OFFICE OF THE SECRETARY

Inadequate Practice and Management Hinder Incident Detection and Response

FINAL REPORT NO. OIG-14-017-A

APRIL 24, 2014

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

FOR PUBLIC RELEASE

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

April 24, 2014

MEMORANDUM FOR: Simon Szykman
Chief Information Officer

Allen Crawley

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

SUBJECT: *Inadequate Practice and Management Hinder Incident Detection and Response*—Final Report No. OIG-14-017-A

Attached please find the final report of our audit of the Department's incident detection and response practices. In accordance with the Federal Information Security Management Act of 2002, we reviewed incident detection and response practices at four bureaus: Bureau of Economic Analysis (BEA), Bureau of Industry and Security (BIS), International Trade Administration (ITA), and United States Patent and Trademark Office (USPTO). We also evaluated these capabilities at the Herbert C. Hoover Building Security Operations Center (SOC). Our objective was to determine whether key security measures are in place to adequately monitor networks, detect malicious activities, and handle cyber incidents.

We found that (1) bureaus' actions in response to suspicious network activities may not stop cyber attacks in a timely manner and (2) lack of collaboration prevents the bureaus from realizing full benefits of incident detection and response capabilities provided by Managed Trusted Internet Protocol Services.

We have summarized your response in the report and included the formal response as appendix B. The final report will be posted on the OIG's website pursuant to section 8L of the Inspector General Act of 1978, as amended.

In accordance with Departmental Administrative Order 213-5, please submit to us within 60 calendar days of the date of this memorandum an action plan that responds to the recommendations in this report

We appreciate the cooperation and courtesies extended to us by your staff and bureau staff during our audit. If you have any questions or concerns about this report, please contact me at (202) 482-1855 or Dr. Ping Sun, Director for IT Security, at (202) 482- 6121.

Attachment

cc: Kirit Amin, Deputy Chief Information Officer and Chief Technology Officer
Brian Callahan, Chief Information Officer, BEA
Eddie Donnell, Acting Chief Information Officer, BIS
Ken Berman, Acting Chief Information Officer, ITA
John B. Owens II, Chief Information Officer, USPTO
Rod Turk, Director, Office of Cyber Security
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

Report In Brief

APRIL 24, 2014

Background

Pervasive and sustained cyber attacks against the United States could have a devastating effect on federal and nonfederal systems, disrupt the operations of governments and businesses, and impact the lives of the American people.

The Department of Commerce is under threat because of its reliance on Internet-based technologies, which interconnect its IT systems and facilitate business with the public. Having effective incident detection and response is crucial to minimizing the impact of cyber attacks and maintaining the Department's business operations.

Why We Did This Review

The Federal Information Security Management Act (FISMA) of 2002 requires federal agencies to establish incident response capabilities. Performing incident response effectively is a complex undertaking that requires continual monitoring for attacks; establishing clear procedures for prioritizing handling of incidents; collecting, analyzing, and reporting data; and communication within and outside of the organization.

Our objective in conducting this audit was to determine whether key security measures are in place to adequately monitor networks, detect malicious activities, and handle cyber incidents.

OFFICE OF THE SECRETARY

Inadequate Practice and Management Hinder Incident Detection and Response

OIG-14-017-A

WHAT WE FOUND

As part of our FISMA audit work, we evaluated incident detection and response capabilities at four Department of Commerce bureaus: the Bureau of Economic Analysis, Bureau of Industry and Security, International Trade Administration, and United States Patent and Trademark Office. We also evaluated these capabilities at the Herbert C. Hoover Building Security Operations Center (SOC) within the Office of the Secretary. We found that

1. *Bureaus' actions in response to suspicious network activities may not stop cyber attacks in a timely manner.* All bureaus that we reviewed have established an incident detection and response capability, although the degree of capabilities varies. To determine how the bureaus respond to real-time incidents, we performed external testing against their Web sites from the Internet. Only one bureau intervened to completely block our test. The rest either took no action or did not take timely action in response to our test.

2. *Lack of collaboration prevents the bureaus from realizing the full benefits of incident detection and response capabilities provided by Managed Trusted Internet Protocol Services (MTIPS).* MTIPS offers Internet and bundled security services that bureaus use to comply with the Office of Management and Budget's Trusted Internet Connection initiative. We found that bureaus do not consider MTIPS security services effective in supporting incident detection and response. We found that most communication between bureaus and the provider occurred when they initiated MTIPS services—and that little communication related to security services has occurred since then. In addition, bureaus indicated that they were not receiving significant incident monitoring and detection services.

