U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

Office of the Secretary

Improvements Are Needed for Effective Web Security Management

Final Report No. OIG-12-002-A
October 21, 2011

FOR PUBLIC RELEASE

Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

October 21, 2011

MEMORANDUM FOR: Simon Szykman, Chief Information Officer

FROM: Allen Crawley Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

SUBJECT: *Improvements Are Needed For Effective*
Web Security Management
Final Report No. OIG-12-002-A

Attached is our final report for the audit of the Department's web applications security. Our audit objective was to determine whether the Department's web applications are properly secured to minimize the risk of cyber attacks. We reviewed the security of 15 public-facing web applications from eight operating units: BEA, BIS, Census, NIST, NOAA, NTIA, NTIS, and USPTO.

We found that these web applications are not properly secured to minimize the risk of cyber attacks. The majority of these web applications have well-known website vulnerabilities, misconfigured back-end databases, and outdated software that support them. Identified vulnerabilities resulted from inadequate software development practices, improper software configuration, and failure to install system updates in a timely manner.

In this final report, we have summarized the Department's response to our draft report and included the formal response as an appendix. We will post this report on the OIG website pursuant to section 8L of the Inspector General Act of 1978, as amended.

Under Department Administrative Order 213-5, you have 60 calendar days from the date of this memorandum to submit an audit action plan to us. The plan should outline the actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extended to us by your staff as well as operating units' staff during our audit. Please direct any inquiries regarding this report to me at (202) 482-1855 or Dr. Ping Sun, Director, IT Security, at (202) 482-6121, and refer to the report title in all correspondence.

Attachment

cc: Dr. Steve Landefeld, Director, Bureau of Economic Analysis
Eric L. Hirschhorn, Under Secretary for Industry and Security
Dr. Robert M. Groves, Director, U.S. Census Bureau
Dr. Patrick Gallagher, Director, National Institute of Standards and Technology
Dr. Jane Lubchenco, Administrator, National Oceanic and Atmospheric Administration

Lawrence E. Strickling, Administrator, National Telecommunications and Information Administration
Bruce Borzino, Director of the National Technical Information Service
David Kappos, Director of the U.S. Patent and Trademark Office
Earl Neal, Director, Office of IT Security, Infrastructure and Technology
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

Report In Brief

U.S. Department of Commerce Office of Inspector General

October 21, 2011

Improvements Are Needed for Effective Web Security Management *(OIG-12-002-A)*

Why We Did This Review

The Federal Information Security Management Act of 2002 requires agencies to secure systems through the use of cost-effective management, operational, and technical controls. In addition, the Department's IT Security policy reinforces these requirements. Accordingly, this report examines whether the Department's web applications are properly secured to minimize the risk of cyber attacks.

Background

In recent years, the federal government and the Department in particular have taken advantage of Internet-based technologies to provide a wide range of essential information to the public. The Internet has become central to the Department's mission to promote growth and retool the economy for sustained U.S. leadership in the 21st century. As this trend continues, the Department inevitably faces greater cybersecurity risks.

Compromised websites could aid intrusions into organizations' internal systems and networks. Therefore, it is essential to configure and maintain web applications properly to protect the confidentiality, integrity, and availability of information supporting the Department's mission.

What We Found

Our assessment identified significant vulnerabilities resulting from inadequate software development practices, improper software configuration, and failure to install system updates in a timely manner. We found critical vulnerabilities in 12 of 15 (or 80 percent of) web applications we reviewed. The majority of web applications have well-known website vulnerabilities, misconfigured back-end databases, and outdated software that support them. Specifically, we found:

- *Websites vulnerable to known weaknesses*, potentially allowing compromise of the data stored on the application and users' computers;
- *Back-end databases not properly configured*, potentially granting an attacker access to sensitive data; and
- *Web applications residing on unsecure software*, increasing the risk of being compromised.

Combined, these security weaknesses put both web applications and users' computers at greater risk of compromise, resulting in disruption of services or unauthorized disclosure of sensitive information.

