United States Government Accountability Office

GAO

Report to Congressional Committees

November 2010

INFORMATION SECURITY

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

GAO

Accountability * Integrity * Reliability

GAO
Accountability • Integrity • Reliability
Highlights

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

November 2010

INFORMATION SECURITY

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

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.

Contents

Tables

Figures

Abbreviations

DISA	Defense Information Systems Agency
DHS	Department of Homeland Security
EAP	extensible authentication protocol
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
IPv6	Internet protocol version 6
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PDA	personal digital assistant
SP	Special Publications
VPN	virtual private network
WEP	wired equivalent privacy
WiMAX	Worldwide Interoperability for Microwave Access
WPA	Wi-Fi Protected Access
WLAN	wireless local area network

G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 30, 2010

The Honorable Richard J. Durbin
Chairman
The Honorable Susan Collins
Ranking Member
Subcommittee on Financial Services
and General Government
Committee on Appropriations
United States Senate

The Honorable José E. Serrano
Chairman
The Honorable Jo Ann Emerson
Ranking Member
Subcommittee on Financial Services
and General Government
Committee on Appropriations
House of Representatives

In the last several years, federal agencies have increasingly adopted the use of wireless technologies. While wireless technologies provide many potential benefits, including greater flexibility for a mobile workforce and ease of installation and use, they also pose significant risks to information and systems. Wireless technologies use radio waves instead of direct physical connections to transmit data between networks and devices. As a result, without proper security precautions, these data can be more easily intercepted and altered than if being transmitted through physical connections.

We have previously reported on the security of wireless networks at federal agencies in 2005.[1] The conference report accompanying the Financial Services and General Government Appropriations Act, 2010, directed us to update our 2005 report.[2] Accordingly, our objectives for this report were to: (1) identify leading practices and state-of-the-art

[1] GAO, *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks*, GAO-05-383 (Washington, D.C.: May 17, 2005).

[2] H.R. Conf. Rep. No. 111-366, at 914 (2009). We briefed the committees on the preliminary results of our review on April 13, 2010.

technologies for deploying and monitoring secure wireless networks and (2) assess agency efforts to secure wireless networks, including their vulnerability to attack.

To identify leading practices and state-of-the-art technologies for deploying and monitoring secure wireless networks, we obtained and reviewed publications, guidance, and other documentation, and interviewed private and federal subject matter experts. To assess agency efforts to secure wireless networks, we reviewed agency documents and conducted structured interviews with agency officials to learn about the wireless posture at 24 major federal agencies.[3] We supplemented these questions with site visits and detailed testing of wireless security controls at five of the agencies.

We conducted this performance audit from January 2010 to November 2010, 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 based on our audit objectives. Appendix I contains additional details on the objectives, scope, and methodology of our review.

Background

The advantages of wireless technology for federal agencies include increased flexibility, easier installation, and easier scalability than wired technologies. If a federal agency has installed a wireless infrastructure, users with wireless-enabled devices can more easily connect to the agency's network throughout its facilities. In addition, agency employees traveling with wireless-enabled devices may be able to connect to an agency network via any one of the many public Internet access points or hot spots. Installation can be easier and less costly because the network can be established without having to pull cables through walls or ceilings or modify the physical network infrastructure. Wireless networks can also

[3] The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

be easily scaled from small peer-to-peer networks to very large enterprise networks. For example, an agency can greatly expand the size of its wireless network and the number of users it can serve by increasing the number of access points. The following wireless technologies are commonly used by federal agencies:

- *wireless local area network (WLAN)*—a group of wireless networking nodes within a limited geographic area that serve as an extension to existing wired local area networks;
- *wireless personal area network*—used to establish small-scale wireless networks such as those using Bluetooth®, which is an open standard for short-range communication; and
- *wireless cellular networks*—a telecommunications network managed by a service provider that supports smartphones, which offer the ability to provide data such as e-mail and Web browsing wirelessly over cellular networks, and cellular data cards, which provide Internet connectivity to laptop computers.

Wireless Local Area Networks

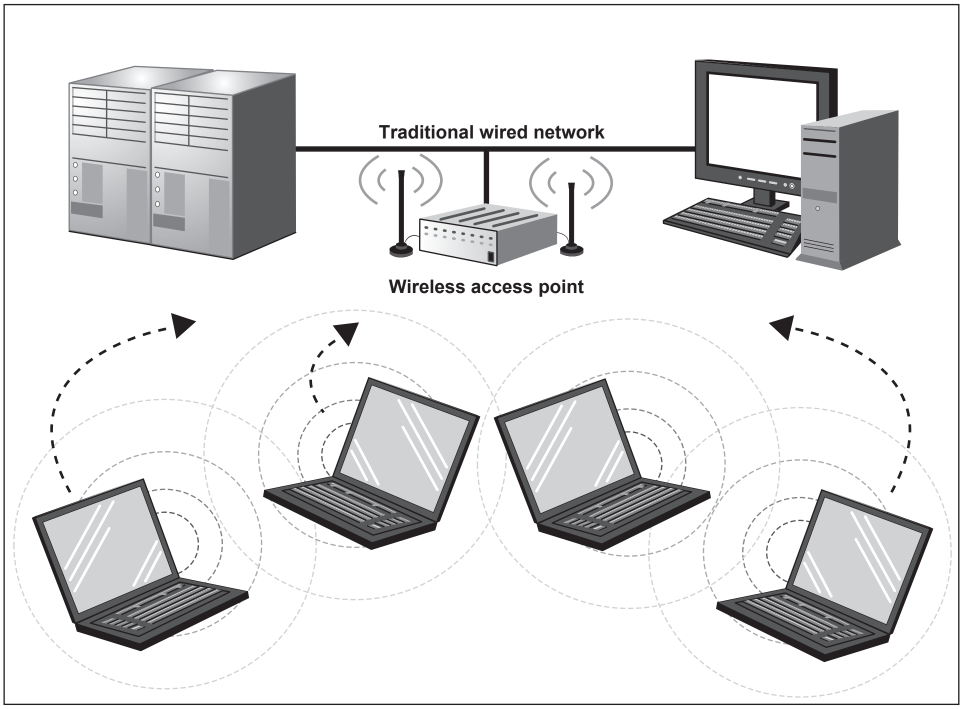
WLANs are generally composed of two basic elements: access points and other wireless-enabled client devices, such as laptop computers. These elements rely on radio transmitters and receivers to communicate with each other. Access points are physically wired to a conventional network and provide a means for wireless devices to connect to them. WLANs that are based on the Institute of Electrical and Electronics Engineers[4] (IEEE) 802.11 standards are also known as Wi-Fi.

WLANs are characterized by one of the following two basic structures, referred to as infrastructure mode and ad hoc mode:

- *Infrastructure mode.* By deploying one or more access points that broadcast overlapping signals, an organization can achieve broad wireless network coverage. Infrastructure mode enables a laptop or other mobile device to be moved about freely while maintaining access to the resources of the wired network (see fig. 1).

[4] IEEE is a professional association focused on electrical and computer sciences, engineering, and related disciplines. IEEE is responsible for developing technical standards through the IEEE Standards Association, which follows consensus-based standards development processes.

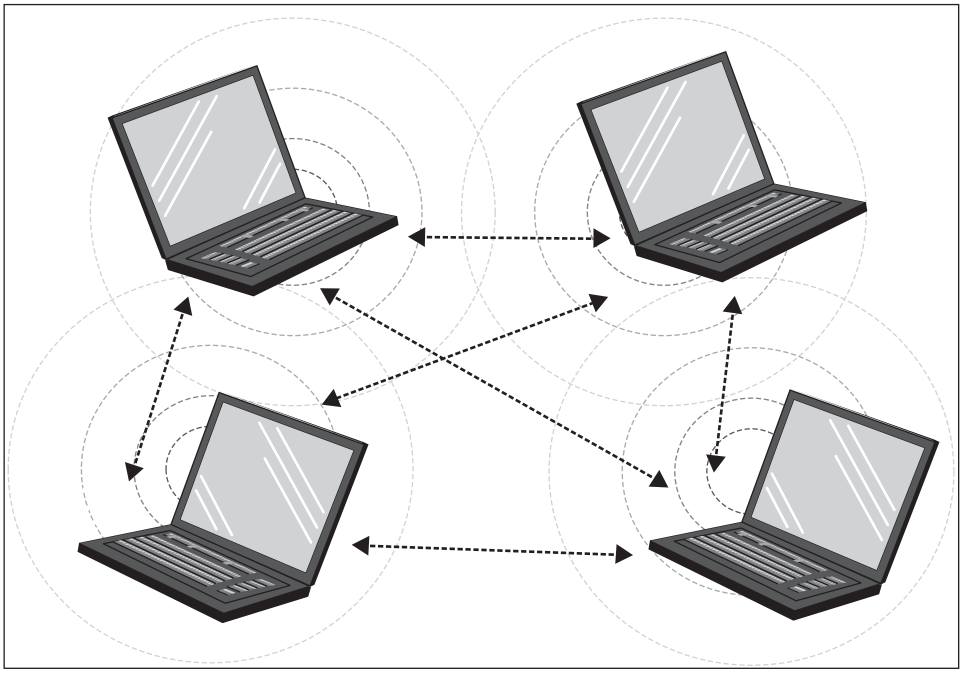
Figure 1: Example of a Wireless Infrastructure Mode Network



Sources: GAO; Microsoft Visio and Art Explosion (images).

- *Ad hoc mode.* This type of wireless structure allows wireless devices that are near one another to easily interconnect. In ad hoc mode, wireless-enabled devices can share network functionality without the use of an access point or a wired network connection (see fig. 2).

Figure 2: Example of Wireless Ad Hoc Networking



Sources: GAO; Microsoft Visio and Art Explosion (images).

After approval of the initial IEEE 802.11 standard in 1997, IEEE released several 802.11 amendments to increase WLAN network speeds to be more comparable to that of wired networks. The 802.11 standard and these subsequent amendments include security features known collectively as wired equivalent privacy (WEP). However, configurations that use WEP have significant security flaws.

To address these flaws, IEEE released the 802.11i security standard in 2004, which specifies security components that work together with 802.11 transmission standards. The IEEE 802.11i security standard supports wireless connections that provide moderate to high levels of assurance against WLAN security threats through the use of different cryptographic techniques.

While IEEE was developing 802.11i, the Wi-Fi Alliance[5] developed the Wi-Fi Protected Access (WPA) security certification as an interim means to

[5] The Wi-Fi Alliance is a nonprofit international association that has the goal of certifying the interoperability of WLAN products based on IEEE 802.11 specifications.

improve security over WEP. The protocols used under the WPA certification address vulnerabilities of WEP, but the certification does not require support for strong encryption.

