Department of Homeland Security
Office of Inspector General

Vulnerabilities Highlight the Need for More Effective Web Security Management

(Redacted)

OIG-09-101

September 2009

Office of Inspector General

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

Homeland
Security

September 10, 2009

Preface

The Department of Homeland Security (DHS), Office of Inspector General, 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 DHS' management of its public-facing websites. It is based on interviews with selected officials and contractor personnel, direct observations, technical security vulnerability assessments, and a review of applicable documents.

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 who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CBP	Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
HQ	Headquarters
ICE	Immigration and Customs Enforcement
IT	Information Technology
NPPD	National Protection and Programs Directorate
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service

Executive Summary

The Department of Homeland Security's (DHS) public-facing websites present a highly accessible point of entry and attack to its information resources. These websites are useful in providing DHS and the public with access to information and services, but must be properly configured and maintained in order to protect sensitive data.

We evaluated nine of DHS' most frequently visited public-facing websites to determine whether DHS has implemented effective security controls and practices. We examined the implementation of DHS' required configuration settings and patch management practices. We also performed vulnerability assessments on these websites. In addition, we reviewed documentation regarding electronic authentication for web-based access according to the *Federal Information Security Management Act of 2002* (FISMA).

Overall, DHS components have followed department policy when configuring operating systems supporting their websites. Recommended security settings and controls were implemented consistently on the servers reviewed. In addition, sites using electronic authentication for web-based access were properly documented according to FISMA. However, patch management practices and periodic security assessments were not consistently being performed, resulting in numerous critical system vulnerabilities. These vulnerabilities could put DHS data at risk. In addition, DHS can make improvements in managing its system inventory and providing technical oversight and guidance in order to evaluate the security threats to its public-facing websites.

We are making six recommendations to the Chief Information Officer. DHS management officials concurred with our findings and recommendations, and we consider them resolved. These recommendations will remain open until DHS provides documentation to support that the implementation of all corrective actions is complete.

Background

The World Wide Web is a system for exchanging information over the internet. At the most basic level, a website can be divided into two principal components: web servers, which are computers that make information available over the internet (provide hosting services), and website applications, software used to access and display the information stored on web servers and support systems. Both parts require security measures designed to protect their content.

Websites are often the most targeted and attacked hosts on an organization's network. As a result, it is essential to secure web servers and the network infrastructure that supports them. Effective security management should include the application of effective controls upon configuration and deployment, as well as ongoing maintenance through the performance of regular vulnerability assessments and software updates.

DHS has more than 125 websites accessible by the public which provide component services and communicate emergency data when needed. These systems are provided as a service to the public, and their accessibility is key to DHS' mission, but this accessibility can also make these sites vulnerable to attack.

The department's websites are supported by a variety of server operating systems, application software programs, hardware platforms, and hosting locations, including DHS, other federal agencies, and contractor facilities. The diversity in software, hardware, physical locations, and the constantly changing content of web pages creates a challenging security environment.

Appropriate management practices are essential to operating and maintaining a secure website. Security practices entail the identification of an organization's information technology (IT) assets and the development and implementation of documented policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources.

Results of Audit

Components Adhere to DHS Policy When Configuring Websites

Components consistently applied DHS policy in building and deploying the servers that host their public-facing websites. Components enforce strong password controls for system administrators, limit shared accounts, and ensure that all unnecessary services are disabled. Implementation of these controls is part of a robust information security program.

We reviewed nine of the most frequently visited DHS websites, based on published monthly statistics for December 2008. These sites represent the main public information portals of DHS' components: Customs and Border Protection (CBP), DHS Headquarters (HQ), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration and Customs Enforcement (ICE), National Protection and Programs Directorate (NPPD), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Citizenship and Immigration Services (USCIS). We evaluated the websites to determine whether security controls required by DHS' configuration guides had been implemented. We tested the websites for technical vulnerabilities and reviewed supporting FISMA documentation.