What We Recommended

We recommend that the Department's Chief Information Officer work with operating unit senior management to:

- Ensure that operating units take corrective action to mitigate vulnerabilities we found during our vulnerability scan assessments;
- Expand the Department's vulnerability scanning practice to include application-level assessments, such as database and website scans; and
- Utilize security best practices for publicly accessible web applications, such as users' input validation, to ensure that only legitimate information is accepted.

Contents

Introduction

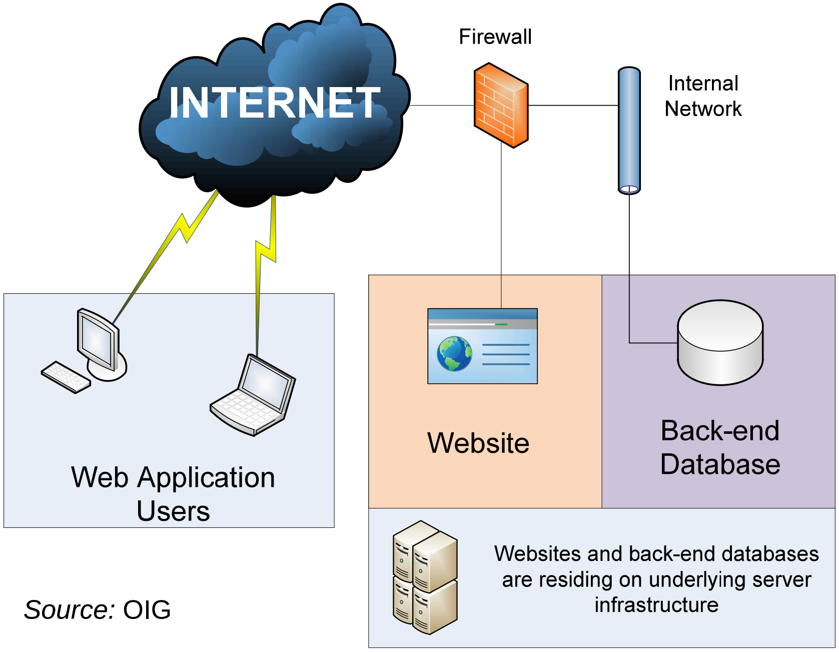
In recent years, the federal government and the Department of Commerce in particular have taken advantage of Internet-based technologies, such as web applications, to provide a wide range of essential technical, economic, social, and environmental information to the public. In addition, the Internet has become central to the Department's mission to promote growth and retool the economy for sustained U.S. leadership in the 21st century. As this trend continues, the Department inevitably faces greater cybersecurity risks over the Internet—where attacks on commerce, vital business sectors, and government agencies have grown exponentially. Recently, two hacker groups have declared war on any government or agency website, attacking major government sites such as those hosted by the U.S. Senate and the Central Intelligence Agency.[1]

Public-facing web applications have additional security risks due to limited network boundary protection. A typical web application consists of:

- a *website*, which is the front-end interface for users to interact with the application via a web browser;
- a *back-end database*, which stores the application data; and
- supporting *server infrastructure*, which hosts the website and database (see figure 1).

Compromised websites could serve as an entry point for intrusions into organizations' internal systems and networks. Therefore, it is essential to configure and maintain these applications properly to protect the confidentiality, integrity, and availability of information supporting the Department's mission.

Figure 1. Major Components of a Typical Web Application


INTERNET
Firewall
Internal Network
Web Application Users
Website
Back-end Database
Websites and back-end databases are residing on underlying server infrastructure

Source: OIG

[1] McCaney, K. June 20, 2011. LulzSec, Anonymous Declare War on Government Websites. *Government Computer News*.

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to secure systems through the use of cost-effective management, operational, and technical controls. The goal is to provide adequate security commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency. In addition, the Department's IT Security policy reinforces these requirements.[2] Accordingly, the objective of this performance audit is to determine whether the Department's web applications are properly secured to minimize the risk of cyber attacks.

We assessed a targeted sample of 15 public-facing web applications selected from 8 operating units (OUs) that support the Department's mission. Five of the selected applications generated annual revenue of over $245 million in fiscal year (FY) 2010 through online sales of goods, services, and permits. The remaining 10 applications supported export control activities, frequency spectrum management, satellite-aided search and rescue, and various mandatory business surveys.