In conjunction with the ratification of the 802.11i security standard in 2004, the Wi-Fi Alliance introduced WPA2—the interoperability certification for 802.11i. The WPA2 certification extends the security capabilities offered by WPA to include all requirements of the 802.11i standard. Both WPA and WPA2 offer two modes of operation: Personal and Enterprise. WPA2-Personal protects unauthorized network access by using a preshared password as a key for network setup and access, while WPA2-Enterprise verifies network users through an authentication server. In most cases, WPA2-Enterprise is recommended to eliminate the continuous process of generating, deploying, and replacing outdated passwords. Although WPA2-Enterprise-certified products provide more security protections than WEP and WPA, recent reports revealed that wireless networks protected with WPA2-Enterprise encryption can also be susceptible to attacks.

Most recently, in 2009, IEEE ratified the 802.11w-2009 standard, which further increases the overall security of 802.11–based networks. Specifically, 802.11w-2009 provides improved protection for WLANs by defining additional encryption security features to help prevent incidents such as denial of service attacks against WLANs.

Wireless Personal Area Networks

Wireless personal area networks provide wireless connectivity to devices such as telephone headsets or computer keyboards within close proximity. Bluetooth is commonly used to establish these types of networks. Several versions of the Bluetooth standard have been adopted by the Bluetooth Special Interest Group.[6]

Each Bluetooth device must operate in one of the four security modes defined by the Bluetooth standard. Each version of Bluetooth supports some, but not all, of these modes.

[6] The Bluetooth Special Interest Group is a not-for-profit trade association developed to serve as the governing body for Bluetooth specifications.

Wireless Cellular Networks

Cellular networks are managed by service providers who provide coverage based on dividing a large geographical service area into smaller areas of coverage called cells. As a mobile phone moves from one cell to another, a cellular arrangement requires active connections to be monitored and effectively passed along between cells to maintain the connection.

In addition to cellular phones, cellular networks support smartphones and cellular data cards. Smartphones offer more functionality than basic cellular phones, including e-mail and other office productivity applications and have extended expansion capabilities through peripheral card slots and other built-in wireless communications such as Bluetooth and Wi-Fi. Cellular data cards allow laptop users to connect to the Internet anywhere cellular service is available. However, cellular data cards can only access the Internet if the user is within the service provider's network coverage area.

Federal Agencies Make Widespread Use of Wireless Technologies

Agencies reported significant use of WLANs to extend working mobility for employees and contractors. For example, 18 agencies reported using WLANs in a variety of ways. Five agencies reported having wireless networks available for headquarters along with field offices or components. Twelve other agencies reported that components have different wireless practices than headquarters. For example, one major agency reported no WLANs at its headquarters, but it has components that use them. Further, several agencies use wireless networks for more limited purposes than connecting to the core agency network. Specifically, five agencies reported offering WLANs that connect directly to the Internet for use in conference rooms or other public spaces. Another agency reported using wireless access points to provide Internet connectivity at outdoor construction sites.

Personal area networks using Bluetooth technology were also reported by many agencies. Specifically, 14 agencies reported using Bluetooth devices. Ten agencies reported permitting cellular phone users to connect wireless headsets, and four agencies reported permitting wireless keyboards or mice.

Agencies also reported extensive use of smartphones and cellular data cards. All 24 agencies we queried reported using smartphones, primarily the BlackBerry® brand. Agencies' smartphone management structures included: management through a central server located at the department level or at the component level and one component or office providing smartphone management to another office. Seventeen agencies reported using cellular data cards to provide Internet connectivity to user laptops.

These cards and services are typically provided by commercial telecommunications carriers.

Wireless Technologies Are Susceptible to Security Risks

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The risk to these systems is well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. Table 1 provides a compilation of threats to wireless and wired networks as identified by the National Institute of Standards and Technology (NIST).

Table 1: Examples of Network Security Threats

Denial-of-service	Preventing or limiting the normal use or management of networks or network devices.
Eavesdropping	Passively monitoring network communications for data, including authentication credentials.
Man-in-the-middle	Actively impersonating multiple legitimate parties, such as appearing as a client to an access point and appearing as an access point to a client. Allows attacker to intercept communications between an access point and a client, thereby obtaining authentication credentials and data.
Masquerading	Impersonating an authorized user and gaining unauthorized privileges.
Message modification	Altering a legitimate message by deleting, adding to, changing, or reordering it.
Message replay	Passively monitoring transmissions and retransmitting messages, acting as if the attacker were a legitimate user.
Misappropriation	Stealing or making unauthorized use of a service.
Traffic analysis	Passively monitoring transmissions to identify communication patterns and participants.

Source: GAO analysis of NIST data.

Wireless networks also face challenges that are unique to their environment. A significant difference between wireless and wired networks is the relative ease of intercepting WLAN transmissions. For WLANs, attackers only need to be in range of wireless transmissions and do not have to gain physical access to the network or remotely compromise systems on the network. WLANs also have to protect against the deployment of unauthorized wireless devices, such as access points, that are configured to appear as part of an agency's wireless network infrastructure. In implementing wireless networks, federal agencies need to address these challenges to maintain the confidentiality, integrity, and availability of the information.

Bluetooth-enabled devices are susceptible to general networking threats and are also threatened by more specific Bluetooth-related attacks such as bluesnarfing, which enables attackers to gain access to a Bluetooth-enabled device by exploiting a software flaw in older devices.

Smartphones are also susceptible to general networking threats and face additional security risks. Those risks include those caused by their size and portability, as well as the availability of different wireless interfaces and associated services. For example, the size and portability of smartphones can result in the loss of physical control of a device that could reveal sensitive data to an unauthorized user.

Recent articles released by the media reinforce the need for federal agencies to secure their wireless networks and devices. Examples of reported incidents and risks include the following:

- A retail company admitted in 2007 that hackers located and tested wireless networks for vulnerabilities and installed programs on these networks to steal the credit card information of more than 45 million consumers.

- An assessment of wireless vulnerability conducted in 2008 at 27 airports that had wireless networks found that personal information could be leaked because only 3 percent of hot spot users used a virtual private network (VPN)[7] to encrypt their data.

- In 2009, a counterintelligence official described how smartphones could have been tagged, tracked, monitored, and exploited at the 2008 Beijing Olympics. The malicious software could have also posed a threat to e-mail servers in the United States.

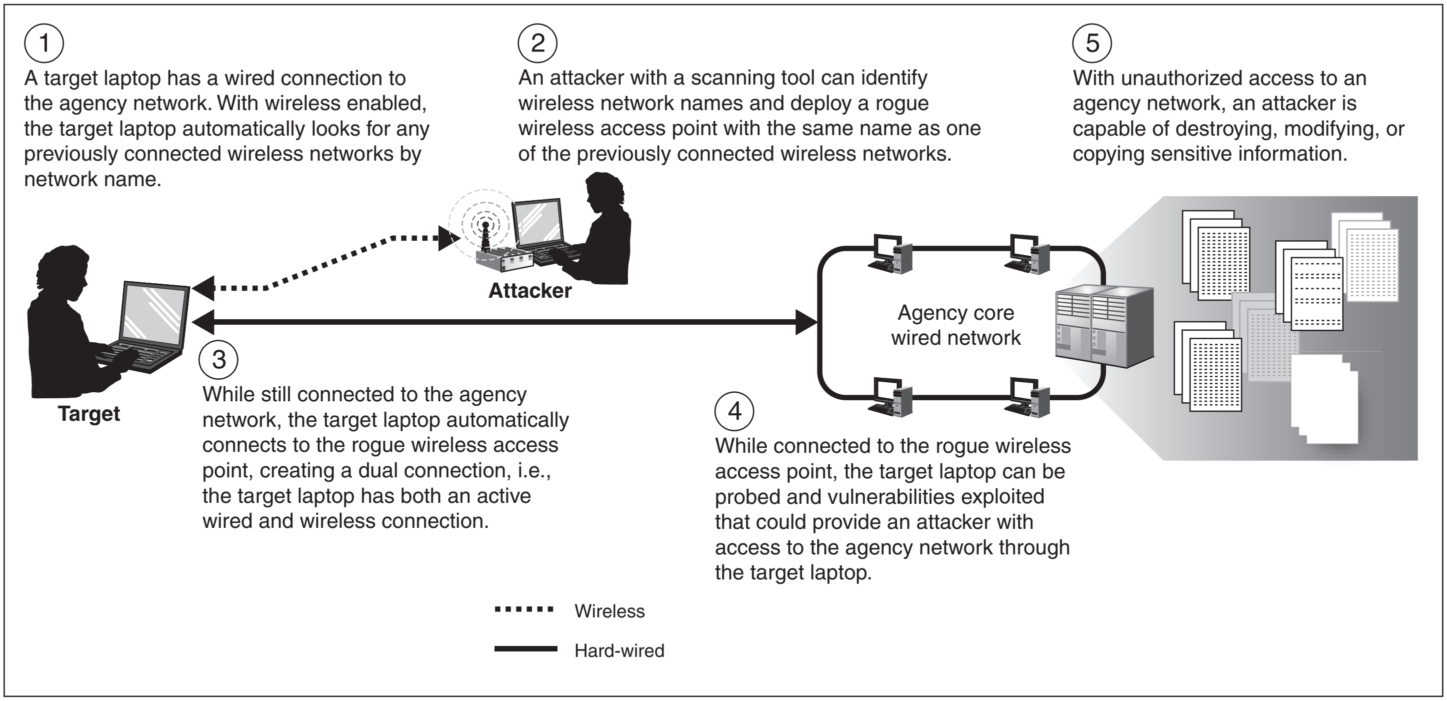
[7] A VPN is a private network that is maintained across a shared or public network, such as the Internet, by means of specialized security procedures. VPNs are intended to provide secure connections between remote clients, such as branch offices or traveling personnel and a central office.

Scenarios Provide Examples of Attacks Using Wireless Vulnerabilities

The following scenarios (figs. 3-5) provide examples of well-known attacks used to exploit vulnerabilities in wireless technologies. These scenarios do not represent all possible attacks on wireless technology vulnerabilities.

In a dual-connect scenario (see fig. 3), the attacker exploits insecure laptop configurations to gain unauthorized access to an organization’s core network.

Figure 3: Dual-Connect Attack Scenario



1 A target laptop has a wired connection to the agency network. With wireless enabled, the target laptop automatically looks for any previously connected wireless networks by network name.

2 An attacker with a scanning tool can identify wireless network names and deploy a rogue wireless access point with the same name as one of the previously connected wireless networks.

3 While still connected to the agency network, the target laptop automatically connects to the rogue wireless access point, creating a dual connection, i.e., the target laptop has both an active wired and wireless connection.