DHS publishes secure baseline configuration guides to assist network security personnel in deploying IT systems throughout the department. These guides outline specific security settings for operating systems and applications. In addition to the application of baseline configuration guide settings, some components regularly test their websites for vulnerabilities.

All web servers tested showed evidence of strong password controls for complexity, reuse, and aging. Web server administrators limited the use of shared accounts, and employed best practices in deactivating services that could allow attackers unauthorized access, such as Telnet and File Transfer Protocol.

Component IT security personnel regularly performed these tests on operating systems, but only a few had the tools or experience testing web applications for security vulnerabilities. As website content is updated or changed, existing vulnerabilities may remain or new vulnerabilities can be introduced, putting the system and data at risk.

Office of Management and Budget Memorandum M-00-13, *Privacy Policies and Data Collection on Federal Web Sites*, limits the use of tracking cookies; small bits of information collected to track website use, on government websites. The results of our vulnerability assessments indicated that all but one of the sites reviewed disabled the use of tracking cookies.

Website Vulnerabilities Could Put DHS Data at Risk

Our review of DHS' most frequently visited websites identified vulnerabilities that could put department information resources at risk. Insufficient security assessments of websites by component security personnel could jeopardize the confidentiality, integrity, and availability of data.

Significant Vulnerabilities Identified

The results of our vulnerability assessments identified [redacted]

Assessment results of web servers showed [redacted] Figure 1 shows the number of critical and high vulnerabilities identified by component.

Figure 1: Website and Server Vulnerabilities by Component

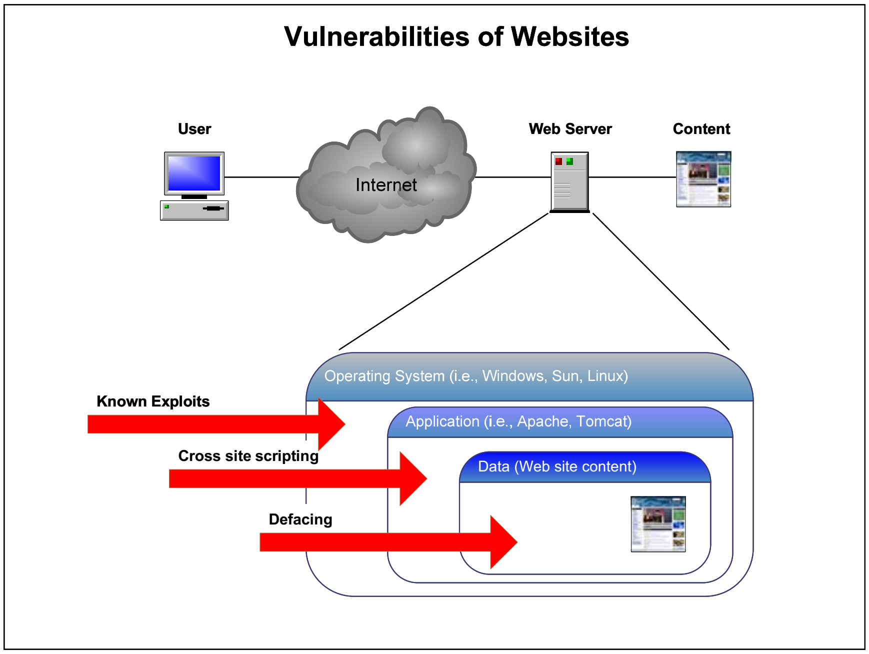
Component	Critical Vulnerabilities Web Application	High Vulnerabilities Server	Total
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Servers hosting websites for [redacted] Our assessments identified [redacted]

Assessment results for servers hosting the [redacted]

DHS has not effectively managed the security programs of these websites by [redacted] While components’ have implemented the initial phases of good security lifecycle practices for their [redacted] Figure 2 shows examples of website vulnerabilities.