WHAT WE RECOMMEND

We recommend that the Department's Chief Information Officer work with the bureaus' management to ensure that

1. Bureaus follow the National Institute of Standards and Technology's *Computer Security Incident Handling Guide* to take timely action in response to potential cyber attacks.

2. Bureaus without around-the-clock SOC coverage work with the MTIPS provider to evaluate MTIPS services to fill gaps in SOC coverage after business hours.

3. Bureaus interact with the MTIPS provider to (a) explore opportunities that leverage MTIPS services to reduce or eliminate security services currently handled by the bureau and (b) ensure that MTIPS security services are fully delivered and effectively utilized.

4. Determine the feasibility and cost effectiveness of independently assessing incident management capabilities at all bureaus' SOCs.

Contents

Introduction

Pervasive and sustained cyber attacks against the United States could have a devastating effect on federal and nonfederal systems, disrupt the operations of governments and businesses, and impact the lives of the American people. The Department is under constant threat because of its reliance on Internet-based technologies, which interconnect its IT systems and facilitate business with the public. Thus, having effective incident detection and response is crucial to minimize the impact of cyber attacks and maintain the Department's business operations.

Our June 2013 Economic Development Administration (EDA) audit[1] found that EDA's critical incident response decisions were based on inaccurate information and that deficiencies in the Department's incident response program impeded EDA's response, which resulted in a prolonged disruption of EDA's normal business operations and the unnecessary spending of more than $2.7 million for its recovery activities. This review highlighted challenges that the Department faces when responding to a cyber incident.

The Federal Information Security Management Act (FISMA)[2] requires federal agencies to establish incident response capabilities. Performing incident response effectively is a complex undertaking that requires continual monitoring for attacks; establishing clear procedures for prioritizing handling of incidents; collecting, analyzing, and reporting data; and communication within and outside of the organization.

[1] U.S. Department of Commerce Office of Inspector General, June 26, 2013. *Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted*, OIG-13-027-A. Washington, DC: DOC OIG.

[2] The Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C § 3541 (2002), *et seq.*, requires agencies to secure systems through the use of cost-effective management, operational, and technical controls. The statute's goal is to provide adequate security commensurate with the risk and extent of harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency. In addition, FISMA requires inspectors general to evaluate agencies' information security programs and practices by assessing a representative subset of agency systems, and results are reported to the Office of Management and Budget, the Department of Homeland Security, and Congress annually.

Objective, Findings, and Recommendations

As part of our FISMA audit work, we evaluated incident detection and response capabilities at four bureaus: Bureau of Economic Analysis (BEA), Bureau of Industry and Security (BIS), International Trade Administration (ITA), and United States Patent and Trademark Office (USPTO). We also evaluated these capabilities at the Herbert C. Hoover Building (HCHB) Security Operations Center (SOC). HCHB SOC, which is part of the Department's Office of the Chief Information Officer (OCIO) within the Office of the Secretary (OS), coordinates with the Department's Computer Security Incident Response Team (DOC CIRT) to provide incident detection and response services to seven bureaus with headquarters located at HCHB. Our objective was to determine whether key security measures are in place to adequately monitor networks, detect malicious activities, and handle cyber incidents. See appendix A for details regarding our objective, scope, and methodology.

We found that (1) bureaus' actions in response to suspicious network activities may not stop cyber attacks in a timely manner and (2) lack of collaboration prevents the bureaus from realizing full benefits of incident detection and response capabilities provided by Managed Trusted Internet Protocol Services.

I. Bureaus' Actions in Response to Suspicious Network Activities May Not Stop Cyber Attacks in a Timely Manner

Incident detection is the process of monitoring network activities and analyzing them for signs of possible security violations or imminent cyber attacks. Various network activities, such as executing malware or gaining unauthorized access to systems from the Internet, can trigger a potential cyber security incident. To effectively respond to a potential incident, responders must quickly analyze and validate each incident by following an established process. Based on National Institute of Standards and Technology (NIST) guidance,[3] responders should:

1. Rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring.

2. Based on that analysis, prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident (e.g., incident responders may decide to prevent a cyber attack by blocking all network traffic originating from the attacker's computer).