Using commercial software tools, we conducted comprehensive vulnerability assessments on the selected websites, back-end databases, and underlying server infrastructure to evaluate their security posture. We tested those components externally from the Internet and internally from the OUs' networks for known security weaknesses. As a result, we found that these web applications are not properly secured to minimize the risk of cyber attacks. Our assessment identified significant vulnerabilities that resulted from inadequate software development practices, improper software configuration, and failure to install system updates in a timely manner.

We have detailed the objective, scope, and methodology of our audit in Appendix A.

[2] The Department's Information Technology Security Program Policy (ITSPP) specifies the security controls required to be implemented on the Department's information systems as well as addressing FISMA requirements.

Findings and Recommendations

I. The Department's Web Applications Have Significant Security Weaknesses That Put Them at Risk of Successful Cyber Attacks

Our security assessment identified various vulnerabilities in all 15 web applications we reviewed. Particularly, we found critical vulnerabilities[3] in 12 of 15 (80 percent) web applications. The majority of web applications have well-known website vulnerabilities, misconfigured back-end databases, and outdated software that support them. Combined security weaknesses can put both web applications and users' computers at a greater risk of compromise, resulting in disruption of services or unauthorized disclosure of sensitive information.

A. Websites Are Vulnerable to Known Weaknesses, Potentially Allowing Compromise of the Data Stored on the Application and Users' Computers

Eleven of the 15 (73 percent) applications contained vulnerabilities known as cross-site scripting (XSS) and structured query language (SQL) injection. Often, web users are asked to submit information such as their name, address, or credit card numbers via forms (referred to as web forms) on the web application. XSS vulnerabilities can allow an attacker to inject malicious code into a web application, by using the web forms, and then execute the malicious code on a user's computer when the user is tricked into accessing the vulnerable site. Affected applications can be used to launch attacks on users' computers—causing, at a minimum, embarrassment and diminishing public trust in the Department. Often such attacks can result in hackers gaining credentials (username and password) to the web application itself, thus compromising the confidentiality, integrity, and availability of the data residing on the application.

SQL injection allows an attacker to bypass the security controls of the front-end website and extract, modify, or destroy the data by issuing direct commands to the back-end database via web forms. This type of critical security weakness seriously undermines the confidentiality, integrity, and availability of the data residing on the application, specifically on the back-end database. We found that one web application, which collects credit card information, is vulnerable to SQL injection.

These vulnerabilities exist because a user's input into a web form is not validated to eliminate potentially embedded malicious code before being accepted by a web application. Proper software programming practices should be implemented while developing web applications to ensure that users can submit only legitimate input via web forms.

B. Back-End Databases Are Not Properly Configured, Potentially Granting an Attacker Access to Sensitive Data

The Department's security policy requires the use of passwords to support authentication for its information systems and applications.[4] In addition, the policy establishes the requirements for a strong password such as the number and type of characters that users should employ.

[3] Critical vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing remote execution of malicious commands.
[4] Commerce Interim Technical Requirements 009: Password Requirements

Seven of the 15 (47 percent) applications assessed are not compliant with password requirements. Specifically, back-end database accounts were configured to have no passwords for authentication or weak passwords (such as common dictionary words or passwords that are the same as user login name). We found three instances of accounts associated with the weak password had database administrator privileges. This security flaw put data stored on those databases at a greater risk of unauthorized disclosure, alteration, or destruction. For example, one web application supporting search and rescue operations had a weak password that allowed full access to the sensitive data stored on the database. The integrity of this data is extremely important, and any unauthorized alteration or destruction could seriously undermine search and rescue activities, thus placing human life at risk.

We also discovered that 5 of the 15 (33 percent) web applications allow excessive access privileges on back-end databases. Such excessive privileges can allow any user to obtain sensitive system information such as other users’ passwords. These flaws, when combined with other identified vulnerabilities, can serve as leverage for further cyber attacks.