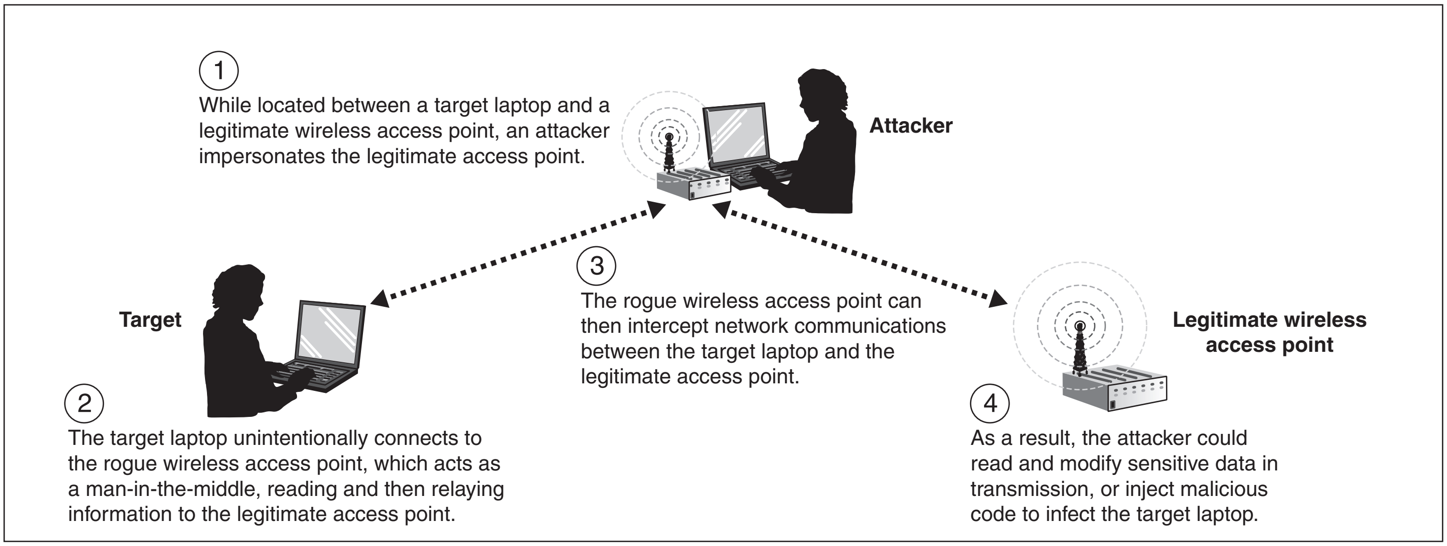
4 While connected to the rogue wireless access point, the target laptop can be probed and vulnerabilities exploited that could provide an attacker with access to the agency network through the target laptop.

5 With unauthorized access to an agency network, an attacker is capable of destroying, modifying, or copying sensitive information.

Source: GAO; Art Explosion (images).

Wireless man-in-the-middle attacks (see fig. 4) use an insecure laptop configuration to intercept or alter information transmitted wirelessly between the target laptop and a wireless access point.

Figure 4: Wireless Man-in-the-Middle Attack Scenario



1 While located between a target laptop and a legitimate wireless access point, an attacker impersonates the legitimate access point.

2 The target laptop unintentionally connects to the rogue wireless access point, which acts as a man-in-the-middle, reading and then relaying information to the legitimate access point.

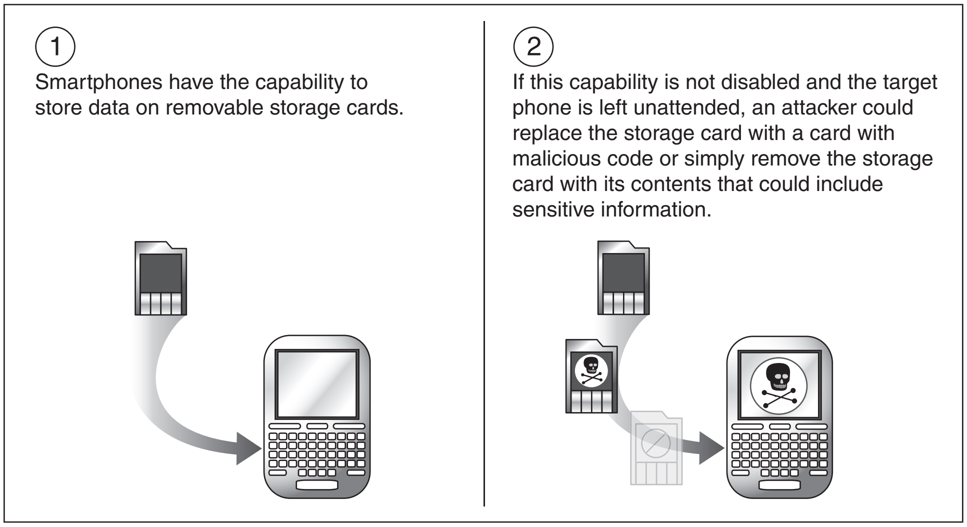
3 The rogue wireless access point can then intercept network communications between the target laptop and the legitimate access point.

4 As a result, the attacker could read and modify sensitive data in transmission, or inject malicious code to infect the target laptop.

Source: GAO; Art Explosion (images).

Attacks on smartphones (see fig. 5) can involve stealing data or injecting malicious code using phone storage cards.

Figure 5: Smartphone Data Attack Scenario



1 Smartphones have the capability to store data on removable storage cards.

2 If this capability is not disabled and the target phone is left unattended, an attacker could replace the storage card with a card with malicious code or simply remove the storage card with its contents that could include sensitive information.

Source: GAO.

Federal Laws and Guidelines Provide a Framework for Wireless Security Policies

The Federal Information Security Management Act (FISMA) of 2002 requires each agency to develop, document, and implement an agencywide information security program to provide security for the data and information systems that support the agency's operations and assets.[8] Significant amounts of agency data are stored on and transmitted through wireless devices and networks. Wireless technologies are often important parts of the information systems that support the agency's operations and assets. Accordingly, wireless technologies are typically encompassed by agency information security programs required under FISMA. FISMA also assigns additional information security responsibilities for the Office of Management and Budget (OMB) and NIST.

FISMA assigns OMB specific responsibilities, including

- overseeing the implementation of policies, standards, and guidelines on information security, including ensuring timely agency adoption of and compliance with standards;
- requiring agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, or information systems used or operated by or on behalf of an agency;
- overseeing agency compliance with FISMA requirements;
- reviewing at least annually, and approving or disapproving, agency information security programs; and
- annual reporting to Congress on agency compliance with the requirements of FISMA, including significant deficiencies in agency information security practices and planned remedial action to address such deficiencies.

In a July 2010 memo, OMB directed the Department of Homeland Security (DHS) to exercise primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to the federal information systems that fall within FISMA.[9] According to the

[8] 44 U.S.C. § 3544(b).

[9] OMB, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (Washington, D.C: July 6, 2010).

memo, DHS is to oversee the implementation of and reporting on information security policies and guidance in federal agencies, oversee agency compliance with FISMA, and annually review agency cybersecurity programs. OMB will continue to report annually to Congress on the progress of agencies' compliance with FISMA.

According to the Director of Federal Network Security—the DHS official responsible for many of DHS's newly assigned FISMA-related activities—DHS is beginning its oversight activities through the annual FISMA reporting process that federal agencies are required to follow. The official stated that the department does not currently have any wireless-security-specific activities under way, but that the department is planning future activities that may address wireless security, including compliance audits and an architecture document.

Under FISMA, NIST is responsible for developing standards and guidelines that include minimum information security requirements. Table 2 describes NIST Special Publications (SP) that include guidelines intended to secure wireless technologies.

Table 2: Wireless Security Guidelines Identified in NIST Guidelines

NIST SP	Purpose
800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*[a]	Provides guidelines to organizations in securing their legacy IEEE 802.11 WLAN that cannot use the IEEE 802.11i standard.
800-53, *Recommended Security Controls for Federal Information Systems and Organizations*[b]	Provides guidelines for selecting and specifying security controls for information systems that include wireless access and access controls for mobile devices.
800-94, *Guide to Intrusion Detection and Prevention Systems*[c]	Provides a basis for designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention systems including a wireless intrusion detection system.[d]
800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*[e]	Assists organizations in understanding, selecting, and implementing technologies based on IEEE 802.11i.
800-101*, Guidelines on Cell Phone Forensics*[f]	Provides basic information on the preservation, acquisition, examination, analysis, and reporting of digital evidence on cell phones, relevant to law enforcement, incident response, and other types of investigations.
800-114, *User's Guide to Securing External Devices for Telework and Remote Access*[g]	Provides guidelines for securing external devices used for telework including wireless home networks and wireless-enabled personal computers.

NIST SP	Purpose
800-120, *Recommendation for EAP Methods Used in Wireless Network Access Authentication*[h]	Formalizes a set of core security requirements for extensible authentication protocol (EAP)[i] for wireless access authentication and key establishment.
800-121, *Guide to Bluetooth Security*[j]	Provides information on the security capabilities of Bluetooth and provides recommendations to secure Bluetooth devices effectively.
800-124, *Guidelines on Cell Phone and PDA Security*[k]	Provides an overview of cell phone and personal digital assistant (PDA) devices in use today and provides safeguards for securing these devices.

Source: GAO analysis of NIST data.

[a] NIST, *Guide to Securing Legacy IEEE 802.11 Wireless Networks,* SP 800-48 Revision 1 (Gaithersburg, MD: July 2008).

[b] NIST, *Recommended Security Controls for Federal Information Systems and Organizations,* SP 800-53 Revision 3 (Gaithersburg, MD: August 2009).

[c] NIST, *Guide to Intrusion Detection and Prevention Systems (IDPS),* SP 800-94 (Gaithersburg, MD: February 2007).

[d] An intrusion detection system monitors the events occurring in a computer system or network and analyzes them for signs of possible incidents.

[e] NIST, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,* SP 800-97 (Gaithersburg, MD: February 2007).

[f] NIST, *Guidelines on Cell Phone Forensics,* SP 800-101 (Gaithersburg, MD: May 2007).

[g] NIST, *User's Guide to Securing External Devices for Telework and Remote Access,* SP 800-114 (Gaithersburg, MD: November 2007).

[h] NIST, *Recommendation for EAP Methods Used in Wireless Network Access Authentication,* SP 800-120 (Gaithersburg, MD: September 2009).

[i] EAP supports multiple authentication methods used when connecting a computer to the Internet.

[j] NIST, *Guide to Bluetooth Security,* SP 800-121 (Gaithersburg, MD: September 2008).

[k] NIST, *Guidelines on Cell Phone and PDA Security,* SP 800-124 (Gaithersburg, MD: October 2008).

NIST is also responsible for administering the United States Configuration Baseline, which is an initiative to create security configuration baselines for information technology (IT) products deployed across federal agencies.

In addition to NIST guidelines, other federal agencies have developed guidance for securing wireless technologies. For example, the Department of Defense's Defense Information Systems Agency (DISA) has created a series of security technical implementation guides that address general purpose or multiuse technologies. These guides serve as configuration standards for the Department of Defense's wireless devices and systems. In addition, DISA has made these guides available for other federal agencies to provide them with a baseline level of security.

GAO Has Previously Recommended Improvements to Wireless Network Security Guidance

In 2005, we reported that federal agencies lacked key controls for securing wireless networks.[10] We recommended that the Director of OMB instruct federal agencies to ensure that wireless network security is incorporated into their agencywide information security programs, in accordance with FISMA. Specifically, we recommended that agencywide security programs should include the following security controls.