Figure 2: Vulnerabilities of Websites


Vulnerabilities of Websites
User
Internet
Web Server
Content
Operating System (i.e., Windows, Sun, Linux)
Application (i.e., Apache, Tomcat)
Data (Web site content)
Known Exploits
Cross site scripting
Defacing

Component Website Vulnerability Testing

TSA and USCG perform regular vulnerability assessments on their websites. This practice protects DHS data and websites by identifying security risks that may be introduced after the initial development and deployment of the website. In addition, the websites for FEMA, NPPD, and USCG contained no vulnerabilities listed as critical or high, and all security patches were applied. These components' security practices, through periodic assessments, patch and update policies, and documented procedures, set the example of an effective defense-in-depth approach to good IT systems security.

[redacted] Components that conduct periodic assessments and perform scans of updates to websites while still in development can identify and mitigate vulnerabilities before DHS data and systems are at risk.

The SysAdmin, Audit, Network, and Security Institute, known as SANS, annually rates cross site scripting as the highest security risk associated with websites. Every week, hundreds of vulnerabilities are reported and actively exploited in commercially available and open source web applications. SANS identified that web application vulnerabilities account for almost half the total number of vulnerabilities being discovered in the past year.

DHS Sensitive Systems Policy Directive 4300A establishes that even public information, such as that contained on a website, requires protection against erroneous manipulation or alteration. Components are required to manage their systems to reduce vulnerabilities through testing and promptly installing patches and critical security updates.

Technical vulnerabilities on department websites expose them to defacing, interruption of services, or loss of resources. Exploits and attacks against websites could compromise the confidentiality, availability, and integrity of department data.

Recommendations

We recommend the Chief Information Officer (CIO):

Recommendation #1: Require components to perform periodic security vulnerability assessments on their public-facing websites.

Recommendation #2: Require components to apply security patches promptly to the servers supporting public-facing websites.

Management Comments and OIG Analysis

DHS concurs with recommendation 1. Management responded that they will have the DHS Security Operations Center (SOC) identify the applications supporting these sites as critical; and track the action for vulnerability scanning each quarter. In addition, the Office of the Chief Information Officer (OCIO) in cooperation with components, will work to develop a plan of action to move these sites to the Enterprise Data Center with the Trusted Internet Connection in order to provide consistent control and security monitoring.

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

DHS concurs with recommendation 2. DHS plans for the SOC to establish tracking of critical security patches specific to these sites by April 2010.

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

Improved Management Controls Could Improve Website Security

DHS management could improve website security through guidance focused on specific threats, and by maintaining an inventory of its public-facing websites. Current DHS guidance does not identify the need for constant security maintenance of websites. As DHS websites are updated with current data, some content may contain security flaws, risking DHS data and services.

Furthermore, DHS management does not have an inventory of its public-facing websites. While most components had knowledge of their own websites, DHS does not track which are inventoried under a general support system or major application. Detailed guidance and improved oversight could protect DHS websites from risk of service interruption and data loss.

DHS policy does not adequately address the risks associated with or the need for specialized security programs for its 125+ public-facing websites. Websites and their support systems face specific threats which need to be addressed beyond the current IT security practices. The current policy, which only mandates security assessments annually, does not clearly describe requirements to assess risks associated with constantly changing web content or the diverse manner in which sites are hosted.

Websites are designed to deliver information to the public as a service and some DHS sites are updated on a weekly basis. We identified sites that were updated as often as three times weekly, with content that had never undergone a security review. These updates constitute new code that could contain vulnerabilities, such as cross site scripting and Structured Query Language injection, and nullify any previous assessment. Any content change to a website could broaden its attack surface, and create a new opportunity for malicious activity.

The availability of a website inventory, or an ability to identify systems' public-facing elements, would assist DHS in managing and securing one of the most targeted and attacked hosts on organizations' networks. An inventory should list those responsible and accountable for website security, as well as assist in identifying accreditation status of legacy systems. CBP's website was not certified or accredited, although it was one of the top five visited sites in DHS. It was not inventoried under a general support system or major application. The main public web site for USSS is still hosted by the Treasury Department. While this site and its security are managed by Treasury, no formal agreement between DHS and Treasury was in place to ensure its protection.