C. Web Applications Reside on Unsecure Software, Increasing the Risk of Being Compromised

The Department’s security policy, encompassing minimum security requirements for federal systems and the National Institute of Standards and Technology Recommended Security Controls for Federal Information Systems, requires by reference the identification, reporting, and correcting of software flaws that result in potential security vulnerabilities.[5] These requirements also include the mandate that newly released security patches, service packs, and “hot fixes” must be promptly installed. Our assessment identified that 11 of 15 (73 percent) applications reside on unsecure operating systems, thus putting them at risk of being compromised. Specifically, we found that operating systems, which host websites and back-end databases, are not being updated in a timely manner. Because of that, these applications are subject to multiple security flaws. In addition, three applications reside on operating systems that are no longer supported by the manufacturers. This means that there are no security patches or updates available, and the manufacturers are less likely to investigate and report new vulnerabilities. Operating systems are the foundation for web applications. When multiple security vulnerabilities coexist with outdated operating systems, the applications become more vulnerable to cyber attacks.

Table 1 presents a summary of each OU’s critical vulnerabilities discussed in this report. The identified security weaknesses are primarily caused by inadequate software development practices, improper configuration of software products (particularly databases), and failure to install system updates in a timely manner.

In addition, vulnerability assessment activities within the Department do not consistently cover websites and databases. The Department’s security policy requires OUs to conduct vulnerability scanning (automated detection of software flaws and malicious code in system components) quarterly or when significant new vulnerabilities potentially affecting the system are identified

[5] Flaw remediation is required control SI-2 in National Institute of Standards and Technology, August 2009. *Recommended Security Controls for Federal Information Systems,* NIST Special Publication 800-53, Revision 3. Gaithersburg, MD: NIST, D-7.

and reported (for example, in a bulletin from a software manufacturer). However, beyond that requirement, the policy includes no specification of the scope and methodology of those vulnerability assessments. We found that this has resulted in inconsistent practices of vulnerability scanning across the Department. For example, only eight of the 15 (53 percent) applications have their front-end websites and back-end databases scanned using an application-specific scanning tool. Website scanning can identify critical application vulnerabilities such as cross-site scripting and SQL injection. Database scanning can check for inadequate security configuration settings on databases, such as weak passwords or excessive privileges. By expanding scanning coverage on websites and databases using application-specific scanning tools, the OUs will be able to identify vulnerabilities on all components of web applications.

Table 1. Identified Critical Vulnerabilities by Operating Unit

OU	Website Vulnerabilities		Back-End Database Vulnerability		Server Operating System Vulnerabilities	
	SQL Injection	Cross-Site Scripting	Weak Passwords	Excessive Access Privilege	Unsupported OS	Unpatched/ Outdated System Software
BEA		X	X	X		
BIS						
Census		X	N/A*	N/A*	X	X
NIST		X		X		X
NOAA/NESDIS		X	X	X	X	X
NOAA/NMFS			N/A*	N/A*		
NOAA/NMFS	X	X	X			X
NOAA/NOS			N/A*	N/A*		
NTIA		X		X		X
NTIS		X	X	X	X	X
USPTO						X
USPTO		X	X			X
USPTO		X	X			X
USPTO		X				X
USPTO		X	X			X

* Databases were not scanned due to the limited capability of vulnerability assessment software tools.
Source: OIG

During our fieldwork, we shared our preliminary assessment results with OU staff, who are currently taking corrective actions to remediate the vulnerabilities identified. OUs remediated the most critical issues, such as weak or no passwords on back-end databases, immediately after our discovery.

II. Recommendations

We recommend that the Department's Chief Information Officer work with operating unit senior management to:

1. Ensure that operating units take corrective action as necessary to mitigate vulnerabilities we found during our vulnerability scan assessments;
2. Expand the Department's vulnerability scanning practice to include application-level assessments, such as database and website scans; and
3. Utilize security best practices for publicly accessible web applications, such as users' input validation to ensure that only legitimate information is accepted, as recommended by NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers* Version 2 (September 2007).

Summary of Agency Comments and OIG Response

We reviewed the Department's official response to our draft report dated September 21, 2011. In its response, the Department concurred with our findings and recommendations—while noting its effort to increase its IT security posture in FY 2011, including a deployment of an enterprise-wide vulnerability management capability.