- Robust policies for authorizing the use of the wireless networks, identifying requirements, and establishing security controls for wireless-enabled devices in accordance with NIST guidelines.
- Security configuration requirements for wireless devices that include
  - security tools, such as encryption, authentication, VPN, and firewalls;
  - placement and strength of wireless access points to minimize signal leakage; and
  - physical protection of wireless-enabled devices.
- Comprehensive monitoring programs, including the use of tools such as site surveys and intrusion detection systems to
  - detect signal leakage;
  - ensure compliance with configuration requirements;
  - ensure only authorized access and use of wireless networks; and
  - identify unauthorized wireless-enabled devices and activities in the agency's facilities.
- Wireless security training for employees and contractors.

In response to our recommendations, OMB has instructed federal agencies to ensure network security is incorporated into their agencywide network security program through the use of NIST guidelines. In addition, OMB's annual FISMA reporting requirements state that agencies must follow NIST standards and guidelines for non-national security programs and information systems. Since our report was issued, NIST has released

[10] GAO-05-383.

guidelines that address the items identified in our recommendations. These guidelines include NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*; NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; and NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* (see table 3).

Table 3: Guidelines in NIST Publications Addressing Recommendations from GAO-05-383

Recommendation	NIST SP 800-48	NIST SP 800-53	NIST SP 800-97	Area
Establish policies	X	X	X	Establishing wireless networking security policies, such as infrastructure and client device security; criteria for identifying and implementing security requirements; access controls for portable and mobile devices; and establishing and maintaining robust security for wireless local area networks.
Configuration requirements include security tools	X	X		Configuring wireless client device security tools and the use of security tools such as personal firewalls, host-based intrusion detection and prevention systems for the protection of wireless clients; the use of VPNs as an alternative method of achieving confidentiality and integrity protection; and security protocols.
Configuration requirements address access points	X			Establishing access point configuration and awareness of access point security concerns, including signal boundary considerations.
Configuration requirements include physical protection	X	X		Ensuring physical protection of wireless devices such as usage restrictions and implementation guidance for organization-controlled portable and mobile devices.
Monitoring programs include tools to detect signal leakage	X			Determining criteria for conducting site surveys and the use of appropriate wall-mounted antennas to minimize signal leakage.
Monitoring programs include tools to ensure configuration compliance	X	X		Using wireless intrusion detection and prevention systems to determine misconfigured clients and using policy driven software solutions to ensure client devices and users comply with defined WLAN policies.
Monitoring programs include tools to ensure access is authorized	X	X	X	Using wireless intrusion detection and prevention systems to determine whether unauthorized users or devices are attempting to access, have already accessed, or have compromised the WLAN; and performing regular audits using wireless sniffers and other tools to determine whether wireless products are transmitting correctly and on the correct channels.
Monitoring programs include tools to identify unauthorized access	X	X	X	Using wireless intrusion detection and prevention systems to detect suspicious or unauthorized activity and completing site surveys to discover any sources of radio interference.
Security training	X	X	X	Establishing wireless security awareness and training for employees and contractors to ensure good security practices and prevent inadvertent or malicious intrusions into an organization's information systems.

Source: GAO analysis of NIST data.

Comprehensive Policies, Use of Secure Technologies, Risk-Based Approach, Training, and Monitoring Among Leading Practices for Deploying and Monitoring Secure Wireless Networks

Leading practices for deploying and monitoring secure wireless networks include comprehensive policies, configuration controls, training, and other practices as described in table 4. Many of these practices are consistent with the key information security controls required for an effective information security program identified in our previous reports and reflect wireless-specific aspects of those controls. Furthermore, experts identified several emerging technologies, such as broadband wireless, third-party device management, and IEEE 802.11n-2009/802.11w-2009, as potentially important in securing wireless networks in the future.

Table 4: Leading Practices for Securing Wireless Networks and Technologies

Practice category	Practice description
1. Policy	Develop comprehensive security policies that govern the implementation and use of wireless networks and mobile devices that include the following safeguards: • implement secure encryption with enterprise authentication, • establish usage restrictions and implementation guidance for wireless access, and • enforce access controls for connection of mobile devices.
2. Risk-based approach	Employ a risk-based approach for wireless deployment.
3. Centralized management	Employ a centralized wireless management structure that is integrated with the existing wired network.
4. Configuration requirements	Establish configuration requirements for wireless networks and devices in accordance with the developed security policies and requirements.
5. Training	Incorporate wireless and mobile device security component in training.
6. Remote access	Use a VPN to facilitate the secure transfer of sensitive data during remote access.
7. Monitoring	Deploy continuous monitoring procedures for detecting rogue access points and clients using a risk-based approach.
8. Security assessments	Perform regular security assessments to help ensure wireless networks are operating securely.

Source: GAO.

Develop Comprehensive Security Policies that Govern Implementation and Use of Wireless Networks and Mobile Devices

Comprehensive information security policies that address the security of wireless networks and mobile devices can help agencies mitigate risks. FISMA recognizes that the development of policies and procedures is essential to cost effectively reducing the risks associated with IT, including wireless IT, to an acceptable level. In addition, experts noted that sound policy is the basis for all effective security measures. Policies should cover areas such as roles and responsibilities, WLAN infrastructure security, WLAN client device security, and security assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of wireless networks.

In addition to these policies, federal guidelines and experts also emphasized key safeguards to address wireless security concerns that have surfaced since our 2005 report. These practices include prohibiting the use of WEP and implementing WPA2 with enterprise authentication, establishing usage restrictions and implementation guidance for wireless access, and implementing access controls for mobile devices that connect to an agency's wireless networks.

Implement Secure Encryption with Enterprise Authentication

Organizations should establish policies requiring procurement of wireless products that have been WPA2-Enterprise certified and Federal Information Processing Standards (FIPS)-validated.[11] NIST guidelines state, and experts agree, that only these devices are capable of fully implementing the IEEE 802.11i robust security network protections, which include enhanced user and message authentication mechanisms, cryptographic key management, and robust enciphering and data integrity mechanisms. Wireless technologies that rely on older wireless security protocols, such as WEP and WPA, can be more easily exploited to circumvent or adversely impact access control and authentication, confidentiality, integrity, and availability since they do not require strong encryption algorithms.

[11] See NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, MD: May 25, 2001). FIPS 140-2 specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. Agencies are required to encrypt agency data, where appropriate, using NIST-validated cryptographic modules as specified in FIPS 140-2.

Establish Usage Restrictions and Implementation Guidance for Wireless Access

Agencies should establish and enforce usage restrictions and implementation guidance for wireless access. According to NIST guidelines, security policies should identify which users are authorized to connect wirelessly to an organization's networks and the types of information allowed to be transmitted across wireless networks. In addition, wireless access to information systems should only be permitted by using authentication and encryption.

NIST guidelines also instruct agencies to identify the acceptable methods of remote access. Specifically, an agency's policies should describe which wireless-enabled devices can connect to the agency's networks remotely and the types of external networks permitted. For example, policies should specify if users connecting remotely through public hot spots to an agency's networks are authorized to use only agency-issued mobile devices.

Enforce Access Controls for Connection of Mobile Devices

Both NIST guidelines and experts identified establishing access controls for mobile devices, which includes those taken to locations the agency deems to be a significant risk, and prohibiting dual connection as a key practice for securely deploying and monitoring wireless networks. Our previous reports have also emphasized the importance of such access controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), in order to protect them from unauthorized use, modification, disclosure, and loss.

Specifically, NIST guidelines state that agencies need to establish and enforce usage restrictions and implementation guidance for agency-issued mobile devices taken to locations the agency deems to be a significant risk. For example, agencies may issue specially configured mobile devices to individuals before traveling to risky locations, such as certain countries, which are in accordance with agency policies and procedures. Upon return from travel, agency-defined inspection and preventative measures can be applied to the mobile device such as re-imaging the hard disk drive on laptops. According to one expert's account, by developing access control requirements for global use of devices (i.e., managing devices that travel internationally), organizations can avoid compromises of devices or information that have occurred at organizations without these practices.

Another component of establishing access controls for mobile devices that NIST and experts identified was restricting the access rights of devices (and individuals) to an organization's network. Enforcing requirements such as usage restrictions, configuration management, and device identification and authentication, and disabling unnecessary hardware can prevent incidents of employees inadvertently connecting their devices to malicious entities and compromising the confidentiality, integrity, and availability of the organization's network.

Employ a Risk-Based Approach for Wireless Deployment

Federal guidelines underscore, and experts agree with, the need for a risk-based approach for deploying wireless networks and technologies. A risk-based approach attempts to ensure that risks to the organization are identified and prioritized so that available resources can be most effectively used in defending against the most significant threats, such as unauthorized access points or devices on the network, and to prevent the incurrence of undue risk.

Federal guidelines and experts also agreed that risks should be considered prior to acquisition of wireless technologies in order to implement management controls early on, determine which WLAN activities pose an acceptable risk, and identify the potential impact of the threat to the organization. The Committee on National Security Systems,[12] in its recently issued *Policy on Wireless Communications: Protecting National Security Information*, recommended that agencies consider protecting against the risks that can occur during various points of data transmission such as at the point of origin, when received, and while stored on wireless media.[13] It is only after considering and then managing such risks that organizations can make informed decisions such as whether or not to deploy wireless networks and technologies or determine the types of devices and extent of their usage throughout the organization. Moreover, since risks change over time, as a general practice, it is essential to periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls organizations have selected to mitigate those risks.

[12] The Committee on National Security Systems consists of 21 members from federal agencies and is charged with establishing national policy and promulgating direction, operational procedures, and guidance for the security of national security systems.

[13] Committee on National Security Systems, *Policy on Wireless Communications: Protecting National Security Information*, CNSSP No.17 (Ft. Meade, MD: May 2010).

Employ a Centralized Wireless Management Structure That Is Integrated with the Existing Wired Network

Security experts agreed that a centralized wireless management structure that is integrated with the management of the existing wired network can provide a more effective means to manage the wireless infrastructure and the information security program as a whole. A centralized structure can provide a coherent, consistent approach to managing the entire wireless network. For example, configuration changes can be centrally monitored, and with centralized reporting, management can have improved visibility and oversight of the organization's entire wireless network. Using tools that allow centralized management of WLANs can provide a management focal point and reduce the number of attack points in the network.

A centralized structure can also facilitate the development and implementation of standardized guidance, which allows organizations to consistently apply information security policies. Organizations can authorize the use of specific products, coordinate the installation of WLANs, and issue other such directives to provide a holistic approach for deploying and monitoring wireless activities. Such implementation can be centralized at the enterprise or component level, based on the business needs of the organization.

In conjunction with a centralized management structure, experts agreed the importance of integrating wireless management with management of the wired network. By extending established information security controls, such as intrusion detection systems and monitoring, from the wired to the wireless network, an organization is better positioned to both understand and defend its overall information security posture.

Experts agreed that a decentralized wireless management structure can result in disparate, ad hoc networks that operate and are managed separately. The existence of multiple networks that are independently managed can impede effective implementation and monitoring of security controls and inhibit sufficient oversight of the wireless network.