3. Document each step taken in the course of incident handling.

All bureaus we reviewed have established incident detection and response capabilities, although the extent of these capabilities varies. For example, one bureau provides around-the-clock

[3] U.S. Department of Commerce, National Institute of Standards and Technology, August 2012. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, SP 800-61, Rev. 2. Gaithersburg, MD: NIST.

monitoring coverage at an operations center, whereas another provides monitoring at a center by having only two incident detection analysts working regular business hours. To see how the bureaus responded to real-time incidents, we used an automated web application security assessment tool to test their public-facing Web sites by accessing them from the Internet. Testing the Web sites simulated a cyber event consisting of prolonged suspicious network traffic that mimics real-world hacking techniques and cyber attacks. We analyzed information such as intrusion detection system (IDS) logs and alerts generated during the test, and evaluated actions taken by the bureaus in response to our testing.

Although all five bureaus' automated tools detected and logged our testing activities, we found that (1) one bureau performed analysis of our simulated cyber event and intervened to completely block our testing; (2) one bureau did not analyze our simulated cyber event in a timely manner; and (3) three bureaus did not perform any analysis and did not take any action to respond to our testing.

Below is a summary of bureaus' actions in response to our testing:[4]

- Bureau 1 conducted timely analysis of the cyber attack generated by our testing and, before our testing was complete, contacted its service provider and requested that all traffic originating from our test computer be blocked.

- Bureau 2 did not perform timely analysis of the cyber attack generated by our testing: analysis was performed 4 days after our testing was completed. The only incident responder assigned to analyze alert data generated by one of bureau 2's incident detection tools was not available as a result of funding limitations. Bureau 2 concluded that the systems we tested were patched and protected by its automated security tools and, therefore, took no further actions. According to bureau 2, since our test, it has made incident alert data available to multiple responders.

- Bureau 3 did not take any action to respond to the cyber attack generated by our testing. Although bureau 3's process specifically requires the blocking of network traffic similar to that generated by our testing, according to bureau 3 officials, it only had an informal discussion about this cyber event. Bureau 3 is currently working on improving its incident handling process.

- Bureau 4 did not take any action to respond to the cyber attack generated by our testing. Bureau 4 only has two analysts; according to its manager, at the time of our test, both of them were unavailable to respond to our simulated cyber attack. We found that, in addition to incident detection, these two analysts have other job responsibilities, such as data loss prevention, antivirus/malware management, and vulnerability assessment. Currently, bureau 4 is considering hiring an additional analyst.

- Bureau 5's incident responders did not intervene to completely block our testing activities. Nevertheless, one day after our testing, bureau 5 did categorize the computer used to conduct our testing among its "top 20 attackers prevented" in its daily

[4] For security reasons, we do not identify bureaus in our summary.

management briefing report. This report was based on the fact that some, but not all, of our testing traffic was blocked by bureau 5's automated security tool. This report could give bureau 5 management the impression that a cyber attack originating from that computer was prevented, even though it actually was not. Bureau 5 officials acknowledged that the incident responder did not follow the proper process to respond to our testing, and this individual is no longer with bureau 5. According to bureau 5, it has recently made improvements to its incident handling process, including reorganization of its incident responder teams.

While testing Web sites, we identified critical- and high-risk vulnerabilities that can be exploited to compromise bureaus' systems as well as users' computers. We issued vulnerability scanning report memorandums to two affected bureaus. In response, the bureaus took action to remediate identified vulnerabilities. Delays in detecting and responding to suspicious network traffic could allow an adversary enough time to look for vulnerabilities, use identified vulnerabilities to compromise systems and networks, and potentially exfiltrate sensitive information. Therefore, early detection and response to potential cyber security incidents is a crucial step in stopping cyber attacks in a timely manner and thus better protecting information systems and assets.

