required by Executive Order 13618. The plan presents a unified strategy that identifies clear cybersecurity and communications roles and responsibilities and sets the conditions for more effective management.
- Implemented effective security controls to protect the information stored and processed by CyberScope. Our vulnerability and configuration reviews only identified a few weaknesses.
- Authorized CyberScope to operate in accordance with applicable DHS, National Institute of Standards and Technology (NIST), and OMB guidance. Our review of the CyberScope security authorization package did not reveal any significant deficiencies.

⁸ CyberStat sessions include DHS, OMB, and agency team representatives working together to examine program data.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

- Performed 18 network and TIC assessments in fiscal year (FY) 2012 to evaluate the security posture, compliance with OMB cybersecurity initiatives, and identify areas of improvement at selected agencies.

Despite these efforts, CS&C can take further actions to implement its additional cybersecurity responsibilities. For example, developing a strategic implementation plan and improving the communication and coordination with Federal agencies will help CS&C refine the FISMA reporting metrics and better evaluate agency information security programs. In addition, CS&C must establish a process to ensure that CyberScope contractor personnel receive adequate security training to perform their job functions. Finally, CS&C must configure CyberScope in accordance with DHS guidance.

Strategic Implementation Plan Needed for Effective Cybersecurity Oversight

FNR has not developed a strategic implementation plan that describes its cybersecurity responsibilities or establishes specific timeframes and milestones to provide a clear plan of action for fulfilling its cybersecurity responsibilities. In addition, FNR has not established performance metrics to measure and monitor its progress in accomplishing its mission and goals. As a result, FNR cannot ensure that it is effectively overseeing Federal agencies' information security programs.

Further, although FNR has developed policies and standard operating procedures that specify its responsibilities and key cybersecurity activities, many of these documents are in draft. In addition, FNR has not developed long-term cybersecurity goals and identified medium-term steps or milestones for Federal agencies to accomplish the long-term goals. Without the long-term goals, CS&C will have difficulty determining whether the CPM program is effective in achieving the desired results to strengthen the security posture of the Federal Government.

Management turnover has hindered CS&C's ability to develop a strategic implementation plan. Specifically, key leadership personnel have departed CS&C within the past year, including the Assistant Secretary of CS&C in January 2013, Director of FNR (previously known as Federal Network Security) in July 2012, and the CPM Branch Chief in March 2013. In addition, the issuance of Executive Order 13618 triggered a comprehensive review of DHS' cybersecurity roles and responsibilities, which resulted in CS&C's reorganization into five new divisions in October 2012. As a result, CS&C has to change its draft strategic implementation plan to reflect the revised organizational structure and incorporate new management priorities.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

The *GPR Modernization Act of 2010* requires the development of a strategic implementation plan that identifies the major functions and operations of an agency.⁹ The plan should include general goals and objectives and a description of how those goals and objectives can be achieved. It should cover at least four years following the fiscal year in which the plan is developed. According to OMB guidance, performance measures are developed to monitor a program's accomplishments and determine whether results are being achieved. In addition, performance measures must be based on a program's mission and priorities. In some instances where the outcome of a program may not be realized for many years, a program should identify specific short- and medium-term milestones to accomplish long-term performance goals. Appropriate performance goals should include performance measures and targets, outcomes, and annual and long-term measures and targets.

Without a strategic implementation plan that specifies long-term goals and performance metrics, it may be difficult for CS&C FNR to manage and evaluate Federal agencies' information security programs effectively. In addition, given the complexity of managing a Federal-wide program and frequent organizational changes, a comprehensive strategic implementation plan will help CS&C FNR achieve its key objectives and milestones.

Recommendations

We recommend that the Acting Assistant Secretary, CS&C:

Recommendation #1: Coordinate with OMB to develop a strategic implementation plan, which identifies long-term goals and milestones, for Federal agency FISMA compliance.

Recommendation #2: Update and finalize internal operating procedures and guidance documents to ensure that cyber responsibilities and procedures are clearly defined.

Management Comments and OIG Analysis

NPPD concurred with recommendation 1. FNR is currently engaged with OMB, NIST, and the Chief Information Officer (CIO) community in a sustained effort to strategically align Continuous Diagnostics and Mitigation (CDM) capabilities, direction, and governance with the requirements and imperatives of the FISMA compliance regime. The overarching aim of the strategic alliance will further

⁹ *GPR Modernization Act of 2010* (Public Law 111-352).