Although centralized wireless management can have many benefits, the level of centralization needs to be determined by business need and a risk-based approach. Centralization can be performed by agency components or departmentwide and should be balanced against the costs of centralization.

Existing federal guidelines recognize the benefits that centralized management of network services and information security can provide for federal agencies. For example, NIST guidelines state that centralized security management is an important consideration for managing mobile devices since it facilitates the configuration control and management processes that support compliance with an organization's security policy. Additionally, we previously reported that establishing a central management focal point for information security is essential to spotting trends, identifying problem areas, and determining whether policies and administrative issues are handled in a consistent manner.[14]

Establish Configuration Requirements for Wireless Networks and Devices in Accordance with the Developed Security Policies and Requirements

Establishing configuration requirements for wireless networks and devices can help ensure they are deployed in a secure manner in accordance with agency policies. For example, NIST SP 800-48 states that agencies should configure their wireless networks in accordance with established security policies and requirements. Establishing settings or configuration requirements for wireless access points can guide their placement and signal strength to minimize signal leakage and exposure to attacks.

In addition to access points, client devices should also be configured to enhance the wireless network security posture. According to NIST, securing the infrastructure without properly securing the client devices renders the entire wireless network insecure. Solutions such as enterprise servers can periodically communicate with managed mobile devices to ensure security and other configuration settings are correct and in compliance with policy.

Incorporate Wireless and Mobile Device Security Component in Training

NIST guidelines and experts stated that training employees and contractors in an organization's wireless policies is a fundamental part of ensuring that wireless networks are configured, operated, and used in a secure and appropriate manner. For security policies to be effective, those expected to comply with them must be aware of the policies. Additionally, FISMA mandates that agencies provide security awareness training for their personnel, including contractors and other users of information systems that support the operations and assets of the agency. NIST recommends that the security awareness training include the risks of wireless security and how to protect against those risks. In addition, NIST guidelines and experts agree that an agency's security training should include mobile device security that addresses (1) maintaining physical control over mobile devices, (2) protecting sensitive data on mobile

[14] See, for example, GAO, *Executive Guide: Information Security Management, Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

devices with encryption, (3) disabling wireless interfaces on mobile devices when not needed, and (4) the procedures for reporting lost or stolen mobile devices. FISMA also requires agency chief information officers to ensure that personnel with significant information security responsibilities receive training with respect to their responsibilities.

Use a VPN to Facilitate the Secure Transfer of Data during Remote Access

A VPN can provide a secure communications mechanism for sensitive data transferred across multiple, public networks. For wireless technologies, VPNs are useful because they provide a way to secure WLANs that may be insecure, such as those at public hot spots, in homes, or other locations. According to NIST guidelines, federal agencies should consider using VPNs to protect the confidentiality of WLAN communications during remote access and telework and should configure the VPNs to use FIPS-140-2-validated encryption. Experts agreed on the use of VPNs as an integral security measure for an increasingly mobile workforce.

Deploy Continuous Monitoring Procedures for Detecting Rogue Access Points and Clients Using a Risk-Based Approach

Continuous monitoring is a means for an organization to ensure that security controls remain effective despite the planned and unplanned changes that can occur to an information system. OMB policy and NIST guidelines require agencies to implement a continuous monitoring approach for all information systems, including those using wireless technologies. According to NIST guidelines, agencies are required to monitor for unauthorized wireless access to information systems and should base their determination of the scope and frequency of such monitoring on an assessment of risk to the agency, the operational environment, the agency’s requirements, and specific threat information. Continuous monitoring allows an organization to defend its security posture in a dynamic environment where threats, vulnerabilities, and technologies are constantly changing. Experts also noted the importance of continuously monitoring the wireless network for rogue access points and client devices. Documenting and implementing an approach to wireless monitoring that uses a risk-based approach helps to ensure that the scope and frequency of monitoring is appropriate for the threats facing the agency. As previously mentioned, centralized management tools can provide continuous monitoring capabilities for improved visibility and oversight of the organization’s entire wireless network.

Both experts and NIST guidelines highlighted the importance of using a wireless intrusion detection system to continuously monitor an agency’s wireless networks to detect and respond to malicious activities on the network before they inflict damage. These types of systems enable an organization's operations or security staff to determine whether unauthorized users or devices are attempting to access, have already accessed, or have compromised a WLAN. A wireless intrusion prevention system builds on the functionality of a wireless intrusion detection system by also automatically taking countermeasures against these unauthorized users or devices. These systems are able to monitor wireless data as it passes from wireless to wired networks. They can also detect misconfigured WLAN clients, rogue access points, ad hoc networks, and other possible violations of an organization's WLAN policy. In addition, these systems can position an organization to proactively assess its wireless network at regular intervals. However, a wireless intrusion detection or prevention system is a significant expense, and it may not be appropriate in all cases. For example, an agency may determine that a smaller agency location with lower risk systems may not warrant the expense that installing a wireless intrusion detection or prevention system may entail.

Other tools exist to detect rogue wireless client devices, such as handheld scanners and network authentication mechanisms, but these may not be as effective or easy to monitor as an intrusion detection system. Consistent with NIST guidelines, an organization should use a risk-based business case to determine the appropriate use of continuous monitoring solutions.

Perform Regular Security Assessments to Help Ensure Wireless Networks are Operating Securely

Experts and NIST guidelines both noted the importance of regular security assessments for checking the security posture of wireless networks and for determining corrective actions needed to ensure the wireless networks remain secure. Regular assessments help to determine whether wireless devices are transmitting correctly and are on the correct channels. Experts noted the importance of consistently and regularly performing security assessments in tandem with continuously monitoring the wireless network. In addition, organizations should maintain an inventory of access points deployed and their mobile devices to help identify rogue devices when conducting assessments. Assessments can help organizations to determine whether controls are appropriately designed and operating effectively to achieve the organization's control objectives.

Broadband Wireless, Device Management, and Newer WLAN Technologies Are Emerging Wireless Technologies

Several current and emerging technologies are important to consider for secure deployment of wireless technologies as follows:

- *Long-Term Evolution*—Long-Term Evolution is a fourth-generation wireless broadband technology that experts stated is expected to improve the speed and quality of service and provide scalable bandwidth capacity. It is also expected to improve security through enhanced encryption to prevent eavesdropping and user identity confidentiality to prevent tracking of specific users. One expert noted that most of the public safety broadband environments used for emergency communications at the state and local levels will adopt Long-Term Evolution and highlighted the importance of its effective implementation by government entities.

- *WiMAX*—Another form of broadband wireless technology known as WiMAX (Worldwide Interoperability for Microwave Access) is intended for wireless metropolitan area networking and is an effort to provide seamless mobile access in much the same way as wide-area cellular networks with higher transmission speeds. Security advantages of WiMAX include mutual device/user authentication, improved traffic encryption, and options for securing data within the core network.

- *Third-party device management*—The technological capabilities of a third-party vendor may provide a means for organizations to establish security for mobile devices. According to experts, a vendor that specializes in wireless security may be more up-to-date on security vulnerabilities and better equipped to assess the security of wireless networks than an agency's own staff. Capabilities provided by a vendor can include incident management, triggers if a device is taken overseas, remote trouble shooting, and usage trends, among others.

- *IEEE 802.11n-2009/802.11w-2009 technologies*—Two additions to the 802.11 family of WLAN technologies–802.11n-2009 and 802.11w-2009–are expected to improve the performance and security of WLANs. The technologies specified in 802.11n-2009 increase WLAN speed, improve reliability, and extend the range of wireless transmissions. The 802.11w-2009 encryption standard builds on the 802.11i framework to protect against certain types of attacks on WLANs.

Agencies Have Acted to Secure Wireless Networks, but Additional Steps Are Needed to Effectively Mitigate Security Challenges

Agencies have taken several steps to address the security of their wireless networks; however, these steps have not been fully and comprehensively applied across the government. Specifically, application was inconsistent among the agencies for most of the following leading practices:

- Most agencies developed policies that reflected NIST guidelines and leading practices, but gaps existed in these policies, particularly with respect to dual-connected laptops and use of mobile devices 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 potential standardization that centralized management can provide, and guidance on centralization is limited.
- The five agencies where we did detailed testing generally securely configured wireless access points, but they had numerous weaknesses in laptop and smartphone configurations. Gaps in governmentwide guidance on configuration contributed to these weaknesses.
- 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 VPN must be used during remote access; four agencies did not require encryption.
- Many agencies had insufficient practices for monitoring or conducting security assessments. Furthermore, federal guidance in this area lacks specificity.

Existing governmentwide guidance and oversight efforts do not fully address agency implementation of the leading practices. Until agencies fully address these practices, they will not have sufficient assurance that the risks to sensitive wireless systems, and sensitive data transmitted across or processed by those systems, are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. Also, until OMB and DHS ensure they have effective means for oversight of federal agencies' efforts to secure wireless networks they may lack full visibility of the vulnerability of these networks to attack.

Agencies Have Developed Policies to Support Secure Use of Wireless Technologies, but Gaps Exist

Almost all agencies required wireless networks to employ encryption, but not all agencies required secure forms of encryption. Specifically, 23 of 24 agencies specified in their policies that agency wireless networks are required to employ encryption. However, 7 of the 23 agencies did not require secure forms of encryption. Specifically, 2 agencies' policies required the use of WEP, an older wireless encryption method that is vulnerable to attack; one agency required the use of WPA, which is not compliant with federal requirements for encryption; and 4 other agencies did not specify any type of encryption or require the use of FIPS 140-2 compliant encryption. In addition, 1 agency did not have any documented requirements for wireless transmissions to be encrypted, even though that agency has a wireless network deployed at its headquarters.

In certain cases, agency policies had been developed several years ago. Agencies had also not always updated their policies to reflect their implementations of WLANs or federal requirements for wireless encryption. Agencies that do not require the use of strong, FIPS-validated encryption algorithms on their wireless networks have limited assurance that sensitive agency information is being adequately protected from unauthorized disclosure or modification.

Most Agencies Have Established Usage Restrictions and Implementation Guidance for Wireless Networks

Twenty-three of the 24 agencies provided specific guidance to agency personnel on the types of information that may be transmitted using wireless networks or on how sensitive information is to be protected when transmitted wirelessly. All 24 of the agencies in our review had also developed policies establishing usage restrictions and implementation guidance for wireless networks; although policies for 3 agencies were in draft and had not yet been approved.

Examples of usage restrictions in agency policies included the following:

- requiring that administration of wireless infrastructure devices (such as access points) be conducted using the wired network,
- prohibiting the use of ad hoc wireless networks, and
- allowing access to agency wireless networks only via a VPN.

Agencies' policies frequently contained wireless implementation guidance such as the following:

- physically securing wireless infrastructure devices,

- adjusting the transmission power of access points to ensure adequate coverage while minimizing signal leakage,
- maintaining audit logs on wireless access points,
- changing default service set identifiers[15] and not using identifiers that would identify the agency,
- enabling media access control[16] address filtering, and
- segregating wireless network traffic from the wired network using firewalls or other methods.