II. Lack of Collaboration Prevents the Bureaus From Realizing Full Benefits of Incident Detection and Response Capabilities Provided by Managed Trusted Internet Protocol Services

The Office of Management and Budget (OMB)'s Trusted Internet Connection (TIC) initiative[5] mandates that federal agencies optimize and standardize the security of their individual external network connections, including connections to the Internet. TIC's goal is to improve the federal government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of the connections. Federal agencies can comply with this mandate by acquiring Managed Trusted Internet Protocol Services (MTIPS) through the General Services Administration's Networx contract.[6]

MTIPS offers Internet service and a bundle of security services—these include providing around-the-clock centralized monitoring and control of the network perimeter (network gateway), scanning all network traffic entering or leaving internal networks, detecting and preventing malicious activities, generating alerts and records of suspicious events, and managing firewalls. If effectively utilized as intended, these security services should provide the first line of defense to federal agencies' interconnected networks, as well as enhance agencies' existing incident detection and response capabilities.

[5] Office of Management and Budget, November 20, 2007. *Implementation of Trusted Internet Connections (TIC)*, Memorandum M-08-05. Washington, DC: OMB. Also see OMB, August 28, 2008. *Transition from FTS2001 to Networx,* Memorandum M-08-26. Washington, DC: OMB.

[6] OMB, August 28, 2008. *Transition from FTS2001 to Networx,* Memorandum M-08-26. Washington, DC: OMB.

Currently, BEA, ITA, OS,[7] and USPTO acquire TIC services from the same MTIPS provider; BIS will acquire services from that provider by mid-2014. Because MTIPS provides security services in addition to Internet service, bureaus are paying substantially more for MTIPS than they previously paid for Internet service (see table 1 below). While the bureaus fully rely on Internet service provided by MTIPS, we found that they do not consider MTIPS security services effective in supporting incident detection and response.

Table 1. Pre-MTIPS Internet Service and MTIPS Monthly Costs, by Bureau

Bureau	Pre-MTIPS monthly cost for Internet service only	Current MTIPS monthly cost for Internet service and security services
USPTO	$28,027	$288,000[a]
BEA	$8,238	$14,853
ITA	$9,974	$29,239
OS	$11,000	$25,217

Source: BEA, ITA, OS, and USPTO

[a] The MTIPS provider cost is significantly higher because USPTO increased the capacity requirements of the network connection. USPTO stated that the cost of the same level of connectivity increased about 240 percent after switching to MTIPS.

The bureaus and the MTIPS provider share responsibilities for ensuring that MTIPS security services are appropriately provided and effectively used. Thus, communication and coordination between the provider and bureaus are crucial to utilizing MTIPS security services to the fullest extent. We found that most communication between the bureaus and the provider occurred when the bureaus initiated MTIPS services—and that little communication related to security services has occurred since then.

In addition, these bureaus indicated that they were not receiving significant incident monitoring and detection services. Some indicated they were receiving no security related notifications or advisories from the MTIPS provider, whereas others indicated receiving only limited notifications or advisories. For example: we learned from a discussion with the MTIPS provider that, during a 3-month period (June–August 2013), the provider investigated 54 security issues, including 2 potential attacks, associated with the bureaus' systems. However, when we followed up with the bureaus, they were completely unaware of these issues. Furthermore, one bureau has not received any incident reports since October 2012, and other bureaus expressed concern that the MTIPS portal used to communicate with the MTIPS SOC is not effective.

Each of the four bureaus we reviewed has its own set of tools that provide security services similar to those provided by MTIPS. However, the bureaus have not determined which of the

[7] Office of the Chief Information Officer within OS, provides MTIPS service access to the following bureaus: EDA, Economic Statistics Administration, Minority Business Development Administration, National Telecommunications and Information Administration, OIG, and OS.

MTIPS services that they are paying for could be used instead of, or as a supplement to, their own services, which could allow for more effective use of MTIPS. For example: ITA, which uses similar security tools as the MTIPS provider, chose not to rely on MTIPS security services. BEA and USPTO asserted that the security tools they use are better than those used by the MTIPS provider and thus minimally rely on MTIPS security services. OS realized that it is not fully utilizing MTIPS security services and, at the time of this audit, has initiated an assessment involving interaction with the MTIPS provider to leverage MTIPS services to reduce or eliminate security services currently handled in-house. ITA, BEA, and USPTO have not done similar assessments. These assessments could lead to potential cost savings.

In addition, we found that the SOCs for three bureaus we reviewed do not provide around-the-clock staffing coverage. These bureaus could possibly use MTIPS services to fill gaps in monitoring coverage of external Internet facing connections when their own SOCs are not staffed.