The Department also provided technical comments separately, which we addressed in the report where appropriate.

Appendix A: Objective, Scope, and Methodology

Our objective was to determine whether the Department's web applications are properly secured to minimize the risk of cyber attacks. This report describes key vulnerabilities that require senior management's attention. In general, we do not detail our findings for the individual applications reviewed unless such is necessary for clarity.

The Department's Office of Chief Information Officer provided us with an inventory of over 800 web applications. Our assessment focused on a targeted sample of 15 web applications from the following departmental operating units/subunits (See table I).

Table I. Applications Selected for Technical Assessment [a]

Operating Unit	**Number of Web Applications**
Bureau of Economic Analysis (BEA)	1
Bureau of Industry and Security (BIS)	1
U.S. Census Bureau (Census)	1
National Institute of Standards and Technology (NIST)	1
National Oceanic and Atmospheric Administration (NOAA) National Environmental Satellite, Data, and Information Service (NESDIS) National Marine Fisheries Service (NMFS) National Ocean Service (NOS)	4
National Telecommunications and Information Administration (NTIA)	1
National Technical Information Service (NTIS)	1
U.S. Patent and Trademark Office (USPTO)	5

Source: OIG

[a] For security purposes, OIG will not disclose specific details about the types of web applications assessed.

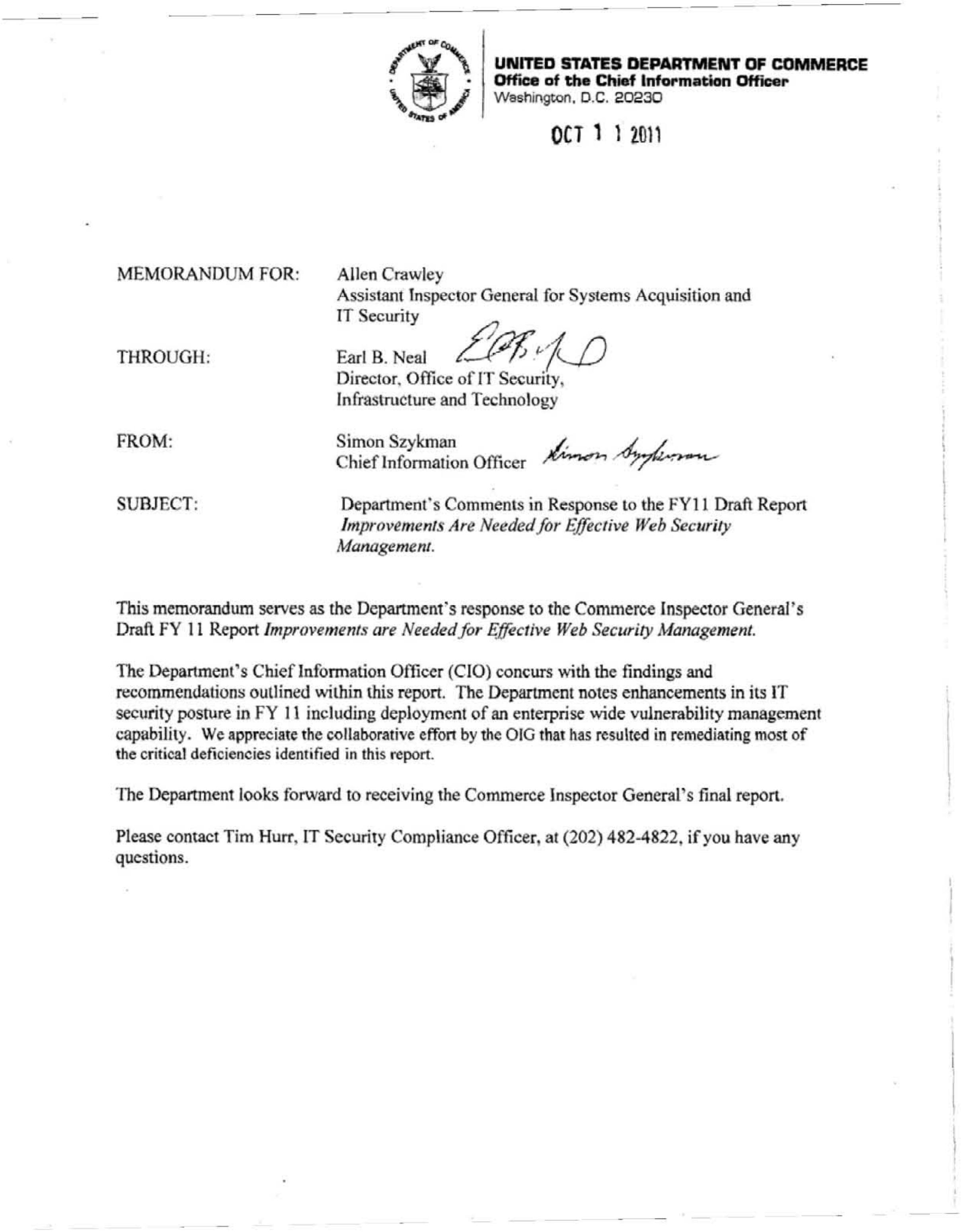
We selected these public-facing web applications based on their business functions, which potentially store or process sensitive, privacy or mission-critical data such as credit cards numbers and business or personal information.