Agencies Established Policies for Access Controls for Mobile Devices, but Several Agencies Did Not Specifically Address Wireless Functionality of Laptops, Dual Connection of Laptops, or International Travel of Mobile Devices

Almost all agencies had established some type of access control policy for mobile devices. Specifically, all 24 agencies developed policies for PDAs, such as smartphones, although 2 agencies' policies had not been finalized. Although 23 of the 24 agencies had developed implementation guidance for laptop computers, the policies of 4 of these agencies did not specifically address wireless functionality on laptops. In addition, 1 of the 24 agencies did not document laptop policies at all.

Fewer agencies had developed access control policies regarding dual connection of laptops. NIST guidelines recommend that client devices, such as laptop computers, should be configured not to allow the simultaneous use of more than one network interface. Although most agencies had established policies for wireless-enabled laptops, many did not address the risk of dual connections of laptops in their policies. As described earlier, the security of an agency network could be compromised when a laptop is connected to an external wireless network, and to an agency's wired network simultaneously, leaving it vulnerable to attack and providing unauthorized access to the wired network. Turning off or disabling the wireless capability when a laptop is connected to a wired network mitigates this risk. Of the 24 agencies in our review, 8 did not have documented policies requiring the wireless capability to be turned off or disabled when the agency's laptop is connected to a wired

[15] A service set identifier is a name assigned to a wireless network that allows wireless clients to distinguish one wireless network from another.

[16] The media access control address is a unique identifier assigned to network adapters usually by the manufacturer for identification. Although intended to be a permanent and unique identification, it is possible to change the media access control address on most hardware.

network. One agency with a decentralized wireless management structure had a high level overall wireless policy, but allowed its components to determine whether to augment it with more detailed policies, including policies prohibiting multiple network connections. Other agency officials incorrectly thought that the dual connection issue was addressed by governmentwide guidance such as the Federal Desktop Core Configuration (FDCC).[17]

Although the baseline FDCC standard disables wireless connectivity, in March 2010,[18] we reported that many agencies have chosen to deviate from the standard and enable wireless functionality on their workstations. No other setting or combination of settings within the FDCC standard prevents multiple network connections. We also previously reported that OMB had not specified any guidance for agencies to use when considering the risks of deviating from the FDCC standard; OMB has therefore not specified any such guidance for agencies regarding permitting the use of wireless technologies. We recommended that OMB clarify its policies regarding FDCC deviations to include guidance for agencies to use when assessing the risks of deviations. Until OMB provides guidance to agencies regarding the risks associated with enabling wireless on agency laptops, including the risk of dually connected laptops, agencies may not document and implement policies prohibiting dual connections, increasing the risk that an attacker would be able to gain unauthorized access into an agency's network and destroy, modify, or copy sensitive information. Further, until agencies fully document and implement policies prohibiting dual connections, an increased risk exists that an attacker would be able to gain unauthorized access into an agency's network and destroy, modify, or copy sensitive information.

Similarly, many agencies also did not have documented policies governing international travel with mobile devices. As noted earlier, according to NIST, a leading practice for client and mobile devices is to issue specially configured laptops, PDAs, and other mobile devices to individuals traveling to locations considered to be high risk and to apply preventative

[17] The FDCC was an initiative launched by OMB to require federal agencies to implement common security configurations on Microsoft Windows XP and Vista operating systems. The initiative has evolved into the United States Government Configuration Baseline, run by NIST.

[18] GAO, *Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements*, GAO-10-202 (Washington, D.C.: Mar. 12, 2010).

measures to devices being returned from such locations. However, only 12 of the 24 agencies had documented policies for safeguarding PDAs taken internationally, and policies for 4 agencies were in draft. Policies of 5 agencies required specially configured devices to be issued for such travel, although policies of 10 agencies required preventative measures to be applied to the devices after they were returned from travel and before being connected to agency networks. In addition, just 9 of the 24 agencies had documented policies for laptops taken internationally; including 2 agencies that had draft policies. Only 4 of the 9 agencies required that a specially configured laptop be used for travel, although 8 agencies required preventative measures to be applied after the devices were returned from travel.

Several agency officials stated that they were aware of the risks posed to mobile devices during international travel, but that agencies had not yet developed policies to address these risks. NIST issued its updated guidelines on this practice in August 2009, and many agencies had not yet updated their security policies to reflect the new guidelines. By not having documented policies, agencies may be at increased risk that sensitive information could be compromised while a device is in another country, or that malware obtained during an international trip could be inadvertently introduced onto agency networks, placing sensitive data and systems at risk.

All Agencies Required a Risk-Based Approach to Wireless Deployment, and Most Required Approval of New Wireless Technologies

All of the agencies in our review required in their policies that decisions related to management of wireless technologies be based on risk. Fifteen agencies had policies that specifically required a risk-based approach to wireless management; the remaining 9 agencies had policies that, while not specific to wireless, required a risk-based approach to all management of IT.

Twenty-two of the 24 agencies had documented policies specifying that new wireless technologies require approval from an appropriate official or governing body before they could be implemented, although one agency's policy was still in draft. The remaining 2 agencies, while not specifying wireless, required all new technologies to be approved.

Many Agencies Did Not Use a Centralized Structure for Wireless Management

Although a centralized wireless management structure can provide a more effective means of managing wireless networks, many agencies reported not using a centralized approach. Eleven agencies indicated that they did have a centralized wireless management structure, and 3 indicated using both a centralized and decentralized structure, depending on agency component. Ten agencies employed a decentralized wireless management structure. As previously mentioned, a decentralized wireless management structure can result in disparate, ad hoc networks that are independently managed, which can impede effective implementation and monitoring of security controls and inhibit sufficient oversight of the wireless network. The following examples describe 2 agencies that are implementing a centralized management approach and identify the benefits and limitations of their implementation efforts.

One agency where we performed detailed testing had deployed a centrally monitored and managed wireless intrusion detection system that was integrated with the agency's national wired networks and operated centrally by its cybersecurity management center. This system had several positive aspects such as eliminating the need for trained personnel in every location, easy integration with other automated tools, and a console that provided a summary view of security events and detected devices. Additionally, it provided a central means to monitor configurations of wireless devices, discover rogue access points, and detect intrusion attempts. However, this system also had limitations. According to agency officials, the center did not always manage the installation and configurations of wireless devices at the facilities being monitored. As a result, the agency could not take full advantage of the improved visibility and oversight of the agency's entire wireless network that centralized management can offer.

Another agency was deploying a centrally managed WLAN nationwide to hundreds of facilities. According to agency officials, the WLAN would provide a platform for numerous systems and devices to be operated in a highly mobile environment. The centrally managed WLAN has the potential to simplify and provide more control over WLAN management. For instance, configuration policies created in templates can be forwarded to all controllers connected to the network and then on to the wireless access points. It can also provide a graphical display of the WLAN and its performance.

Agencies had decentralized approaches to wireless management for several reasons. Several agencies managed IT in a decentralized manner, delegating responsibility to agency components based on their business needs. Other agencies were just beginning to consider use of WLANs, or had only deployed WLANs in a limited manner. Technological advances have also made centralized management of wireless more feasible than in the past. Furthermore, while existing federal guidelines recognizes the benefits that centralized management of information security can provide for federal agencies; existing NIST guidelines on wireless security do not provide detail on the appropriate ways agencies can centralize their management of wireless technologies based on business need.

Until agencies effectively implement a centralized wireless management structure, they will have limited visibility and control over WLANs and a limited ability to integrate wireless management controls with the existing wired network to provide continuity and robustness to their organization's overall information security program.

Although Access Points Were Generally Configured Securely, Weaknesses Existed in Configurations of Laptops, Firewalls, and Smartphones Used for Wireless Access

At the five agencies where we conducted detailed testing, the access points used to provide WLANs were generally configured in a secure manner. However, we identified weaknesses in laptop or firewall configurations at these agencies as the following examples illustrate:

- None of the five agencies had fully implemented controls to prevent laptops from connecting to a wireless network while also being connected to the agency's internal wired network. As described earlier, when a laptop is connected to a wireless network and to an agency's wired network simultaneously, an attacker could exploit this dual connection to gain unauthorized access to the agency's network, placing sensitive information and systems at risk. In certain cases, agency officials were unaware that the potential for a dual connection existed. In other cases, officials were aware of the risk, but were unsure of the appropriate controls that could mitigate this risk, or were concerned that these controls might interfere with needed functionality of the device. In general, workstations using Microsoft Windows require an additional third-party application or other specialized configuration to disable wireless connectivity. Although NIST guidelines recommend that client devices, such as laptop computers, be configured to not allow the simultaneous use of more than one network interface, existing NIST guidelines on wireless networks do not provide specific technical information on steps that agencies should take to implement this control.

- One of the five agencies had configured a laptop to allow nonprivileged users to enable Bluetooth and to connect to other personal Bluetooth devices. Furthermore, Bluetooth was configured to default to "discovery" mode, making the laptops visible to other Bluetooth devices. As a result, an attacker with a Bluetooth device within range could connect to the agency's laptop, providing a means of unauthorized access to sensitive information on the laptop itself, as well as to the agency's network.

- Two agencies allowed general users to have administrative privileges on their laptops, thus reducing the effectiveness of established security controls on those machines and increasing the risk that users could install unapproved and potentially malicious software, which could allow sensitive information to be viewed, modified, or deleted.
- At one agency, a firewall[19] segmented a guest wireless network from the agency's internal network. However, the firewall was configured to allow all traffic that used Internet protocol version 6 (IPv6) to flow between the networks without controls. As a result, any user—whether malicious or not—connected to the guest wireless network using the IPv6 protocol could traverse the guest network without any authentication or access controls and could potentially gain unauthorized access to the internal network, placing sensitive agency information and systems at risk of unauthorized disclosure, modification, misuse, or destruction.

Many agencies also did not enforce secure configurations on their BlackBerry smartphones. DISA has developed a configuration checklist to help its administrators securely configure its BlackBerry Enterprise Servers, which are servers that allow agencies to centrally control security policy for BlackBerry smartphones. These guidelines have also been made available to other organizations, including federal agencies, as part of a NIST program providing secure configurations for computing devices. Although not mandatory, the guidelines provide a starting point for securely configuring BlackBerry smartphones. However, 18 of the 24 agencies had server configurations that were less secure than the DISA guidelines. For example:

- Fourteen agencies allowed BlackBerry passwords of insufficient length. DISA recommends that passwords on BlackBerry smartphones be a minimum of eight characters in length.

[19] A firewall is a hardware or software component that protects given computers or networks from attacks by blocking network traffic or by allowing only authorized protocols and services to cross the boundary between networks.

- Seven agencies did not require the use of complex passwords. DISA recommends that this value be configured to require passwords to contain, at a minimum, at least one alphabetic character and one numeric character.

- Eleven agencies did not set a sufficient security timeout period. DISA recommends that this value be set to 15 minutes or less.

- Ten agencies did not configure a setting that prevents applications from opening internal and external connections simultaneously, exposing the device to malware.

