November 2010

# INFORMATION SECURITY

## Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-43, a report to congressional committees

### Why GAO Did This Study

Over the past several years, federal agencies have rapidly adopted the use of wireless technologies for their information systems. In a 2005 report, GAO recommended that the Office of Management and Budget (OMB), in its role overseeing governmentwide information security, take several steps to help agencies better secure their wireless networks.

GAO was asked to update its prior report by (1) identifying leading practices and state-of-the-art technologies for deploying and monitoring secure wireless networks and (2) assessing agency efforts to secure wireless networks, including their vulnerability to attack.

To do so, GAO reviewed publications, guidance, and other documentation and interviewed subject matter experts in wireless security. GAO also analyzed policies and plans and interviewed agency officials on wireless security at 24 major federal agencies and conducted additional detailed testing at these 5 agencies: the Departments of Agriculture, Commerce, Transportation, and Veterans Affairs, and the Social Security Administration.

### What GAO Recommends

GAO is making two recommendations to OMB to enhance governmentwide oversight and four recommendations to the Department of Commerce for additional guidelines related to wireless security. The Department of Commerce concurred with GAO's recommendations. OMB did not provide comments on the report.

View GAO-11-43 or key components. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

### What GAO Found

GAO identified a range of leading security practices for deploying and monitoring secure wireless networks and technologies that can help secure these networks. The leading practices include the following:

- comprehensive policies requiring secure encryption and establishing usage restrictions, implementation practices, and access controls;
- a risk-based approach for wireless deployment and monitoring;
- a centralized wireless management structure that is integrated with the management of the existing wired network;
- configuration requirements for wireless networks and devices;
- incorporation of wireless and mobile device security in training;
- use of encryption, such as a virtual private network for remote access;
- continuous monitoring for rogue access points and clients; and
- regular assessments to ensure wireless networks are secure.

Agencies have taken steps to secure their wireless networks, but more can be done to improve security and to limit vulnerability to attack. Specifically, application was inconsistent among the agencies for most of the following leading practices:

- Most agencies developed policies to support federal guidelines and leading practices, but gaps existed, particularly with respect to dual-connected laptops and mobile devices taken on international travel.
- All agencies required a risk-based approach for management of wireless technologies.
- Many agencies used a decentralized structure for management of wireless, limiting the standardization that centralized management can provide.
- The five agencies where GAO performed detailed testing generally securely configured wireless access points but had numerous weaknesses in laptop and smartphone configurations.
- Most agencies were missing key elements related to wireless security in their security awareness training.
- Twenty agencies required encryption, and eight of these agencies specified that a virtual private network must be used; four agencies did not require encryption for remote access.
- Many agencies had insufficient practices for monitoring or conducting security assessments of their wireless networks.

Existing governmentwide guidelines and oversight efforts do not fully address agency implementation of leading wireless security practices. Until agencies take steps to better implement these leading practices, and OMB takes steps to improve governmentwide oversight, wireless networks will remain at an increased vulnerability to attack.