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

advance performance and produce measurable results. OMB is being provided with short-, mid-, and long-term concept of operations (CONOPs) roadmaps for CDM via the Joint Continuous Monitoring Working Group. FNR is also working directly with NIST to map measurements to controls. These collaborations are directly influencing OMB guidance to departments and agencies, including the revision of OMB Circular A-130. Suggested exit criteria are the Joint Continuous Monitoring Working Group CONOPs containing short-, mid-, and long-range CDM roadmaps; deliverables related to the CDM capability model; and CDM control mappings.

We agree that the steps that NPPD plans to take begin to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that planned corrective actions are completed.

NPPD concurred with recommendation 2. FNR has finalized all of its internal standard operating procedures for FISMA reporting and metric guidance, cybersecurity performance reviews, and performance analysis. Operational process and procedure documents for the CPM branch are consolidated in the single document; '*Cybersecurity Performance Management Operations Guide v1.0*'. In addition, FNR has updated their CONOPs in *Performance Management Concept of Operations (CONOPs), v2.0*. The *Operations Guide v1.0* and *CONOPs v2.0* are currently under final review and will be shared as soon as they are signed.

We agree that the steps that NPPD plans to take begin to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that planned corrective actions are completed.

Improved Communication and Collaboration With Federal Agencies Can Help Improve the FISMA Reporting Process

CS&C FNR can improve communication and collaboration with Federal agencies to enhance the annual FISMA reporting process. Although agency representatives said that CS&C has taken actions, some agencies indicated that CS&C FNR can make further improvements to the clarity and quality of the FISMA reporting metrics and enhance the levels of communication regarding agencies' vulnerability submissions.

We collected comments from 10 Federal agencies and representatives from the Chief Information Security Officer Council and Federal Audit Executive Council to obtain their perspective on the FISMA reporting metrics and monthly



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

CyberScope vulnerability data submissions.¹⁰ We also gathered comments regarding the cybersecurity assessments conducted by CS&C FNR at selected Federal agencies.

Five agencies indicated that some of the FY 2012 and FY 2013 FISMA reporting metrics were unclear and should be revised to reduce ambiguity. For example, one agency stressed the need for additional descriptions and details in the reporting metrics and would like for CyberScope to include dialog or pop-up boxes within the application. Its representatives stated that this enhancement would ensure that agencies are providing DHS and OMB with the information to assess properly Federal agencies' information security programs. In addition, two agencies stated that the annual FISMA reporting process is a strain on available personnel resources as DHS and OMB are developing too many metrics.

Further, one agency stated that, instead of spending resources to implement technical controls and automated capabilities to monitor and protect its networks, it had to divert available funding to ensure FISMA compliance and address the annual reporting metrics. In addition, two agencies indicated that the recent reporting metrics are paperwork driven and do not reflect the current effort for a Federal-wide continuous monitoring programs.¹¹ As a result, these agencies expressed concerns on the inefficient use of resources. For example, they must divide available resources between continuous monitoring efforts and those associated with outdated criteria, such as FISMA legislation, OMB Circular A-130, and some NIST publications.

Federal agencies are required to submit various data elements monthly, such as configuration management, vulnerability data, and audit trails.¹² DHS has been collecting these data since 2011. Three agencies indicated that they have received little or no reaction from DHS regarding their monthly vulnerability submissions. For example, agencies stated that DHS has not provided any detailed information, such as trending analysis, regarding their monthly vulnerability data submissions. In addition, one agency stated that it did not know how or whether DHS used or evaluated its submitted data.

¹⁰ The 10 Federal agencies are the Board of Governors of the Federal Reserve System; the Departments of Energy, Health and Human Services, Homeland Security, Interior, Justice, State, and Treasury; the Securities and Exchange Commission; and the Office of Personnel Management.

¹¹ NIST defines continuous monitoring as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Continuous monitoring, a critical aspect of the organization-wide risk management process, is most effective when automated mechanisms are employed where possible.