Several agency officials stated that the DISA checklist was not mandatory for federal agencies; however, no other federal configuration standard for BlackBerry smartphones currently exists. Due to their portability and capacity to collect and store significant amounts of sensitive information, smartphones such as the BlackBerry are susceptible to security threats such as loss, theft, unauthorized access, malware, electronic eavesdropping, and tracking. Without securely configuring their BlackBerry Enterprise Servers, agencies are at an increased risk that their BlackBerry smartphones could be compromised, resulting in tampered, lost, or stolen data.

Agencies Have Improved Wireless Security Training Efforts, but Training Often Lacked Key Elements

Many agencies did include key information on the risks of wireless technologies and how to mitigate such risks in their training programs. Specifically, 18 agencies provided training on the inherent lack of security of wireless technology and gave information on how employees and contractors could protect information that is transmitted wirelessly. However, 6 agencies did not address wireless security in their annual training.

In addition, although most agencies included information on mobile devices in their security awareness training, most agencies did not include key elements in accordance with NIST guidelines. Specifically, only 2 of the 24 agencies included in their training that users should disable the wireless interfaces on their mobile devices when not needed. In addition, training at 14 agencies did not address physical control over mobile devices; 5 did not describe the procedures for reporting lost or stolen mobile devices; and 5 did not include information on encrypting sensitive data on mobile devices. Finally, 1 agency did not address mobile device security in its annual training.

Awareness about wireless security challenges can assist employees in complying with policies and procedures to reduce agency information security risks. Without such training, employees and contractors may practice behaviors that threaten the safety of the agency's data.

Agency Policies Did Not Always Require the Use of a VPN or Encryption for Remote Access

Policies on remote access are important to the security of wireless devices because a frequent use of wireless technologies is for access to agency networks from remote locations, such as a home or hotel WLAN. Twenty of the 24 agencies required remote access sessions to be encrypted, and 8 of these agencies specified that a VPN must be used. However, 4 of the 24 agencies did not require remote access to be encrypted using a VPN or other encryption method. Without having policies requiring remote access sessions to employ adequate encryption, agencies will not be able to ensure that sensitive information is protected from unauthorized access, use, disclosure, or modification when users connect to agency information systems remotely.

Many Agency Policies and Practices for Monitoring 802.11 Networks and Conducting Assessments Were Insufficient

All 24 agencies in our review reported some form of monitoring for the existence of unauthorized or "rogue" wireless networks. Sixteen agencies reported that they continuously monitored 24 hours a day at one or more agency facilities. However, we found significant weaknesses in agency policies for wireless monitoring. Only 18 agencies required any type of monitoring for unauthorized access points in their policies, sometimes as rarely as once per year. In addition, two agencies used outdated scanning tools that could miss key wireless activities. Six agencies lacked any requirements for wireless monitoring. This lack of requirements, combined with the ease of setting up wireless networks, creates a situation in which wireless networks can be operating in these agencies without authorization or the required security configurations.

At the five agencies where we performed detailed testing, we found that the approach that several locations took toward monitoring and assessments for 802.11 wireless activity had significant weaknesses. Five agency locations did not have routine procedures for performing wireless assessments for unauthorized devices and networks. Two of these locations had not performed wireless scans in the past 2 years; two other agency locations did not document the results of scans.

One agency where we performed detailed testing had deployed a centrally monitored and managed wireless intrusion detection system at one of its locations. However, according to agency officials, because of the costs of the system, it was not deployed to all locations. At the location we visited that did not have the system deployed, there was no alternate approach to wireless monitoring, posing the risk of undetected wireless access points, intrusions, and loss of sensitive, proprietary data.

Further, while three other agencies also used a wireless intrusion detection system at some locations to continuously monitor for unauthorized devices and networks, the monitoring at these locations was ineffective. Specifically, the systems at each location had not been tailored to ignore known false positives. As a result, the systems generated large numbers of alerts for rogue access points, most of which were false. Local network administrators therefore had no way to determine which alerts were actual security events, hindering their ability to take advantage of the security aspects of the system.

Although NIST guidelines recommend that agencies use wireless monitoring, it does not specify criteria for selecting tools to ensure they provide comprehensive monitoring capabilities, nor does it suggest appropriate frequencies for recurring assessments or recommendations for when continuous monitoring may be appropriate.

Regular monitoring and security assessments are key practices for ensuring the security of wireless networks and devices. Even at agencies that have no wireless networks deployed, wireless-enabled devices that are deployed on the network, such as laptop computers, can provide a potential means for an attacker to gain unauthorized access to the network, putting critical agency systems and information at risk of unauthorized modification, misuse, disclosure, or destruction. Until regular monitoring and assessment policies and practices are implemented, these networks are at increased vulnerability to attack.

Existing Governmentwide Reporting and Oversight Efforts Do Not Fully Address Key Wireless Security Practices

The annual FISMA reporting process administered by OMB (and recently devolved from OMB to DHS by an OMB memorandum), which serves as a means of oversight of federal agency information security, does not fully address implementation of leading practices in wireless security. As of October 2010, the fiscal year 2010 draft reporting metrics do contain measures related to automated configuration management, vulnerability management, and incident management. However, they do not include specific metrics related to wireless security issues identified in this report, such as measures to address the risk of dual-connected laptops, policies related to international travel with mobile devices, the extent to which agencies have centralized their management of wireless devices, and agency practices for monitoring and assessment of wireless networks.

Furthermore, although the DHS official responsible for the agency's newly assigned governmentwide FISMA compliance activities stated that the agency plans additional activities that may address aspects of wireless security governmentwide, the scope and time frames for these activities have not yet been finalized.

Until OMB and DHS ensure they have effective means for oversight of federal agencies' efforts to secure wireless networks, they lack full visibility of the vulnerability of these networks to attack.

Conclusions

Federal agencies are making significant use of wireless networks and devices, including WLANs, laptop computers, and smartphones. Several leading practices exist to secure these technologies, including developing comprehensive policies, employing a centralized approach to management, establishing secure network and device configurations, and having effective training and monitoring in place.

Agencies have taken several steps to address the security of their wireless networks and devices, including development of security policies, centralized management, training, and monitoring; however, these steps have not been fully and comprehensively applied across the government. Gaps exist in policies, network management was not always centralized, and numerous weaknesses existed in configurations of laptops and smartphones. Particular issues are the risk of dual-connected laptops and risks related to mobile devices being taken on international travel In addition, many agencies had insufficient policies and practices for monitoring or conducting assessments of wireless technologies. Until OMB, DHS, NIST, and individual agencies take steps to fully implement leading security practices, federal wireless networks will remain at increased vulnerability to attack, and information on these networks is subject to unauthorized access, use, disclosure, or modification.

Recommendations for Executive Action

To improve governmentwide oversight of wireless security practices, we recommend that the Director of OMB, in consultation with the Secretary of Homeland Security, implement the following two recommendations:

- include metrics related to wireless security as part of the FISMA reporting process, and
- develop the scope and specific time frames for additional activities that address wireless security as part of their reviews of agency cybersecurity programs.

We also recommend that the Secretary of Commerce instruct the Director of NIST to develop and issue guidelines in the following four areas:

- technical steps agencies can take to mitigate the risk of dual connected laptops,
- governmentwide secure configurations for wireless functionality on laptops and for smartphones such as BlackBerries,
- appropriate ways agencies can centralize their management of wireless technologies based on business need, and
- criteria for selection of tools and recommendations on appropriate frequencies of wireless security assessments and recommendations for when continuous monitoring of wireless networks may be appropriate.

In addition, in a separate report with limited distribution, we are making 134 recommendations to 24 major federal agencies to address weaknesses in wireless-related information security controls, including policies, procedures, and technical configurations.

Agency Comments and Our Evaluation

We provided a draft of this report to the Director of OMB and the Secretary of Commerce for their review and comment. However, OMB did not provide comments on the report.

In written comments on a draft of this report, the Secretary of Commerce stated that the department concurred with our recommendations that NIST develop additional guidance related to wireless security. The Secretary also suggested that we use the term "NIST guidelines" rather than "NIST guidance" throughout the report, in addition to other technical comments. We have incorporated these comments in the report where appropriate.

We are sending copies of this report to the appropriate congressional committees, the Director of OMB, the Secretary of DHS, the Secretary of Commerce, and other interested congressional parties. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact Gregory Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499, or by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati

Dr. Nabajyoti Barkakati
Chief Technologist

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) identify leading practices and state-of-the-art technologies for deploying and monitoring secure wireless networks and (2) assess agency efforts to secure wireless networks, including vulnerability to attack. The scope of our review included the 24 major federal agencies covered by the Chief Financial Officers Act.[1]

To identify leading practices for deploying and monitoring secure wireless networks, we first identified subject matter experts, including leading organizations and individuals, by reviewing information security-related Web sites and professional literature. In addition, we identified organizations that received recognition based on an industry magazine's rankings for top wireless or other information security-related products. We also solicited suggestions on subject matter experts from individuals working in the field of wireless security at major information technology (IT) and telecommunications companies and federal government agencies, such as the National Institute of Standards and Technology (NIST), National Security Agency, and Committee on National Security Systems, because they were in a position to evaluate and compare wireless security practices at numerous organizations. We contacted approximately 10 organizations and individuals that met the above criteria; 8, including 5 organizations and three individuals, agreed to be interviewed and provide input on the practices we identified. The organizations were prominent and nationally known, and the individuals were recognized as experts in the information security community. The participants included a wireless services provider, a global technology products and services provider, a global telecommunications provider, a nonprofit industry organization, a standards laboratory, a government information security consortium, a defense agency, and a wireless security consultant.

Then, to determine the specific leading practices, we obtained information, primarily through analysis of publications, guidance, checklists, presentations, and other documentation, and interviews with subject matter experts. We supplemented the information gathered with information obtained from our professional literature review. We then

[1] The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

analyzed the information obtained to identify common wireless security leading practices and validated the practices we identified with the subject matter experts.

