Report In Brief

U.S. Department of Commerce Office of Inspector General

October 21, 2011

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.

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

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 The majority of web applications have well-known website vulnerabilities, misconfigured back-end databases, and outdated software that support them.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.