Other Matter

The Department has a long-term initiative—the Enterprise Security Oversight Center—to enhance Department-wide security situational awareness, by providing near-real-time cybersecurity status information and timely decision making for both the Department and its bureaus. In support of this initiative, OCIO arranged to have the Department of Homeland Security (DHS) conduct an independent assessment focusing on incident management capabilities within the Department beginning in June 2013. This assessment originally intended to include both SOCs at NOAA and HCHB. However, OCIO SOC management later decided to exclude HCHB SOC from the assessment. As a result, the Department missed an opportunity for the independent assessor's in-depth review to identify weaknesses in the HCHB SOC.

Recommendations

We recommend that the Department's Chief Information Officer work with the bureaus' management to ensure that:

1. Bureaus follow NIST's *Computer Security Incident Handling Guide* to take timely action in response to potential cyber attacks.

2. Bureaus without around-the-clock SOC coverage work with the MTIPS provider to evaluate MTIPS services to fill gaps in SOC coverage after business hours.

3. Bureaus interact with the MTIPS provider to (a) explore opportunities that leverage MTIPS services to reduce or eliminate security services currently handled by the bureau and (b) ensure that MTIPS security services are fully delivered and effectively utilized.

4. Determine the feasibility and cost effectiveness of independently assessing incident management capabilities at all bureaus' SOCs.

Summary of Agency Response and OIG Comments

In response to our draft report, the Department concurred with the overall findings and recommendations. In addition, the Department noted OIG's concern regarding communications between four of the bureaus, as outlined in the draft report and the MTIPS provider. The Department plans to meet with the provider to discuss security services rendered to all of its operating units.

The Department's response is provided in appendix B.

Appendix A: Objective, Scope, and Methodology

Our objective was to determine whether key security measures are in place to adequately monitor networks, detect malicious activities, and handle cyber incidents. We reviewed the overall Department incident management process, including monitoring, detection and response.

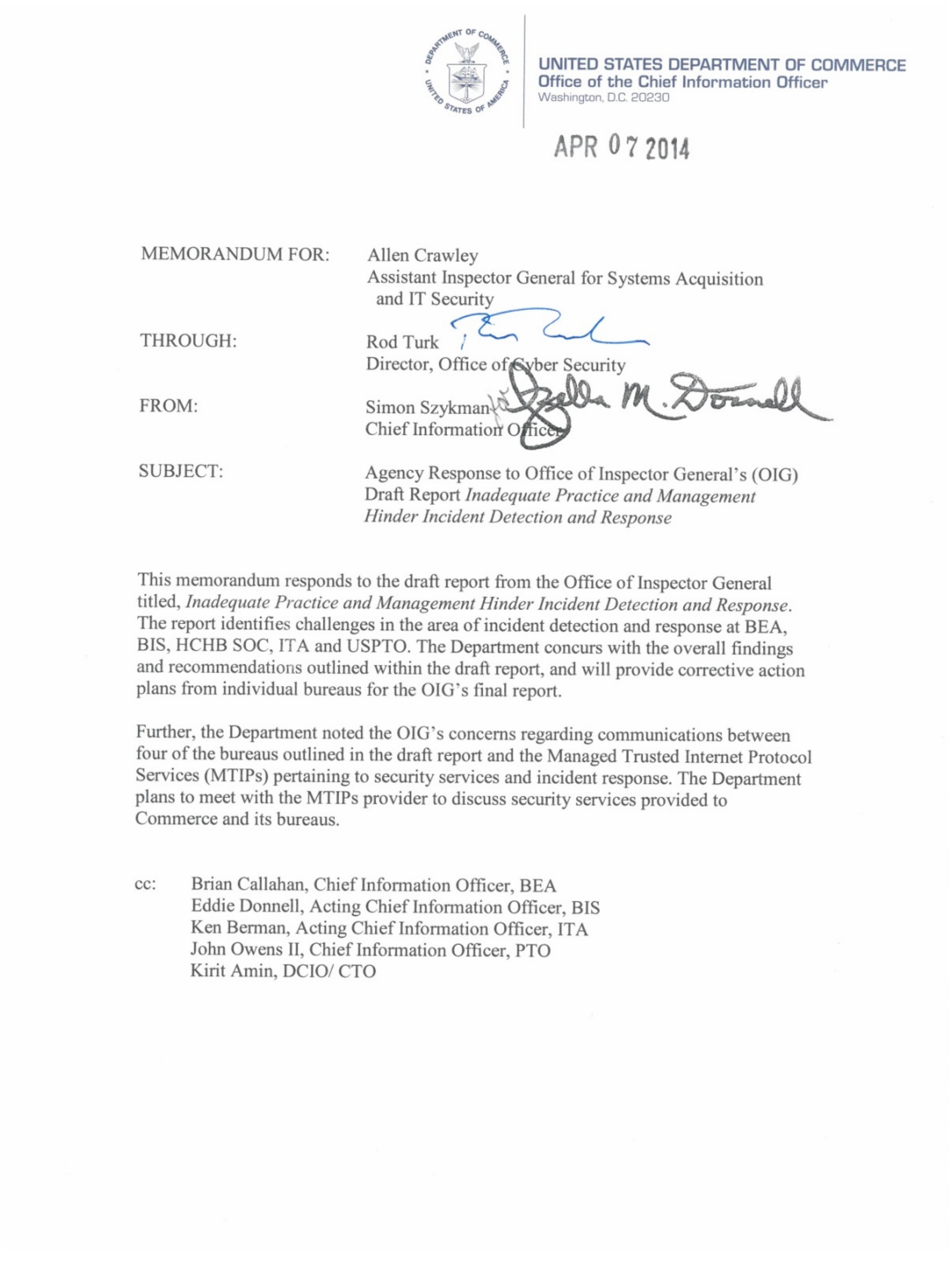
In March 2013, we conducted a survey of all the Department's bureaus to gather background information about their incident handling capabilities. Based on this survey, we selected USPTO, ITA, HCHB SOC, BEA, and BIS for in-depth review. To avoid duplicative work, we did not include Census because it had been previously assessed by GAO in 2012–2013. Also, we did not include NOAA because of a separate ongoing OIG review of its IT security program.