DHS Sensitive Systems Policy Directive 4300A establishes that leadership must assess risk and ensure the security of each system throughout its lifecycle. DHS components must conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment occur. Public-facing websites whose attack surfaces could be broadened by frequent content changes fit this definition.

All web content updates should be scanned by security software for exploitable vulnerabilities; existing websites should be scanned frequently to identify risks. Current DHS policy establishes that systems should be assessed annually for security vulnerabilities, but in the case of constantly changing public-facing websites, this is not enough. Changes to websites are not identified within the policy as being a significant change that would require a new risk or security vulnerability assessment.

The rapid growth of the popularity and number of DHS websites highlights the need to address specific threats with more effective web security management. DHS information security practices should include more stringent controls for websites. DHS' public-facing websites are at risk from attacks that could include defacing, manipulation, or alteration. Sophisticated attacks on federal websites have proven they can disrupt service and risk the confidentiality, integrity, and availability of services and data.

Recommendations

We recommend the CIO:

Recommendation #3: Clarify the department's vulnerability assessment policy and guidelines to address threats specifically associated with its websites.

Recommendation #4: Develop an inventory of the public-facing website elements of major applications and general support systems.

Recommendation #5: Direct CBP's CIO to ensure its public-facing website is certified and accredited.

Recommendation #6: Direct USSS' CIO to develop and implement a plan to move its website under DHS' security program.

Management Comments and OIG Analysis

DHS concurs with recommendation 3. DHS agrees that in order to properly address the threats confronting the public-facing websites, the processes must adhere to those included within the master service agreement. In addition, under the direction of the SOC, all systems will adhere to the guidance as directed through the Information Security Vulnerability Messages.

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

DHS concurs with recommendation 4. The OCIO has agreed to leverage the information in the Department's Enterprise Architecture and the Trusted Agent FISMA (TAF) database to establish an inventory of public- facing major applications and support systems.

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

DHS concurs with recommendation 5. As part of the collaboration between OCIO and CBP, DHS has initiated the certification and accreditation process for the www.cbp.gov website in March 2009.

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

DHS concurs with recommendation 6. USSS has established communications with the OCIO to perform this action.

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

Appendix A
Purpose, Scope, and Methodology

The objective of our review was to determine whether DHS has implemented effective security controls to protect its web servers and website applications, and has documented electronic authorization for web-based access in accordance with FISMA. We interviewed selected personnel at DHS headquarters; component offices, and contractor sites in Pennsylvania, Maryland, and Virginia. In addition, we reviewed and evaluated DHS security policies and procedures, configuration management practices, and other appropriate documentation.

We used [redacted] Upon completion of the assessments, we provided program officials with the technical reports detailing the specific vulnerabilities detected and the actions needed for remediation. The table below shows the websites and components tested.