¹² OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 14, 2011, requires agencies to establish monthly data feeds to CyberScope.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

According to the former CPM Branch Chief and internal procedures, CPM is not performing detailed analysis of monthly vulnerability submissions provided through CyberScope.¹³ Because of insufficient staff resources, CPM acknowledged that it may not be able to satisfy all of its requirements and responsibilities, including project management, communications, and outreach efforts.¹⁴

Improved communication and collaboration with Federal agencies would allow DHS to improve the quality and clarity of the annual FISMA reporting metrics. Without clear and concise reporting metrics, it may be difficult for Federal agencies to provide accurate information regarding the status of their information security programs. As a result, DHS' and OMB's ability to properly assess FISMA compliance across the enterprise may be hindered. Finally, if the Department does not provide detailed analyses regarding agency data, it may be difficult for Federal agencies to identify potential vulnerability trends or properly secure their information systems and networks.

Recommendations

We recommend that the Acting Assistant Secretary, CS&C:

Recommendation #3: Improve communication and coordination with Federal agencies by providing additional clarity regarding the FISMA reporting metrics.

Recommendation #4: Implement a process to analyze and provide detailed feedback to Federal agencies concerning monthly vulnerability data feeds.

Management Comments and OIG Analysis

NPPD concurred with recommendation 3. FNR's CPM branch is committed to continuous improvement. CPM has dedicated mechanisms in place for developing and vetting metrics and guidance using subject matter experts in full collaboration with OIG and CIO communities. Working groups are currently being held with representatives of the OIG community and subgroups of the Information Security and Identity Management Committee in order to incorporate feedback in the development of the FY 2014 metrics. As the OIG report notes, the Federal community has experienced improvements in the FISMA reporting process. Those improvements are due in large part to FNR's commitment to continuous improvement, and FNR fully expects each successive round of metrics to be an improvement over the previous round. In addition,

¹³ *Cybersecurity Performance Analytics Standard Operating Procedures*, April 26, 2012.

¹⁴ *Cybersecurity Performance Management Mission Needs Statement*, April 23, 2012.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

the CPM branch will produce the following additions to the *Cybersecurity Performance Management Operations Guide v1.0*: (a) stakeholder awareness matrix that outlines communication activities; (b) service descriptions that include procedures, practices, and expectations for collaboration with and support of Federal agencies; and (c) an impact matrix that identifies specific criteria for assessing the quality of a question.

We agree that the steps that NPPD plans to take begin to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that planned corrective actions are completed.

NPPD concurred with recommendation 4. NPPD stated that the current data feeds do not provide the fidelity or reliability required to provide a detailed vulnerability picture. The current data feeds are useful for informing decision makers of large-scale trends and possible threats concerning the existence of unsupported (end-of-life) operating system and software. The feeds also provide useful (though rough) situational awareness data regarding the types of monitoring tools being used and the fullness of current implementations.

Resources are assigned and analysis is under way to glean additional useful vulnerability data from the feeds. However, the CyberScope data feeds must be seen as a transitional activity in the bigger picture of CDM. The feeds constitute an important first step in achieving the *enterprise view* essential to a successful continuous monitoring program. The alignment of tools, standards, resources, governance, and operations needed to bring about the feeds constitute a significant early success and critical baseline in the evolution of CDM.

Additionally, the CPM branch in coordination with CDM program resources will produce a transition plan. The transition plan will identify the tasks and activities involved in moving from the Cyberscope data feeds to the CDM dashboard. It will include the following elements: a scope statement addressing background information on the project; a description of the relationship of the project to other projects and/or organizations; maintenance resources; and identification of the transition team's responsibilities. It also includes the deployment schedule, resource estimates, management controls, reporting procedures, and risks and contingencies.

We agree that the steps that NPPD plans to take begin to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

CS&C Does Not Maintain an Adequate Security Training Program for Contractors

CS&C has not established an effective process to ensure that its CyberScope contractors (i.e., system administrators) have received the required security awareness or adequate specialized role-based training, commensurate with assigned responsibilities. Specifically, CS&C does not maintain records or provide documentation to support that these contractors have received DHS' security awareness or specialized information technology (IT) training. We identified a similar finding in our 2011 report.¹⁵

According to the CyberScope Information System Security Officer (ISSO), FNR does not have a process to maintain training records for CyberScope contractors or ensure that all training requirements have been completed. Additionally, CS&C does not require contractors to receive any specialized IT training in addition to what is mandated by the hosting facility.

FISMA requires agencies to provide employees, contractors, and other users of information systems with security awareness and specialized IT training annually. The training is designed to inform personnel about the risks associated with their activities when accessing government information systems and their responsibilities in complying with agency policies and procedures designed to reduce these risks. DHS also requires components to establish an information security training program for its users, which includes security awareness and specialized IT training for those with significant security responsibilities. ISSOs are also required to maintain training records for users and system personnel.