We reviewed internal controls significant within the context of our audit objective and employed a comprehensive methodology to validate the bureaus' incident detection and response practices. Specifically, we

- Reviewed applicable laws, regulations, and NIST guidance.
- Examined bureaus' incident detection and response policies and procedures, as well as reviewed MTIPS contract and supporting documentation.
- Interviewed Department OCIO senior executives and managers responsible for incident management.
- Interviewed bureaus' IT security officers and incident responders, as well as MTIPS provider officials and DHS United States Computer Emergency Readiness Team personnel.
- Validated bureaus' analytical process for incident handling by observing their security analysts' day-to-day actions to detect, respond to, recover from, and document incidents.
- Validated bureaus' responses to a cyber incident by using an automated software tool to generate prolonged suspicious network traffic directed at bureaus' public-facing Web sites in order to simulate cyber attacks and thus trigger actions from selected bureaus' incident responders.

We conducted our fieldwork from February 2013 to October 2013 at the Department's offices in the Washington, DC, metropolitan area. We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated April 26, 2013, and 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: Agency Response



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

APR 07 2014

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

THROUGH: Rod Turk
Director, Office of Cyber Security

FROM: Simon Szykman for Izella M. Donnell
Chief Information Officer

SUBJECT: Agency Response to Office of Inspector General's (OIG)
Draft Report *Inadequate Practice and Management*
Hinder Incident Detection and Response

This memorandum responds to the draft report from the Office of Inspector General titled, *Inadequate Practice and Management Hinder Incident Detection and Response*. The report identifies challenges in the area of incident detection and response at BEA, BIS, HCHB SOC, ITA and USPTO. The Department concurs with the overall findings and recommendations outlined within the draft report, and will provide corrective action plans from individual bureaus for the OIG's final report.

Further, the Department noted the OIG's concerns regarding communications between four of the bureaus outlined in the draft report and the Managed Trusted Internet Protocol Services (MTIPs) pertaining to security services and incident response. The Department plans to meet with the MTIPs provider to discuss security services provided to Commerce and its bureaus.

cc: Brian Callahan, Chief Information Officer, BEA
Eddie Donnell, Acting Chief Information Officer, BIS
Ken Berman, Acting Chief Information Officer, ITA
John Owens II, Chief Information Officer, PTO
Kirit Amin, DCIO/ CTO