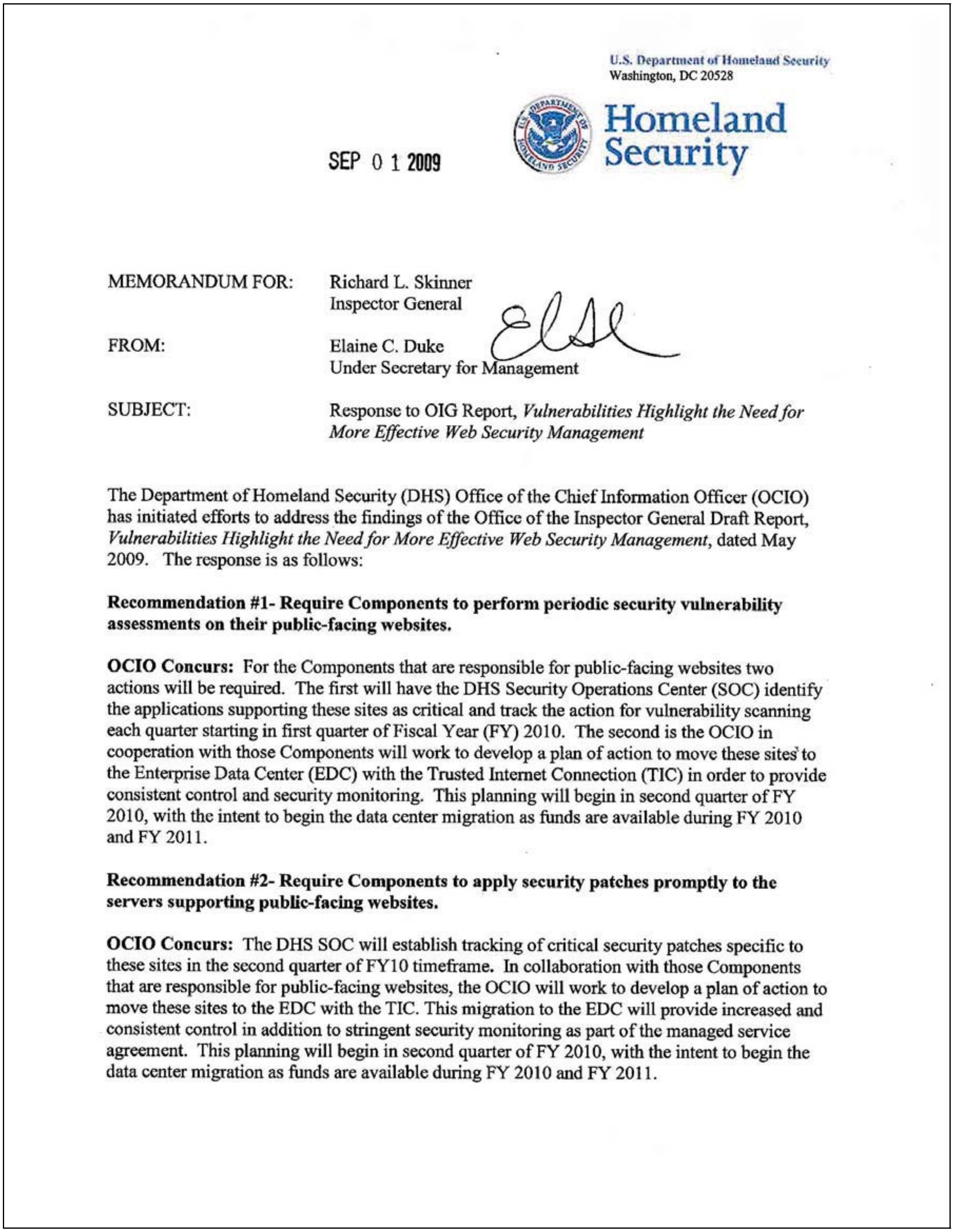
Website	Component
cbp.gov	CBP
interactive.dhs.gov	DHS HQ
fema.gov	FEMA
fletc.gov	FLETC
ice.gov	ICE
us-cert.gov	NPPD
twicprogram.tsa.dhs.gov	TSA
uscg.mil	USCG
uscis.gov	USCIS

Note: We did not evaluate the USSS website for technical vulnerabilities, as it is hosted by the Treasury.

We conducted this performance audit between November 2008 and April 2009 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Major OIG contributors to the audit are identified in Appendix C.

The principal OIG points of contact for the evaluation are Frank Deffer, Assistant Inspector General, Office of Information Technology, at (202) 254-4041 and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254-5444.

Appendix B
Management Comments to the Draft Report



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

Homeland
Security

SEP 0 1 2009

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Elaine C. Duke
Under Secretary for Management

SUBJECT: Response to OIG Report, *Vulnerabilities Highlight the Need for More Effective Web Security Management*