Using a combination of automated software tools and manual review, we performed internal (e.g., bypassing network boundary protection, such as firewalls) and external vulnerability assessments on 15 selected public facing web applications, focusing on their front-end website interfaces, the back-end databases, and supporting servers. Due to the limited capability of vulnerability assessment software tools, we were not able to scan back-end databases associated with three web applications. For two other web applications, we limited our scans to their test environment systems due to the concern that such activity can disrupt the service. We validated that the test systems had very similar configurations to the production systems. We shared our assessment results with web application owners, and sought their feedback to validate identified vulnerabilities to eliminate false positives. We also interviewed operating unit staff as needed to assess the effectiveness of the Department's security practices.

We conducted our field work from January to August 2011 at Commerce headquarters, various field offices, and contractor hosting facilities in the District of Columbia, Florida, Maryland, and Virginia.

We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated August 31, 2006. We conducted this performance audit in accordance with 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.

Appendix B: Response to OIG Draft Report



UNITED STATES DEPARTMENT OF COMMERCE
Office of the Chief Information Officer
Washington, D.C. 20230

OCT 1 1 2011

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for Systems Acquisition and
IT Security

THROUGH: Earl B. Neal
Director, Office of IT Security,
Infrastructure and Technology

FROM: Simon Szykman
Chief Information Officer Simon Szykman

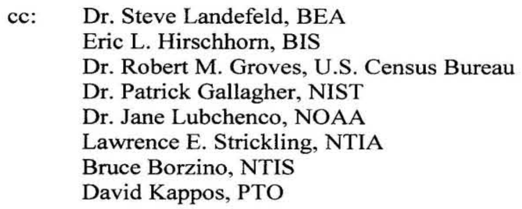
SUBJECT: Department's Comments in Response to the FY11 Draft Report
Improvements Are Needed for Effective Web Security Management.

This memorandum serves as the Department's response to the Commerce Inspector General's Draft FY 11 Report *Improvements are Needed for Effective Web Security Management.*

The Department's Chief Information Officer (CIO) concurs with the findings and recommendations outlined within this report. The Department notes enhancements in its IT security posture in FY 11 including deployment of an enterprise wide vulnerability management capability. We appreciate the collaborative effort by the OIG that has resulted in remediating most of the critical deficiencies identified in this report.

The Department looks forward to receiving the Commerce Inspector General's final report.

Please contact Tim Hurr, IT Security Compliance Officer, at (202) 482-4822, if you have any questions.



cc:
Dr. Steve Landefeld, BEA
Eric L. Hirschhorn, BIS
Dr. Robert M. Groves, U.S. Census Bureau
Dr. Patrick Gallagher, NIST
Dr. Jane Lubchenco, NOAA
Lawrence E. Strickling, NTIA
Bruce Borzino, NTIS
David Kappos, PTO

(1200000-117)