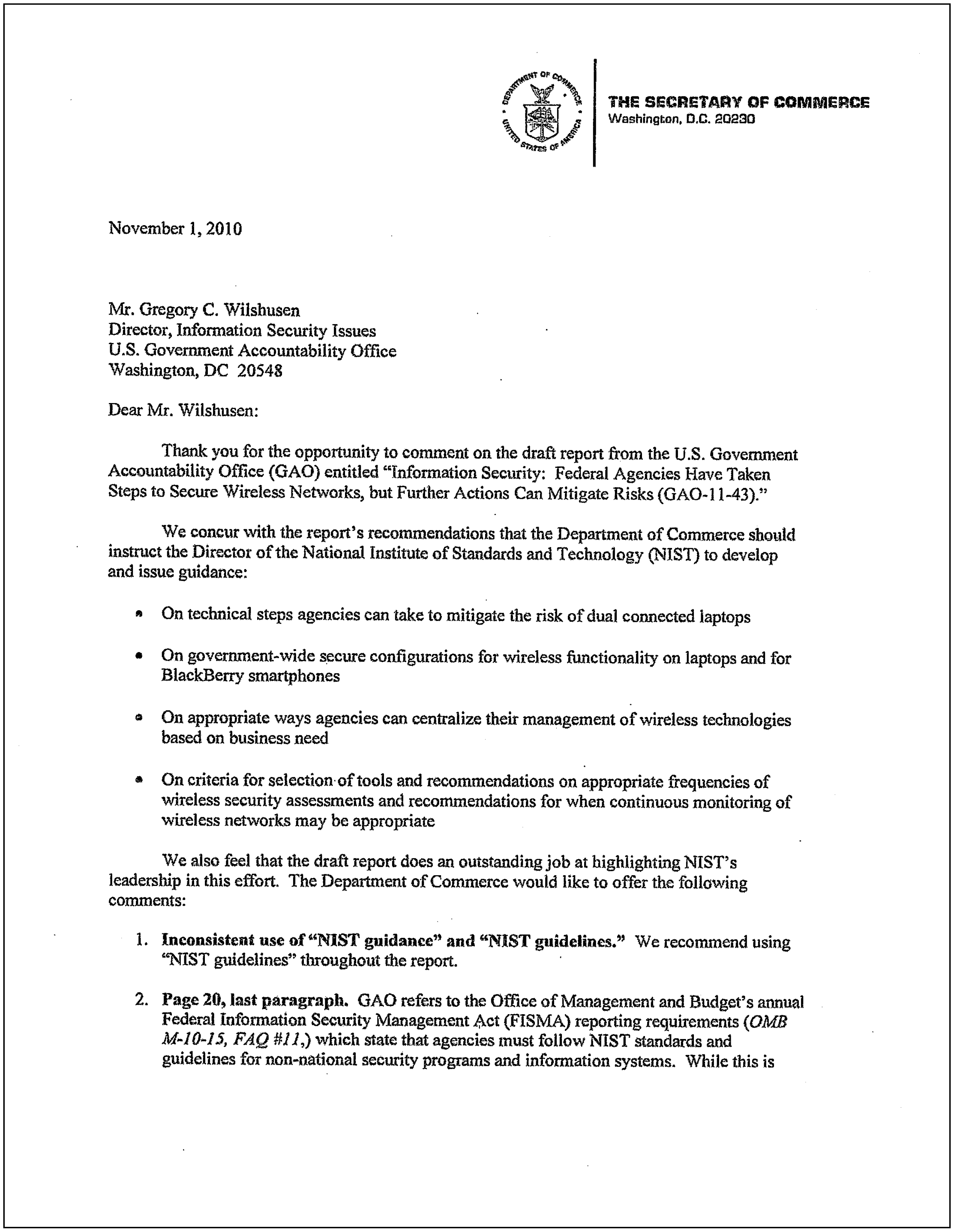
To assess agency efforts to secure wireless networks, we obtained and analyzed documents such as departmental and component policies, plans, configuration documents, and training materials to determine the extent of wireless technologies used and the security controls implemented at each of the 24 major federal agencies. We also obtained information through structured interviews with officials responsible for wireless security policies and practices for each of the 24 agencies. For each of these agencies, we used a laptop equipped with an antenna that served as a mobile scanning device and walked or drove around the perimeters of publicly accessible areas of their headquarters facilities in the Washington, D.C., area to collect data to determine wireless technologies that were deployed in the buildings. We also conducted scans of multiple agency facilities in another major metropolitan area outside of the Washington, D.C., region. This area was chosen based on the following criteria:

- contained regional offices for the multiple major federal agencies in locations that were sufficiently dispersed to not have too many 802.11 signals within a narrow proximity; and
- had several regional offices with additional field offices nearby.

Based on the initial data collected from scans at the headquarters and field locations, we chose 5 of the 24 agencies at which to complete additional detailed wireless security testing, specifically, the Departments of Agriculture, Commerce, Transportation, and Veterans Affairs, and the Social Security Administration. These agencies were selected based on several criteria, including the amount of usage of wireless technologies, the level of centralization of IT management, and potential security issues revealed by the initial scan results. More in-depth testing at these agencies included a review of the configurations of client devices, wireless infrastructure, and monitoring practices. We inspected client devices to determine if security controls had been implemented to protect the local network. We also examined each agency's network infrastructure to determine if access points were encrypted and configured to deny unauthorized access. Finally, we determined if the agencies monitored the IEEE 802.11 wireless spectrum.

We conducted this performance audit from January 2010 to November 2010, 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 based on our audit objectives.

Appendix II: Comments from the Department of Commerce



THE SECRETARY OF COMMERCE
Washington, D.C. 20230

November 1, 2010

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

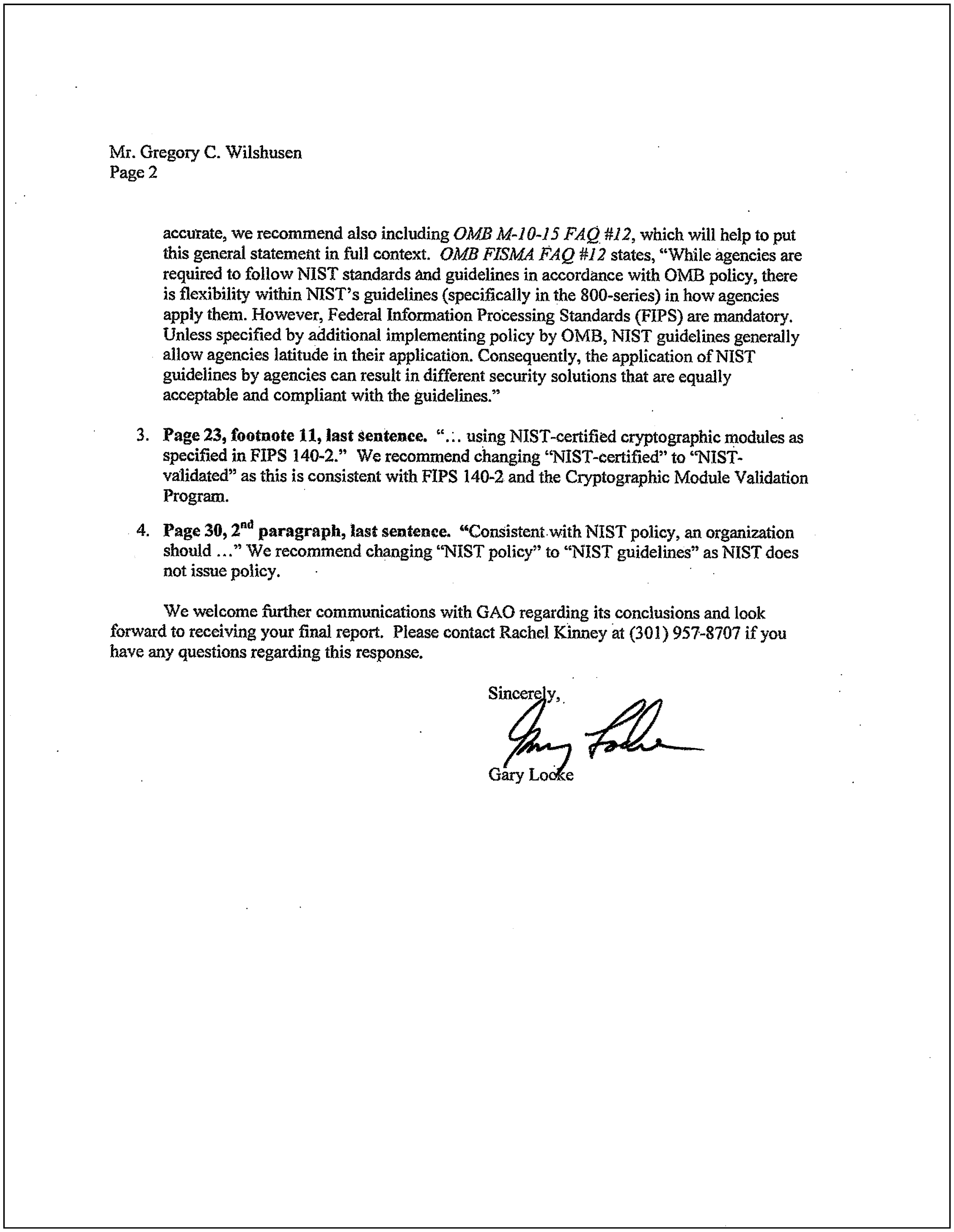
Thank you for the opportunity to comment on the draft report from the U.S. Government Accountability Office (GAO) entitled "Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risks (GAO-11-43)."

We concur with the report's recommendations that the Department of Commerce should instruct the Director of the National Institute of Standards and Technology (NIST) to develop and issue guidance:

- On technical steps agencies can take to mitigate the risk of dual connected laptops
- On government-wide secure configurations for wireless functionality on laptops and for BlackBerry smartphones
- On appropriate ways agencies can centralize their management of wireless technologies based on business need
- On criteria for selection of tools and recommendations on appropriate frequencies of wireless security assessments and recommendations for when continuous monitoring of wireless networks may be appropriate

We also feel that the draft report does an outstanding job at highlighting NIST's leadership in this effort. The Department of Commerce would like to offer the following comments:

1. **Inconsistent use of "NIST guidance" and "NIST guidelines."** We recommend using "NIST guidelines" throughout the report.
2. **Page 20, last paragraph.** GAO refers to the Office of Management and Budget's annual Federal Information Security Management Act (FISMA) reporting requirements (*OMB M-10-15, FAQ #11,*) which state that agencies must follow NIST standards and guidelines for non-national security programs and information systems. While this is



Mr. Gregory C. Wilshusen
Page 2

accurate, we recommend also including *OMB M-10-15 FAQ #12*, which will help to put this general statement in full context. *OMB FISMA FAQ #12* states, "While agencies are required to follow NIST standards and guidelines in accordance with OMB policy, there is flexibility within NIST's guidelines (specifically in the 800-series) in how agencies apply them. However, Federal Information Processing Standards (FIPS) are mandatory. Unless specified by additional implementing policy by OMB, NIST guidelines generally allow agencies latitude in their application. Consequently, the application of NIST guidelines by agencies can result in different security solutions that are equally acceptable and compliant with the guidelines."

3. **Page 23, footnote 11, last sentence.** "... using NIST-certified cryptographic modules as specified in FIPS 140-2." We recommend changing "NIST-certified" to "NIST-validated" as this is consistent with FIPS 140-2 and the Cryptographic Module Validation Program.

4. **Page 30, 2nd paragraph, last sentence.** "Consistent with NIST policy, an organization should ..." We recommend changing "NIST policy" to "NIST guidelines" as NIST does not issue policy.

We welcome further communications with GAO regarding its conclusions and look forward to receiving your final report. Please contact Rachel Kinney at (301) 957-8707 if you have any questions regarding this response.

Sincerely,

Gary Locke

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, or wilshuseng@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499, or barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Lon Chin and Vijay D'Souza (Assistant Directors), Monica Anatalio, Mark Canter, William Cook, Neil Doherty, Rebecca Eyler, Nancy Glover, Matthew Grote, Min Hyun, Javier Irizarry, Franklin Jackson, Vernetta Marquis, Sean Mays, Lee McCracken, and Michael Stevens made key contributions to this report.

(311060)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548