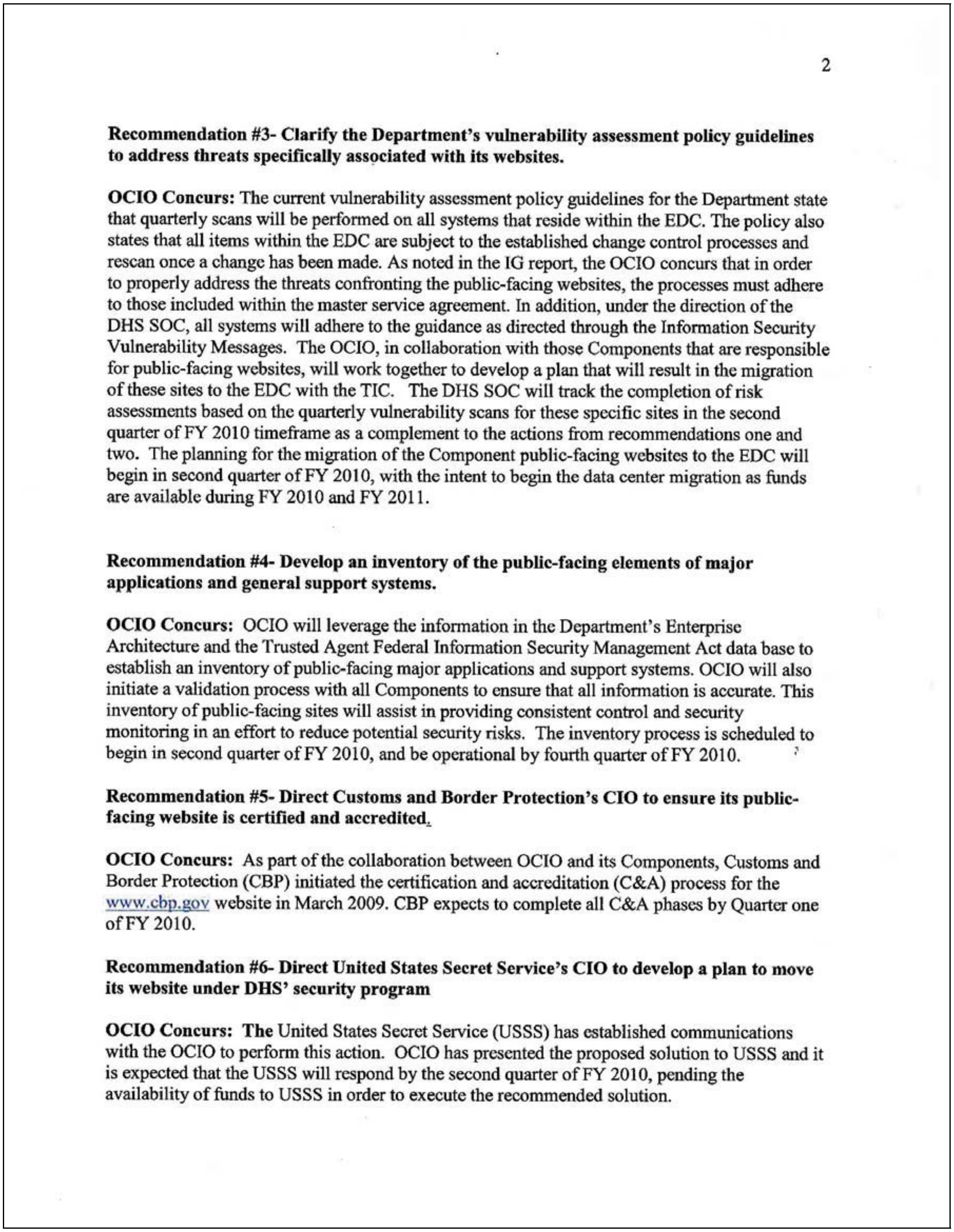
The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) has initiated efforts to address the findings of the Office of the Inspector General Draft Report, *Vulnerabilities Highlight the Need for More Effective Web Security Management*, dated May 2009. The response is as follows:

Recommendation #1- Require Components to perform periodic security vulnerability assessments on their public-facing websites.

OCIO Concurs: For the Components that are responsible for public-facing websites two actions will be required. The first will have the DHS Security Operations Center (SOC) identify the applications supporting these sites as critical and track the action for vulnerability scanning each quarter starting in first quarter of Fiscal Year (FY) 2010. The second is the OCIO in cooperation with those Components will work to develop a plan of action to move these sites to the Enterprise Data Center (EDC) with the Trusted Internet Connection (TIC) in order to provide consistent control and security monitoring. This planning will begin in second quarter of FY 2010, with the intent to begin the data center migration as funds are available during FY 2010 and FY 2011.

