G A O
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-05-383, a report to the Honorable Wm. Lacy Clay, House of Representatives

May 2005

INFORMATION SECURITY

Federal Agencies Need to Improve Controls over Wireless Networks

Why GAO Did This Study

The use of wireless networks is becoming increasingly popular. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops. They can offer federal agencies many potential benefits but they are difficult to secure.

GAO was asked to study the security of wireless networks operating within federal facilities. This report (1) describes the benefits and challenges associated with securing wireless networks, (2) identifies the controls available to assist federal agencies in securing wireless networks, (3) analyzes the wireless security controls reported by each of the 24 agencies under the Chief Financial Officers (CFO) Act of 1990, and (4) assesses the security of wireless networks at the headquarters of six federal agencies in Washington, D.C.

What GAO Recommends

GAO recommends that the Director of the Office of Management and Budget (OMB) instruct the agencies to ensure that wireless network security is incorporated into their agencywide information security programs in accordance with the Federal Information Security Management Act. OMB generally agreed with the contents of this report.

www.gao.gov/cgi-bin/getrpt?GAO-05-383.

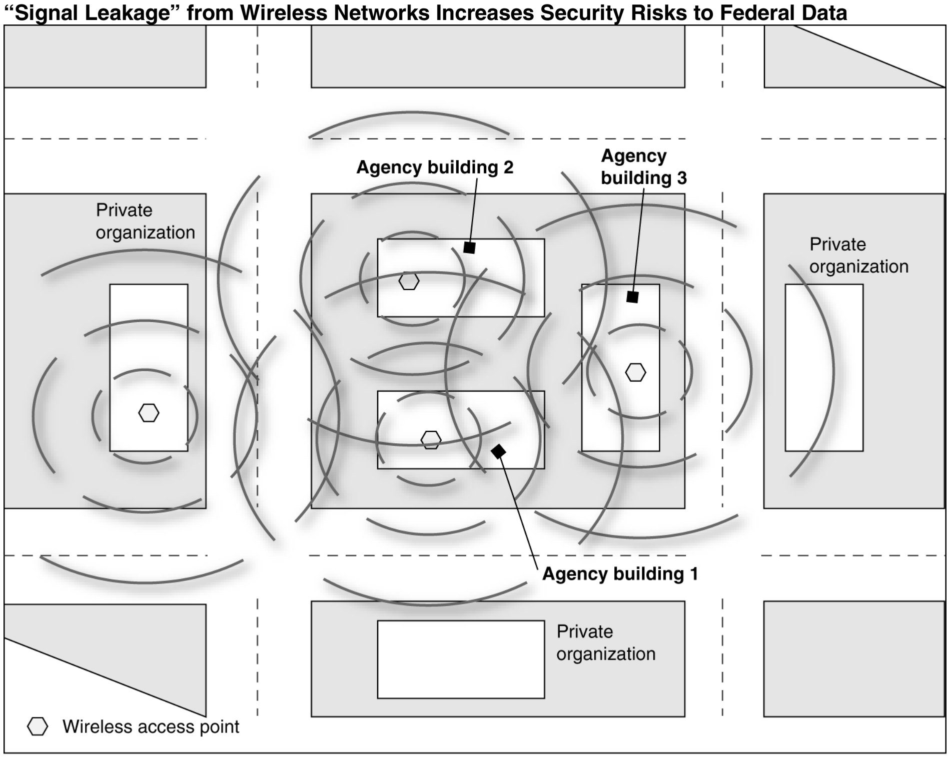
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Keith Rhodes at (202) 512-6412 or rhodesk@gao.gov

What GAO Found

Wireless networks offer a wide range of benefits to federal agencies, including increased flexibility and ease of network installation. They also present significant security challenges, including protecting against attacks to wireless networks, establishing physical control over wireless-enabled devices, and preventing unauthorized deployments of wireless networks. To secure wireless devices and networks and protect federal information and information systems, it is crucial for agencies to implement controls—such as developing wireless security policies, configuring their security tools to meet policy requirements, monitoring their wireless networks, and training their staffs in wireless security.

However, federal agencies have not fully implemented key controls such as policies, practices, and tools that would enable them to operate wireless networks securely. Further, our tests of the security of wireless networks at six federal agencies revealed unauthorized wireless activity and "signal leakage"—wireless signals broadcasting beyond the perimeter of the building and thereby increasing the networks' susceptibility to attack (see figure). Without implementing key controls, agencies cannot adequately secure federal wireless networks and, as a result, their information may be at increased risk of unauthorized disclosure, modification, or destruction.

"Signal Leakage" from Wireless Networks Increases Security Risks to Federal Data



Source: GAO.