Without an effective process to track training completion, CyberScope contractors may not have received the appropriate skills or knowledge to properly administer and secure the systems against potential cyber threats. In addition, the skills and knowledge required to maintain and improve system operations may not be developed. Training helps personnel obtain knowledge about current security threats, risks, trends, and mitigation techniques. CS&C cannot guarantee the security of the data collected through CyberScope without ensuring that all people involved understand their roles and responsibilities and are adequately trained to perform them.

¹⁵ *Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure* (OIG-11-89, June 2011).



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

Recommendation

We recommend that the Acting Assistant Secretary, CS&C:

Recommendation #5: Establish a process to ensure that all CyberScope contractor system administrators have received adequate security training in compliance with applicable DHS, OMB, and NIST guidance.

Management Comments and OIG Analysis

NPPD concurred with recommendation 5. FNR is developing a standard operating procedure that defines the procedural controls for tracking CyberScope administrators to ensure that training meets or exceeds applicable DHS, OMB, and NIST guidance.

We agree that the steps that NPPD plans to take begin to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that planned corrective actions are completed.

Technical Enhancements Can Improve CyberScope Security

CS&C has not implemented all DHS security controls on its CyberScope database, which may allow unauthorized individuals to gain access to sensitive data. To assess the security posture of CyberScope, we interviewed selected IT and program management personnel. In addition, we performed vulnerability assessments on the web and database servers. We also reviewed configuration settings on selected servers for compliance with applicable DHS Sensitive Systems Configuration Guidance.

Implementing the Required Configuration Settings Can Further Secure CyberScope

Although CS&C has implemented effective controls on CyberScope, the database was not configured with all required DHS baseline configuration settings to protect the information it stores. For example, we evaluated whether selected security controls, such as access control, identification and authentication, encryption, and network security settings were implemented on CyberScope. We identified the following three instances of noncompliance:

- A guest account exists on a database that may allow an unauthorized user to gain anonymous access. DHS guidance prohibits the use of guest accounts on databases.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

- A default account has not been disabled or renamed. The use of well-known default accounts increases the risks that individuals may gain unauthorized access to the database. DHS requires all default accounts be renamed or disabled.
- Elevated permissions have been granted to a public group which may allow users to get sensitive system information in the Windows registry.¹⁶ DHS requires that users be granted the most restrictive set of privileges needed to perform their assigned tasks.

Subsequent to the completion of our audit work, CS&C personnel stated that they had taken or planned to take corrective action to address the deficiencies identified during our vulnerability assessment. As fieldwork had already been completed, we did not verify whether the deficiencies had been remedied.

DHS baseline configuration guidance provides the settings and parameters for ensuring a minimum baseline of security when installing or configuring databases, such as access control, identification and authentication, auditing, and encryption requirements. The guidance should be used to help protect databases from potential software flaws and help reduce the likelihood of potential threats, including unauthorized access or hacks. In addition, FISMA requires that all systems meet minimally acceptable system configuration requirements, as determined by the agency.

When databases are not properly configured, unauthorized individuals could gain access to sensitive data. As a result, DHS cannot ensure that effective security controls have been implemented, restricting the ability of management officials to make effective, risk-based decisions.

Recommendation

We recommend that the Acting Assistant Secretary, CS&C:

Recommendation #6: Implement all required DHS baseline configuration settings on the CyberScope database.

¹⁶ A Microsoft Windows registry is a hierarchical database that stores configuration settings, and keeps track of the software installed on the computer and how each program relates to others.



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

Management Comments and OIG Analysis

NPPD concurred with recommendation 6. Cyberscope system operators are expected to adhere to all required DHS baseline configuration settings. CyberScope, like any other hosted application, is subject to configuration management policies and procedures. Furthermore, CyberScope is subject to continuous vulnerability scanning and configuration audits. FNR provided documentation to OIG in early March that addresses the remaining finding. FNR continues to work within DHS to ensure that all DHS baseline configuration settings are set and maintained within CyberScope.

We agree that the steps that NPPD plans to take begin to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that planned corrective actions are completed.



