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.