Recommendation #2- Require Components to apply security patches promptly to the servers supporting public-facing websites.

OCIO Concurs: The DHS SOC will establish tracking of critical security patches specific to these sites in the second quarter of FY10 timeframe. In collaboration with those Components that are responsible for public-facing websites, the OCIO will work to develop a plan of action to move these sites to the EDC with the TIC. This migration to the EDC will provide increased and consistent control in addition to stringent security monitoring as part of the managed service agreement. This planning will begin in second quarter of FY 2010, with the intent to begin the data center migration as funds are available during FY 2010 and FY 2011.



Recommendation #3- Clarify the Department's vulnerability assessment policy guidelines to address threats specifically associated with its websites.

OCIO Concurs: The current vulnerability assessment policy guidelines for the Department state that quarterly scans will be performed on all systems that reside within the EDC. The policy also states that all items within the EDC are subject to the established change control processes and rescan once a change has been made. As noted in the IG report, the OCIO concurs that in order to properly address the threats confronting the public-facing websites, the processes must adhere to those included within the master service agreement. In addition, under the direction of the DHS SOC, all systems will adhere to the guidance as directed through the Information Security Vulnerability Messages. The OCIO, in collaboration with those Components that are responsible for public-facing websites, will work together to develop a plan that will result in the migration of these sites to the EDC with the TIC. The DHS SOC will track the completion of risk assessments based on the quarterly vulnerability scans for these specific sites in the second quarter of FY 2010 timeframe as a complement to the actions from recommendations one and two. The planning for the migration of the Component public-facing websites to the EDC will begin in second quarter of FY 2010, with the intent to begin the data center migration as funds are available during FY 2010 and FY 2011.

Recommendation #4- Develop an inventory of the public-facing elements of major applications and general support systems.

OCIO Concurs: OCIO will leverage the information in the Department's Enterprise Architecture and the Trusted Agent Federal Information Security Management Act data base to establish an inventory of public-facing major applications and support systems. OCIO will also initiate a validation process with all Components to ensure that all information is accurate. This inventory of public-facing sites will assist in providing consistent control and security monitoring in an effort to reduce potential security risks. The inventory process is scheduled to begin in second quarter of FY 2010, and be operational by fourth quarter of FY 2010.

Recommendation #5- Direct Customs and Border Protection's CIO to ensure its public-facing website is certified and accredited.

OCIO Concurs: As part of the collaboration between OCIO and its Components, Customs and Border Protection (CBP) initiated the certification and accreditation (C&A) process for the www.cbp.gov website in March 2009. CBP expects to complete all C&A phases by Quarter one of FY 2010.

Recommendation #6- Direct United States Secret Service's CIO to develop a plan to move its website under DHS' security program

OCIO Concurs: The United States Secret Service (USSS) has established communications with the OCIO to perform this action. OCIO has presented the proposed solution to USSS and it is expected that the USSS will respond by the second quarter of FY 2010, pending the availability of funds to USSS in order to execute the recommended solution.

Appendix C
Major Contributors to this Report

Information Security Audit Division

Edward Coleman, Director
Mike Horton, IT Officer
Barbara Bartuska, Audit Manager
Thomas Rohrback, IT Specialist
David Bunning, Program and Management Clerk

Advanced Technology Division

John Molesky, IT Specialist

Robert Durst, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretariat
Assistant Secretary for Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
CIO
Deputy CIO
Chief Information Security Officer
Director, Compliance and Oversight
Director, GAO/OIG Liaison Office
CIO Audit Liaison
Chief Information Security Officer Audit Manager
CIO, CBP
CIO, FEMA
CIO, FLETC
CIO, ICE
CIO, NPPD
CIO, TSA
CIO, USCG
CIO, USCIS
CIO, USSS

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.

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; 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.