Appendix A

Objectives, Scope, and Methodology

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

The objective of our audit was to determine whether NPPD has effectively implemented its additional cybersecurity responsibilities to improve the security posture of the Federal Government. Specifically, we determined the progress and effectiveness of NPPD's actions in (1) implementing its FISMA cybersecurity responsibilities, (2) overseeing the TIC initiative, and (3) addressing Executive Order 13618 regarding DHS' national security/emergency preparedness communications functions and responsibilities. We also determined whether NPPD has implemented effective system security controls to protect sensitive information stored and processed by the DHS CyberScope system, including a review of its security documentation to assess compliance with applicable DHS, NIST, and OMB policies and guidance.

To determine the effectiveness of NPPD actions in implementing its FISMA cybersecurity responsibilities, we interviewed selected CS&C personnel and management officials. We also collected comments from OIG and OCIO personnel from 10 Federal agencies and representatives from the Chief Information Security Officer Council and Federal Audit Executive Council. In addition, we reviewed and evaluated CS&C security policies, standard operating procedures, training data, and other appropriate documentation. Because of the recent issuance of Executive Order 13618 and its early stage of implementation, we did not perform a compressive evaluation on NPPD's actions and requirements. We also conducted automated security assessments using Tenable Nessus and Application Security, Inc. AppDetective Pro on databases and operating systems. Finally, we reviewed CyberScope configuration settings, cryptography implementation, vulnerability assessment processes, and patch management.

Fieldwork was performed in the Washington, DC, area. We conducted this performance audit between October 2012 and March 2013 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B Management Comments to the Draft Report

National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528



Homeland
Security

MAY 22 2013

Mr. Charles K. Edwards
Deputy Inspector General
Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Edwards:

Re: Office of Inspector General Report, DHS Can Take Actions to Address Its Additional Cybersecurity Responsibilities (OIG Project No. 12-171-ITA-NPPD)

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

The National Protection and Programs Directorate (NPPD) is pleased that the OIG highlighted accomplishments regarding actions taken by the Office of Cybersecurity and Communications' (CS&C) Federal Network Resilience (FNR) division to implement its additional cybersecurity responsibilities effectively. Specifically, the report recognizes improvements made to the Federal Information Security Management Act (FISMA) reporting process and progress made in assisting with the improvement of cybersecurity programs at Federal agencies.

The FNR has developed and refined the annual FISMA reporting metrics, in coordination with the Office of Management and Budget (OMB), and has conducted seven CyberStat reviews since October 2012. As a result, FNR was able to support Federal agency efforts to identify capability limitations and to develop action plans that work to improve information security operations. In addition, 18 network and Trusted Internet Connection assessments were performed in FY 2012, which evaluated security posture and compliance with OMB cybersecurity initiatives. It's important to note that FNR is currently deploying a proven diagnostic technology across the .gov realm that automatically scans government networks every three days, thus enabling agencies to identify and repair the worst network problems first. This automated Continuous Diagnostics and Mitigation (CDM) program will replace costly and infrequent manual inspections of systems.

Six recommendations were made to the CS&C Acting Assistant Secretary:

Recommendation 1: Coordinate with OMB to develop a strategic implementation plan which identifies long-term goals and milestones for Federal agency FISMA compliance.

Response: Concur. FNR is currently engaged with OMB, the National Institute of Standards and Technology (NIST), and the Chief Information Officer (CIO) community in a sustained



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

effort to strategically align CDM capabilities, direction, and governance with the requirements and imperatives of the FISMA compliance regime. The overarching aim of the strategic alliance will further advance performance and produce measurable results. OMB is being provided short-, mid-, and long-term concept of operations (CONOPS) roadmaps for CDM via the Joint Continuous Monitoring Working Group (JCMWG). FNR is also working directly with NIST to map measurements to controls. These collaborations are directly influencing OMB guidance to departments and agencies, including the revision of OMB Circular A-130. Suggested exit criteria are the JCMWG CONOPs containing short-, mid-, and long-range CDM roadmaps; deliverables related to the CDM capability model; and CDM control mappings.

Recommendation 2: Update and finalize internal operating procedures and guidance documents to ensure that cyber responsibilities and procedures are clearly defined.

Response: Concur. FNR has finalized all of its internal Standard Operating Procedures (SOPs) for FISMA reporting and metric guidance, cybersecurity performance reviews, and performance analysis. Operational process and procedure documents for the Cybersecurity Performance Management (CPM) branch are consolidated in the single document; *Cybersecurity Performance Management Operations Guide v1.0*. In addition, FNR has updated their CONOPs in *Performance Management Concept of Operations (CONOPS), v.2.0*. The *Operations Guide v1.0* and *CONOPS v2.0* are currently under final review and will be shared as soon as they are signed.

Recommendation 3: Improve communication and coordination with Federal agencies by providing additional clarity regarding the FISMA reporting metrics.

Response: Concur. FNR's CPM branch is committed to continuous improvement. CPM has dedicated mechanisms in place for developing and vetting metrics and guidance using subject matter experts in full collaboration with IG and CIO communities. Working groups are currently being held with representatives of the IG community and subgroups of the Information Security and Identity Management Committee in order to incorporate feedback in the development of the FY14 metrics. As the OIG report notes, the Federal community has experienced improvements in the FISMA reporting process. Those improvements are due in large part to FNR's commitment to continuous improvement, and FNR fully expects each successive round of metrics to be an improvement over the previous round. In addition, the CPM Branch will produce the following additions to the *Cybersecurity Performance Management Operations Guide v1.0* (a) stakeholder awareness matrix that outlines communication activities; (b) service descriptions that include procedures, practices, and expectations for collaboration with and support of Federal agencies; and (c) an impact matrix that identifies specific criteria for assessing the quality of a question.

Recommendation 4: Implement a process to analyze and provide detailed feedback to Federal agencies concerning monthly vulnerability data feeds.

Response: Concur. The data feeds however currently do not provide the fidelity or reliability required to provide a detailed vulnerability picture. The current data feeds are useful for informing decision makers of large-scale trends and possible threats concerning the existence of



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

unsupported (end-of-life) operating system and software. The feeds also provide useful (though rough) situational awareness data regarding the types of monitoring tools being used and the fullness of current implementations.

Resources are assigned and analysis is underway in order to glean additional useful vulnerability data from the feeds. However, the CyberScope data feeds must be seen as a transitional activity in the bigger picture of CDM. The feeds constitute an important first step in achieving the *enterprise view* essential to a successful continuous monitoring program. The alignment of tools, standards, resources, governance, and operations needed to bring about the feeds constitute a significant early success and critical baseline in the evolution of CDM.

Additionally, the CPM branch in coordination with CDM program resources will produce a transition plan. The Transition Plan will identify the tasks and activities involved in moving from the Cyberscope data feeds to the CDM dashboard. The Transition Plan will include the following elements: a scope statement addressing background information on the project, a description of the relationship of the project to other projects and/or organizations, maintenance resources, and identification of the transition team's responsibilities. It also includes the deployment schedule, resource estimates, management controls, reporting procedures, and risks and contingencies.

Recommendation 5: Establish a process to ensure that all CyberScope contractor system administrators have received adequate security training in compliance with applicable DHS, OMB, and NIST guidance.


Response: Concur. FNR is developing a SOP that defines the procedural controls for tracking CyberScope administrators—to ensure training meets or exceeds applicable DHS, OMB, and NIST guidance.

Recommendation 6: Implement all required DHS baseline configuration settings on the CyberScope database.

Response: Concur. The CyberScope system operators are expected to adhere to all required DHS baseline configuration settings. CyberScope, like any other hosted application is subject to configuration management policies and procedures. Furthermore, CyberScope is subject to continuous vulnerability scanning and configuration audits. FNR provided documentation to the OIG in early March that addresses the remaining finding. FNR continues to work within DHS to ensure that all DHS baseline configuration settings are set and maintained within CyberScope.

Again, we thank you for the opportunity to review and provide comment on this draft report, and we look forward to working with you on future homeland security engagements.

Sincerely,


Suzanne E. Spaulding
Acting Under Secretary



Appendix C

Major Contributors to This Report

Chiu-Tong Tsang, Director
Aaron Zappone, Team Lead
Thomas Rohrback, IT Specialist
Michael Kim, IT Auditor
Pachern Thapanawat, IT Auditor
Sheldon Liggins, IT Auditor
Swati Nijhawan, Referencer



Appendix D

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
Under Secretary for Management
Under Secretary, NPPD
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, DHS
Chief Information Security Officer, DHS
Chief Information Officer, NPPD
Chief Information Security Officer, NPPD
Acting Chief Privacy Officer
Director, Compliance and Oversight, DHS OCISO
Director, GAO/OIG Liaison Office
Audit Liaison, CIO, DHS
Audit Liaison, CISO, DHS
Audit Liaison, NPPD

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

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

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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